Taiwan-CA Inc. (TWCA)

Certification Practice Statement (CPS)

Version 4.0

Effective Date：2025/04/17

Revision History

Version	Effective Date	Released by	Remarks
Version. 1.0	89/03/20	TaiCA	First release.
Version. 1.1	91/03/01	TaiCA	Revised according to the integration of TaiCA CA PKI system documents (CPS, CP, etc.) and the EDI (PAA CP) of Trade-VAN.)
Version 1.2	91/11/04	TaiCA	1. Revised according to the Electronic Signatures Act, Enforcement Rules of the Electronic Signatures Act and Regulations on Required Information for Certification Practice Statements established by made by the Ministry of Economic Affairs, the competent authorities. 2. Submission for review of TaiCA certification authorities: (1) Network Banking Certification Authority, (2) Enterprise EC Certification Authority, (3) Business EC Certification Authority, and (4) Financial eXtensible Markup Language Certification Authority. 3. Approved by the Ministry of Economic Affairs on 4 November 2002 in Letter Jing-Shang-Zi No. 09102245130.
Ver.1.3	94/02/18	TWCA	1. Revised according to the addition of the electronic stock-affairs certificate operations, on-line insurance certificate operations, and certificate multipurpose operations. 2. Revised the applicability of certificate and transaction amount limit. 3. The term "Certificates Service Provider" (CSP) is over generalized and unable to accurately describe the nature of CA. In this version, it is substituted with "User Certification Authority (UCA)" or "Certification System".
Ver.2.0	97/03/04	TWCA	1. Deleted the Enterprise EC Certificate section after the service is suspended. 2. Revised Certification Authority to Certification Management Authority. 3. Revised the Financial XML Certificate to Commercial XML to avoid confusion with the XML Certificate issued by the Bankers Association of the Republic of China.
Ver.2.1	97/11/12	TWCA	1. Added the applicability of e-voting services. 2. Adjusted the descriptions of Name. 3. Improved the descriptions for key length.

Ver 2.2	98/07/14	TWCA	1. Added the applicability of online patent/trademark application. 2. Rhetoric changes.
Ver 2.3	99/07/23	TWCA	1. Revised the English diction of the CPS. 2. Added the applicability of certificates. 3. Added the S/MIME UCA under the Commercial XML Certificate System. 4. Separated the SSL from EC+ UCA to form the SSL UCA. 5. Revised the description of refund.
Ver 2.4	100/07/08	TWCA	1. Supplementary notes to SSL server certificates application procedure. 2. Supplementary notes to C-XML certificates application procedure.
Ver 2.5	103/07/02	TWCA	Addition of certificate re-issuance and algorithm upgrading.
Ver 2.6	104/06/22	TWCA	1. Addition of applicability. 2. Addition of the application of e-government, application of e-commerce and e-voting, under business EC certificates. 3. Addition of the application of e-government and e-voting under C-XML certificates.
Ver 3.0	106/02/20	TWCA	1. Revision per RFC3647. 2. Revision of the applicability of certificates. 3. Deletion of SSL certificates. 4. Deletion of NB certificates. 5. Addition of the authentication for Class 3 Certificate categorized into “Authentication in Face-to-face” and “Authentication in non Face-to-face”.
Ver 3.1	113/06/28	TWCA	1. Add ECC key description: Adjust 5.4.1, 6.1.5, 6.1.6, 7.1.3, Appendix 1, Appendix 2. 2. Adjust URL from http to https.
Ver 4.0	114/04/17	TWCA	Revise based on the new version of the Electronic Signature Act and its enforcement rules and Required Information for Certification Practice Statements.

Table of Contents

Executive Summary .... 錯誤! 尚未定義書籤。

1. Introduction **18**

1.1 Overview **18**

1.2 Document Name and Identification **18**

1.3 PKI Participants and Applicability **19**

1.3.1 Certification Authority 19

1.3.2 Registration Authority (RA) 21

1.3.3 Subscribers 22

1.3.4 Replying Parties 22

1.3.5 Other Participants 22

1.4 Certificate Usage **23**

1.4.1 Applicability of Certificate 23

1.4.2 Prohibited Certificate Uses 31

1.5 Policy Administration **31**

1.5.1 Organization Administering the Document 31

1.5.2 Contact Person 31

1.5.3 Person Determining CPS Suitability for the Policy 32

1.5.4 CPS Approval Procedures 32

1.6 Definitions and Acronyms **32**

2. Publication and Repository **33**

2.1 Repositories **33**

2.2 Publication of Certification Information **33**

2.3 Frequency of Publication **33**

2.4 Access Controls on Repositories **33**

3. Identification and Authentication **35**

3.1 Naming **35**

3.1.1 Types of Names 35

3.1.2 Need for Names to be Meaningful 37

3.1.3 Anonymity and Pseudonymity of Subscribers 38

3.1.4 Rules for Interpreting Various Name Forms 38

3.1.5 Uniqueness of Name 38

3.1.6 Recognition, Verification and Role of Trademarks 38

3.2 Initial Identity Validation **39**

3.2.1 Method to Prove Possession of Private Key 39

3.2.2 Authentication of Organization Identity 39

3.2.3 Authentication of Individual Identity 41

3.2.4 Non-verified Subscriber Information 42

3.2.5 Validation of Authority 43

3.2.6 Criteria for Interoperation 43

3.3 Identification and Authentication of Rekey Requests **43**

3.3.1 Identification and Authentication for Routine Rekey 43

3.3.2 Rekey after Certification Revocation 44

3.4 Certificate Revocation Request **44**

4. Certificate Life Cycle Operational Requirements **45**

4.1 Certificate Application **45**

4.1.1 Who Can Submit a Certificate Application 45

4.1.2 Enrollment Process and Responsibilities 45

4.2 Certificate Application Processing **45**

4.2.1 Performing Identification and Authentication Functions 45

4.2.2 Approval and Rejection of Certificate Applications.. 47

4.2.3 Time to Process Certificate Applications 47

4.3 Certificate Issuance 47

4.3.1 Certificate Issuance by the CA 47

4.3.2 Notification of Certificate Issuance by the CA to Subscribers.......................... 47

4.4 Certificate Acceptance 47

4.4.1 Conduct Constituting Certificate Acceptance.. 47

4.4.2 Publication of the Certificate by the CA.. 48

4.4.3 Notification of Certificate Issuance by the CA to Other Entities 48

4.5 Key Pair and Certificate Usage 48

4.5.1 Subscriber Private Key and Certificate Usage 48

4.5.2 Relying Party Public Key and Certificate Usage 49

4.6 Certificate Renewal... 49

4.6.1 Circumstances for Certificate Renewal 49

4.6.2 Who May Request Renewal Certificate... 49

4.6.3 Processing Certificate Renewal Requests 49

4.6.4 Notification of Renewal Certificate Issuance to Subscribers........................... 50

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 50

4.6.6 Publication of the Renewal Certificate by the CA 50

4.6.7 Notification of the Renewal Certificate Issuance by the CA to Other Entities . 50

4.7 Certificate and Private Key Renewal... 50

4.7.1 Circumstances for Certificate Key Renewal.. 50

4.7.2 Who May Request Renewal Certificate Key 50

4.7.3 Certificate Key Renewal Procedure 50

4.7.4 Notification of Renewal Certificate Key Issuance to Subscribers 50

4.7.5 Acceptance Procedure of Renewal Certificate Key 50

4.7.6 Publication of the Renewal Certificate Key by the CA 51

4.7.7 Notification of Renewal Certificate Key Issuance by the CA to Other Entities 51

4.8 Certificate Modification 51

4.8.1 Circumstances for Certificate Modification 51

4.8.2 Who May Request Certificate Modification 51

4.8.3 Certificate Modification Procedure 51

4.8.4 Notification of the Modified Certificate Issuance to Subscribers 51

4.8.5 Acceptance Procedure of the Key Certificate Modification 51

4.8.6 Publication of the Modified Certificate by the CA 51

4.8.7 Notification of the Modified Certificate Issuance by the CA to Other Entities . 51

4.9 Certificate Revocation and Suspension 52

4.9.1 Circumstances for Certificate Revocation 52

4.9.2 Who May Request Certificate Revocation 52

4.9.3 Procedure for Certificate Revocation 53

4.9.4 Revocation Request Grace Period 54

4.9.5 Time Within Which CA Shall Process the Revocation Request 55

4.9.6 Revocation Checking Requirements for Relying Parties 55

4.9.7 CRL Issuance Frequency 55

4.9.8 Maximum Latency for CRLs 55

4.9.9 Online Certificate Revocation/Status Enquire Service 55

4.9.10 Online Revocation/Status Enquire Checking Requirements 55

4.9.11 Other Forms of Publishing Revocation 55

4.9.12 Special Requirements of Rekey Compromise 56

4.9.13 Circumstances for Certificate Suspension 56

4.9.14 Who Can Request Certificate Suspension 57

4.9.15 Procedure for Certificate Suspension 57

4.9.16 Limits on Certificate Suspension Period 58

4.10 Certificate Status Service 59

4.10.1 Operational Characteristics 59

4.10.2 Service Availability 59

4.10.3 Additional Features 59

4.11 Termination of Certificate 59

4.12 Key Escrow and Recovery 59

4.12.1 Policy and Practices of Key Escrow and Recovery 59

4.12.2 Encryption Key Encapsulation and Recovery Policy and Practices 59

5. Facility, Management and Operational Controls 60

5.1 Physical Controls 60

5.1.1 Site Location and Construction 60

5.1.2 Physical Access 60

5.1.3 Power and Air Conditioning 60

5.1.4 Water Resistence 61

5.1.5 Fire Resistence 61

5.1.6 Media Storage 61

5.1.7 Waste Disposal 61

5.1.8 Offsite Backup 61

5.2 Procedural Control 62

5.2.1 Trusted Roles 62

5.2.1.1 Certification Authority (CA) 62

5.2.1.2 Registration Authority (RA) 63

5.2.2 Number of Persons Required Per Task 63

5.2.3 Identification and Authentication for Each Role 63

5.2.4 Roles Requiring Separation of Duty 63

5.3 Personnel Controls 64

5.3.1 Background, Qualifications, and Experience ... 64

5.3.2 Background Check Procedures ... 64

5.3.3 Training Requirements ... 64

5.3.4 Training Frequency and Requirements ... 65

5.3.5 Job Rotation Frequency and Sequence ... 65

5.3.6 Sanctions for Unauthorized Actions ... 65

5.3.7 Independent Contractor Requirements ... 65

5.3.8 Documentation Supplied to Personnel ... 66

5.4 Audit Logging Procedure ... 66

5.4.1 Types of Events Recorded ... 66

5.4.2 Frequency of Processing Log ... 67

5.4.3 Retention Period for Audit Log ... 67

5.4.4 Protection of Audit Log ... 67

5.4.5 Audit Log Backup Procedures ... 68

5.4.6 Audit Log Collection System ... 68

5.4.7 Notification to Event-Causing Subject ... 69

5.4.8 Vulnerability Assessment ... 69

5.5 Records Archival ... 69

5.5.1 Types of Records Archived ... 69

5.5.2 Retention Period for Archive ... 70

5.5.3 Protection of Archive ... 70

5.5.4 Archive Backup Procedures ... 70

5.5.5 Requirements for Time-Stamping of Records ... 71

5.5.6 Archive Collection System ... 71

5.5.7 Procedures to Obtain and Verify Archive Information ... 71

5.6 Key Changeover ... 71

5.6.1 Key Changeover of Subscriber ... 71

5.6.2 Key Changeover of UCA 72

5.6.3 Key Changeover of PCA 72

5.6.4 Key Changeover of RCA 73

5.7 Key Cracked and Disaster Recovery Procedures 73

5.7.1 Key Cracked and Emergency Handling Procedures 73

5.7.2 Corrupted Computing Resources, Software and Data Handling Procedures .. 73

5.7.3 Entity Private Key Cracked Handling Procedures 74

5.7.4 Business Continuity Capabilities after a Disaster 74

5.8 CA Service Termination 75

6. Technical Security Controls 77

6.1 Key Pair Generation and Installation 77

6.1.1 Key Pair Generation 77

6.1.2 Private Key Delivery to Subscriber 77

6.1.3 Public Key Delivery to Certificate Issuer 77

6.1.4 CA Public Key Delivery to Trusted Certificate Parties 77

6.1.5 Key Sizes 77

6.1.6 Public Key Parameters Generation and Quality Checking 78

6.1.7 Key Usage Purposes 78

6.1.8 Subscriber Key Generation Equipment 78

6.2 Private Key Protection and Cryptographic Module Engineering Control 78

6.2.1 Cryptographic Module Standards 78

6.2.2 Private Key (m-out-of-n) Multi-Person Control 79

6.2.3 Private Key Escrow, Recovery and Storage 79

6.2.4 Private Key Backup 79

6.2.5 Private Key Archival 79

6.2.6 Private Key Transfer Into or From a Cryptographic Module 79

6.2.7 Private Key Storage on Cryptographic Module ... 80
6.2.8 Method of Activating Private Key ... 80
6.2.9 Method of Deactivating Private Key ... 80
6.2.10 Method of Destroying Private Key ... 80
6.2.11 Cryptographic Module Rating ... 80
6.3 Other Aspects of Key Pair Management ... 80
6.3.1 Public Key Archival ... 81
6.3.2 Public Key and Private Key Validity Periods ... 81
6.4 Activation Data ... 81
6.4.1 Activation Data Generation and Installation ... 81
6.4.2 Activation Data Protection ... 81
6.4.3 Other Aspects of Activating Data ... 82
6.5 Computer Security Controls ... 83
6.5.1 Specific Computer Security Technical Requirements ... 83
6.5.2 Computer Security Rating ... 83
6.6 Life Cycle Technical Controls ... 83
6.6.1 System Development Controls ... 83
6.6.2 Security Management Controls ... 83
6.6.3 Life Cycle Security Level ... 84
6.7 Network Security Controls ... 84
6.8 Time-stamp ... 84
7. Certificate, CRL, and OCSP Profiles ... 85
7.1 Certificate Profile ... 85
7.1.1 Version Number(s) ... 85
7.1.2 Certificate Extension Columns ... 85
7.1.3 Algorithm Object Identifiers ... 85

7.1.4 Name Forms Identification 85

7.1.5 Name Constraints Identification 86

7.1.6 Certificate Policy Object Identifier 86

7.1.7 Usage of CP Constraints Extension Columns 86

7.1.8 CP Qualifiers Syntax and Semantics 86

7.1.9 Processing Semantics for the Critical Certificate Policy Extension Column ... 86

7.2 CRL Profile 87

7.2.1 Version Number(s) 87

7.2.2 CRL and CRL Entry Extension Columns 87

7.3 OCSP Profile 87

7.3.1 Version Number(s) 87

7.3.2 OCSP Extensions 87

8. Compliance Audit and Other Assessments 88

8.1 Frequency and Circumstances of Assessment 88

8.2 Identity and Qualifications of Assessors 88

8.3 Assessor’s Relationship to Assessed Entity 88

8.4 Topics Covered by Assessment 88

8.5 Actions Taken to Deficiency of the Result of Assessment 89

8.6 Publication of Results 89

9. Other Business and Legal Regulations 90

9.1 Fees 90

9.1.1 Certificate Issuance or Renewal Fees 90

9.1.2 Certificate Access Fees 90

9.1.3 Certificate Revocation or Status Information Access Fees 90

9.1.4 Fees for Other Services 90

9.1.5 Refund Policy 90

9.2 Financial Responsibility 90

9.2.1 Liability Coverage 90

9.2.2 Other Assets 91

9.2.3 Liability for End-Entities 91

9.3 Confidentiality of Business Information 93

9.3.1 Scope of Confidential Information 93

9.3.2 Information Not Within the Scope of Confidential Information 93

9.3.3 Responsibility to Protect Confidential Information 93

9.4 Privacy of Personal Information 94

9.4.1 Privacy Protection Plan 94

9.4.2 Types of Personal Privacy Information 94

9.4.3 Types of Non-personal Privacy Information 95

9.4.4 Responsibility to Protect Personal Privacy Information 95

9.4.5 Notice and Consent to Use Personal Privacy Information 95

9.4.6 Disclosure Pursuant to Judicial or Administrative Requirement 95

9.4.7 Other Information Disclosure Circumstances 95

9.5 Intellectual Property Rights 95

9.6 Responsibility and Obligation 96

9.6.1 CA Responsibilities and Obligations 96

9.6.2 RA Responsibility 96

9.6.3 Subscriber Responsibilities and Obligations 97

9.6.4 Relying Party's Responsibilities and Obligations 98

9.6.5 Repository Representations and Warranties 98

9.7 Disclaimers of Responsibilities 99

9.8 Limitation of Liability 100

9.9 Indemnities 100

9.10 Term and Termination ... 100

9.10.1 Term ... 100

9.10.2 Termination ... 100

9.10.3 Effect of Termination and Survival ... 100

9.11 Individual Notices and Communications with Users ... 100

9.12 Amendments and Publications ... 100

9.12.1 Procedure for Amendment ... 100

9.12.2 Amendments Notification Mechanism ... 101

9.12.3 Circumstances Under Which OID Shall be Changed ... 101

9.13 Dispute Resolution Procedures ... 101

9.14 Governing Law ... 102

9.15 Compliance with Applicable Law ... 102

9.16 Miscellaneous Provisions ... 102

9.16.1 Entire Agreement ... 102

9.16.2 Assignment ... 102

9.16.3 Survival ... 103

9.16.4 Enforcement ... 103

9.16.5 Act of God ... 104

9.17 Other Provisions ... 104

Appendix 1 Glossary ... 105

Appendix 2 Acronyms and Abbreviations ... 108

Executive Summary

The Certification Practice Statement (CPS) of Taiwan-CA Inc (TWCA) specifies the regulations for managing the following legally established Certificates Service Providers (CSP): (1) Business EC Certification Authority (EC+ CA) and (2) Commercial XML Certification Authority (C-XML CA), including the issuance, revocation, management and renewal of certificates. The important issues of the Taiwan CA Certification Practice Statement (CPS) are as follows:

1. Certificates to Issue

Types of certificates and applicability:

	Types of certificates	Level of Assurance	Applicability
1	EC+	Class 3	e-banking transactions, on-line order securities & futures transactions, e-financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, online patent/trademark applications, application of issuance and transaction of short-term bill, application of e-government, and personal identification service.
		Class 2	low-risk e-banking transactions, e-financial transactions, e-commerce applications, online tax declaration, e-invoice, application of emails, e-voting, application of e-government, and personal identification service.
		Class 1	e-Commerce applications and personal identification service.
2	C-XML	Class 3	e-banking transactions, on-line order securities & futures transactions, e-financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, online patent/trademark applications, and application of issuance and transaction of short-term bill, application of e-government, and personal identification service.
		Class 2	low-risk e-banking transactions, e-financial transactions, e-commerce applications, online tax declaration, e-invoice, application of emails, e-voting, application of e-government, and personal identification service.
		Class 1	e-Commerce applications and personal identification service.
Note: The assurance levels are detailed in Section 1.4, while the certificate applicability and liability are described in Section 1.4.1, Table 1.			

2. Legal Liabilities and Important Matters

Registration:

When applying for registration to the registration authority (RA), subscribers shall provide detailed and correct documents and data for certifying their identity and fully understand and agree to the rights and obligations specified in the application form and contract and the regulations for the application and use of certificates. Subscribers shall also accept the rules in such regulations prior to signing them as a sign of acceptance. When subscribers cause damage to another party by providing untrue or false data out of deliberation, negligence or indecent intentions, the subscriber shall be in full liability for indemnifying such party.

Use of certificates:

Subscribers shall properly retain the private key and personal identification number (PIN) of their certificates and mustnot disclose or lend them to another party. When there are security considerations or doubts about using the certificate as a result of identify fraud, exposure and loss of certificates, subscribers shall immediately report to the RA for further arrangements. When subscribers cause damage to another party for withholding the identify fraud, exposure and loss of certificates out of deliberation or negligence, they shall be in full liability for indemnifying such party.

Subscribers shall follow the rules and regulations specified in the CPS and Business Application System Standards to legally and correctly use their private keys and PINs in the relevant business systems. users shall have full liability for any damage resulted from the use of the private key and PIN (1) outside of the scope of certificate uses specified in the CPS, (2) in applications or business systems that may cause physical and mental injuries or death to the human body or critical hazards to social order and social environment, or (3) in applications or businesses prohibited in the laws and regulations related to the Electronic Signatures Act and by the competent authorities. Otherwise, the users shall have full liability for the damage that is caused.

Liability:

When employees of TWCA cause damage to users out of negligence as a result of processing subscriber registration, certificate issuance, certificate suspension and certificate revocation without following the CPS, CP and other relevant operating procedures and standards or by violating the relevant laws and regulations, TWCA shall indemnify the affected subscribers according to the liability specified in this CPS. The maximum amount of indemnity for a single certificate shall be subject to the amount defined in Section 1.4.1.2. When such damage is caused by TWCA employees out of deliberation or gross negligence, TWCA shall be fully liable for the actual damage that is caused to the corresponding subscribers.

When damage is caused during the issue of certificates as a result of an interruption or failure of Internet transmission, neither the deliberation nor negligence of TWCA or an act of God (e.g. war or earthquake), TWCA shall be free from any liability for indemnifying such damage.

After a subscribers or any person entitled to make a request of certificate revocation makes a request of certificate revocation or suspension and before the UCA publishes the revocation (CRL) of that certificate, if that certificate is used in illegal transactions or there are disputes arising out of or in connection with the transactions made with that certificate, TWCA shall be free from any liability when the request of certificate revocation is processed according to this CPS and the relevant operating procedures.

3. Other Important Matters

(1) The company obtained ISO/IEC 27001:2005 certification for its Information Security Management System (ISMS) in September 2007 and has continuously maintained its validity. The certification was subsequently upgraded to ISO/IEC 27001:2013 in December 2014 and to ISO/IEC 27001:2022 in June 2024.

(2) The company obtained BS 10012 certification for its Personal Information Management System (PIMS) in November 2013. In July 2018, the certification was upgraded to BS 10012:2017, and the company simultaneously acquired ISO/IEC 27701 certification for Privacy Information Management. Both certifications remain valid to date.

(3) The company obtained ISO/IEC 20000-1 certification for its IT Service Management System (ITSMS) in December 2020, and it remains valid to date.

(4) The company obtained ISO 22301 certification for its Business Continuity Management System (BCMS) in November 2021 and has maintained its validity since.

(5) The company engages an independent accounting firm annually to conduct external audits in order to ensure compliance with the Certification Practice Statement (CPS) and Certificate Policy (CP).

1. Introduction

1.1 Overview

In order to build a secure and reliable network environment where no fabrication, alteration or theft of data during network transfer is assured, the identity of both parties involved in a transaction is identified, and the repudiation of transactions after completion is prevented, the government thus promoted the implementation of certification authority where identity certification and transaction certification services are provided to develop faith in users and ensure the rights and benefits of both parties in a transaction.

As a trustworthy certification authority, Taiwan-CA Inc. (TWCA) is a joint venture formed by the following corporations: Taiwan Stock Exchange Corporation (TWSE), Financial Information Service Corporation (FISC), Trade-van Information Services Corporation (TRADEVAN), Taiwan Depository & Clearing Corporation (TDCC), HiTRUST.COM Incorporated (HiTRUST), etc.

In order to provide subscribers the certification services needed for online transactions, 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, subscriber 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

The Object Identifiers (OID) of the corresponding CPs of individual certificate classes specified in this CPS are described as follows:

- EC+ Certificate

  OID=2.16.886.3.1.3.1

- C-XML Certificate

  OID=2.16.158.3.1.8.5

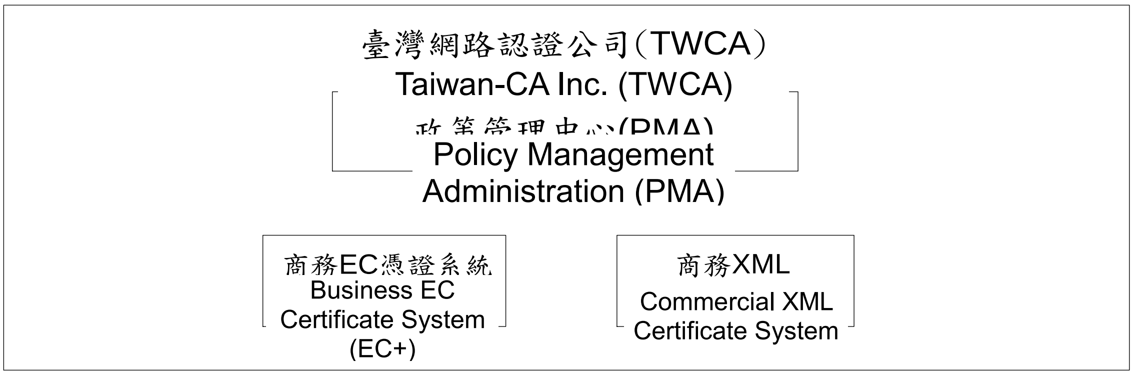
1.3 PKI Participants and Applicability

1.3.1 Certification Authority

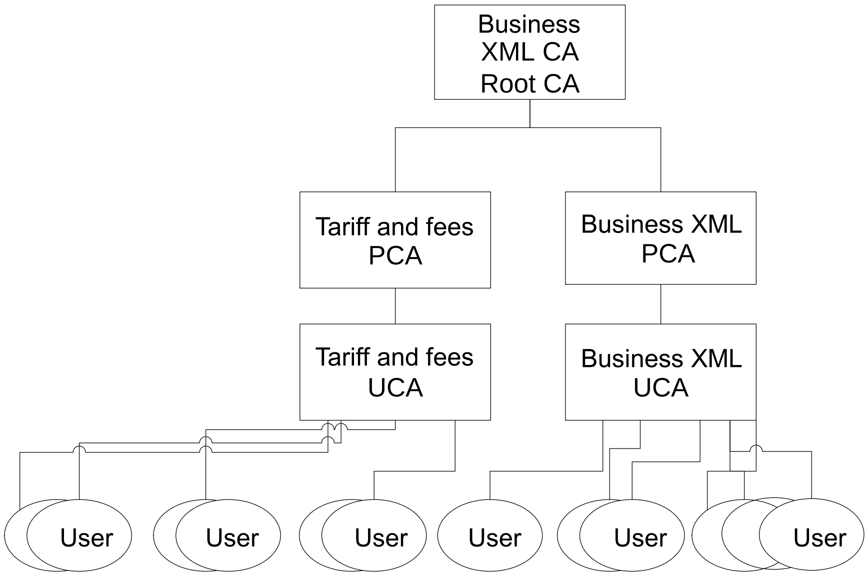
TWCA is an authority engaged in issuing and managing the following types of certificates: (1) Business EC Certificate (EC+) and (2) C-XML Certificate.

Along with the laws, policies, the Electronic Signatures Act and its enforcement rules and Required Information for Certification Practice Statements established by the competent authorities and business requirements, TWCA establishes, publishes and manages the identification and verification of the following identities and certificates.

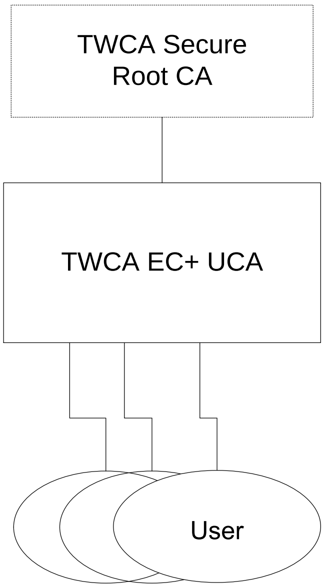
- The PKI framework and specifications of the Root Certification Authority (RCA), Policy Certification Authority (PCA) and User Certification Authority (UCA).
- CP and CPS.
- The contents of certificates and certificate revocation list.
- The code of operations and procedures of transnational certificate PKI cross certification.


臺灣網路認證公司（TWCA）
Taiwan-CA Inc. (TWCA)
政策管理中心(PMA)
Policy Management Administration (PMA)
商務EC憑證系統
Business EC Certificate System (EC+)
商務XML
Commercial XML Certificate System

C-XML Certificate System:



Business EC Certificate System (EC+):



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:

- Manages and publishes the operating procedures and verification code of operations of the registration, certificate and Certificate Revocation List (CRL) of CAs.

- Issues, manages and delivers the certificates and CRLs of PCAs.
- Implemented in an independent operating environment with security control where public keys are generated and implemented by two authorized personnel and CA certificates are issued. The Root CA certificates are self-issued certificates. When a new certificate is generated or there is a certificate change, the Root CA shall immediately deliver the new certificate to subscribers or notify them to collect the new certificate from the Root CA with the fastest method.

1.3.1.2 Policy Certification Authority (PCA)

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

- Follows the instructions established by the Root CA.
- Manages and publishes the operating procedures and verification code of operations of the registration, certification and CRL of UCAs.
- Issues, manages and delivers the CA certificates and CRLs.

1.3.1.3 User Certification Authority (UCA)

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

- Issues and manages user certificates and CRLs.
- Manages and publishes user certificates and users CRLs in the repository.
- Maintains the stability and operations of the repository.

1.3.1.4 Policy Management Authority (PMA)

The PMA is an organization under TWCA responsible for establishing the following items:

- Certification Policy (CP).
- Certification Practices Statement (CPS).
- Code of operations.

1.3.2 Registration Authority (RA)

An RA manages the UCA registration:

- Selects quality financial institutions or relevant units as RAs; these RAs shall process user registration after signing a contract with TWCA.
- A department dedicated to the registration affairs shall be established.
- Manages and publishes the operating procedures of applications for user registration

and requirements about personal identification.

- Verifies the application messages in user registration, certificate issue and revocation, and certificate access; the authenticity of identity and the veracity of messages.
- Delivers the messages of application for user registration, certificate revocation and certificate access to the UCA.
- Processes the certificate registration, certificate application and certificate revocation; and sends reply to users after verifying the veracity of the reply messages.
- Publishes and manages the registration name, URL, e-mail account and contact information of RAs.
- Processes charges.

1.3.3 Subscribers

Subscribers are the holders of certificates issued by the UCA. They include natural persons; juristic persons of profit or non-profit businesses; government agencies; financial group juristic persons; educational, charity and other related organizations; computer systems; and machinery. The scope of use of their certificates and the corresponding private keys are subject to this CPS. These shall include the relevant businesses, such as the e-commerce transactions of individuals or enterprise juristic persons over network banking systems, online ordering systems, online insurance systems, online bills and securities systems and online enterprise systems. Subscribers can sign the transaction message with the private key corresponding to their certificates.

1.3.4 Replying Parties

Replying parties refer to those using the certificate chain information of in the certificates of others (subscribers), UCA, PCA and RCA for verifying the integrity and non-repudiation of the received signature message, or those using the certificate message of others (recipients) and sending it to the recipients after encryption to ensure the message confidentiality of both parties.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Applicability of Certificate

1.4.1.1 Certificate personal identification level of security

When a user registers to the TWCA certification service system, the following classes of security and levels of assurance are assigned to the user according to the manner of personal identification.

Level of Assurance	Assurance Meaning
Class 1	The UCA and RA only guarantee the uniqueness of the subscriber's identity information within the company's database. All other subscriber-related information is considered unverified.
Class 2	The UCA and RA guarantee the uniqueness of the subscriber's identity information within the company's database. Other subscriber-related information is provided based on verification procedures, but no guarantee of absolute accuracy is made.
Class 3	In addition to ensuring the uniqueness of the subscriber's identity information within the company's database, the UCA and RA apply rigorous, multi-layered operational procedures to provide a level of identity assurance comparable to in-person verification.
Test Certificate	The UCA and RA make no warranties of any kind. These certificates are issued exclusively for authorized test users of the Subscriber Certificate Authority and are intended for testing purposes only. They shall not be used for any application or business purpose beyond testing.

1.4.1.2 Liability

The scope of use, limit on transaction amount and limit of indemnity of TWCA certificates are tabulated in Table 1. The level of assurance and scope of use of certificates are described below. The code of class of TWCA certificates consists of 4 parts classified and coded according to the following principles:

☆ Format of the class code:
[Part 1]・[Part 2]・[Part 3]・[Part 4]
Ex. 3.1.2.1 represents [Class 3 Identity authentication]. [Single usage]. [Held by natural person]. [For use in financial transactions].

Part 1 [Level of Assurance]	Part 2 [Usage]	Part 3 [User status]	Part 4 [Business Category]
1. Class 1 2. Class 2 3. Class 3 4. Test Certificate	1. Single usage 2. Multi-usage in limited category	1. Juristic person 2. Natural person 3. Others	1. Financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting,

			application of issuance and transaction of short-term bills and securities, application of e-government, and personal identification service 2. Securities transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, application of e-government, and personal identification service 3. e-commerce applications, online tax declaration, e-invoice, e-voting, online patent/trademark application, e-mail application, application of e-government, and personal identification service.

1. Part 1: Personal Identification Level of Security:

   It falls into 3 classes: (1) Class 1, (2) Class 2, (3) Class 3, and (0) Testing Certificates.The security level of certificates is classified by the method of personal identification in user registration. Please refer to Section 1.4.1.1 for details.

2. Part 2: Usage:

   It falls into (1) single usage, and (2) Multi-usage within a limited category (e.g. within a financial holdings business) as described below:

   (1) Single usage: It refers to a specific usage or specific transaction target of certificates, such as property declaration, online ordering or network banking. Also, the specific usage or specific transaction target of certificates is specified in the TerseStatement column of the certificate issuer in the Certificate Policy (CP) of the certificate.

   (2) Multi-usage in limited category: If the usage codes are specified in the TerseStatement column of the certificate issuer in the CP of the certificate, the class shall be limited to the usage represented by these codes. If no code is specified in the TerseStatement column, the usage shall be subject to the contract signed by TWCA or the publishing of TWCA website. The followings FXML, EC, MARKET are the code of limited usage, which will be recorded in the TerseStatement column of the certificate issuer in the CP of the certificate:

- FXML: For certificate holders to transact with TWCA-approved RAs. However, certificate holders shall register to counterpart of transactions in advance. Banks are the original RAs of FXML certificates.
- EC: For certificate holders to transact with TWCA-approved RAs. However, certificate holders shall register to counterpart of transactions in advance, and the transaction shall be limited to online e-commerce transaction.
- MARKET: For certificate holders to transact within the transaction platforms provided by TWCA-approved RAs. However, certificate holders shall register to the corresponding RA in advance.

3. Part 3: User Identity:

It falls into (1) juristic person, and (2) natural person.

4. Part 4: Business Category:

Category:

(1) E-banking transactions, e-financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, online patent/trademark applications, and application of issuance and transaction of short-term bill, application of e-government, and personal identification service.

(2) On-line order securities & futures transactions, e-financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, online patent/trademark applications, and application of issuance and transaction of short-term bill, application of e-government, and personal identification service.

(3) e-financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, online patent/trademark applications, and application of issuance and transaction of short-term bill, application of e-government, and personal identification service.All.

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

Class 3 Assurance Level (3)・Single Usage (1)・Institutional User (1)・For use in financial transactions (1).

✪ Transaction amount limit, indemnity limit and scope of use of individual certificates:

(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 user status of certificates. This limit refers to the maximum amount of liability for a single certificate of users. 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 user 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 user shall be subject to the contract terms.

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

*The applicability and liability of certificates are tabulated below:

Table 1 (expressed in NT$)

Class	Level of Assurance	Usage	Subscriber Status	Transaction Amount Limit	Indemnity Amount Limit
1.1.1.3	Class 1	Single Usage	Juristic person	3,000	3,000
1.1.2.3	Class 1	Single Usage	Natural person	3,000	3,000
2.1.1.1 2.1.1.2 2.1.1.3	Class 2	Single Usage	Juristic person	900,000	300,000
2.1.2.1 2.1.2.2 2.1.2.3	Class 2	Single Usage	Natural person	300,000	100,000
2.2.1.1 2.2.1.2 2.2.1.3	Class 2	Multi-usage in limited category	Juristic person	900,000	300,000
2.2.2.1 2.2.2.2 2.2.2.3	Class 2	Multi-usage in limited category	Natural person	300,000	100,000
3.1.1.1 3.1.1.2 3.1.1.3 3.1.1.4	Class 3	Single Usage	Juristic person	Unspecified	2,000,000 2,000,000 2,000,000 2,000,000

3.1.2.1 3.1.2.2 3.1.2.3 3.1.2.4	Class 3	Single Usage	Natural person	Unspecified	300,000 300,000 300,000 300,000
3.2.1.1 3.2.1.2 3.2.1.3 3.2.1.4	Class 3	Multi-usage in limited category	Juristic person	Unspecified	2,000,000 2,000,000 2,000,000 2,000,000
3.2.2.1 3.2.2.2 3.2.2.3 3.2.2.4	Class 3	Multi-usage in limited category	Natural person	Unspecified	300,000 300,000 300,000 300,000

Note: If the class specified in the certificate does not appear in the above table, this certificate shall not be used in any applications or businesses other than testing. Most importantly, TWCA assumes no liability resulted from the use of such certificate.

1.4.1.3 Applicability and Restrictions of Certificate

1. When the class code of TWCA is not specified in the “TerseStatement column of the certificate issuer in the CP of the certificate”:

   As the original CA system of TWCA is unable to add remarks in the “TerseStatement column of the certificate issuer in the CP of the certificate”, TWCA thus makes additional descriptions below. Certificates that are not defined below cannot be used in any applications or businesses other than testing, and TWCA assumes no liability resulted from the use of such certificate.

   <1> Business EC Certificate System (EC+)

   Certificates issued by TWCA with “CN=TaiCA Secure CA, OU=Certification Service Provider, O=TAIWAN-CA.COM Inc., C=TW” specified in issuer DN (Issuer Distinguished Name) column are EC certificates. EC certificates issued by TWCA with the “Company Uniformed Tax Code” specified in the CN column under the issuer DN column are held by juristic persons; e.g. “CN=TW1674277416742774”. EC certificates issued by TWCA with the “Citizen Identity Card Number” specified in the CN column under the issuer DN column are held by natural persons; e.g. “CN=TWH14520147801”.

   - EC certificates issued by TWCA with the “Bank English Name” specified in the OU column under the issuer DN column; e.g. “OU=Cathay United Bank”, the scope of use and liability of these certificates are “Class 3.1.1.1, or Class 3.1.2.1, or 3.2.1.1, or 3.2.2.1”.
   - EC certificates issued by TWCA with the “Securities Company English Name”

specified in the OU column under the issuer DN column; e.g. "OU=DASHIN SECURITIES CO. LTD.", the scope of use and liability of these certificates are "Class 3.1.1.2, or Class 3.1.2.2, or 3.2.1.2, or 3.2.2.2".

- EC certificates issued by TWCA with the "e-Commerce Unit English Name and which is not the English name of neither a Bank or Securities Company" specified in the "OU" column under the issuer DN column; e.g. "OU=TAIWAN-CA.COM Inc. (FORMOSA RA)", the scope of use and liability of these certificates are "Class 3.1.1.3", "3.1.2.3", "3.2.1.3" or "3.2.2.3".

<2> C-XML Certificate System

- Certificates issued by TWCA with "CN=TaiCA Information User CA, OU=User CA, O=TaiCA, C=TW" specified in the issuer DN (Issuer Distinguished Name) column are C-XML certificates.

  C-XML certificates issued by TWCA with the "Company Uniformed Tax Code" specified in the CN column under the issuer DN column are held by juristic persons; e.g. "CN=16742774-16-A742774". C-XML certificates issued by TWCA with the "Citizen Identity Card Number" specified in the CN column under the issuer DN column are held by natural persons; e.g. "CN=H145201478-01-001". The scope of use and liability of these certificates are "Class 3.2.1.3, or Class 3.2.2.3, or Class 3.2.1.1, or Class 3.2.2.1".

- Certificates issued by TWCA with "CN=TaiCA Finance User CA, OU=User CA, O=TaiCA, C=TW" specified in the issuer DN (Issuer Distinguished Name) column are tariff-and-charge-free certificates.

  Tariff-and-charge-free certificates issued by TWCA with the "Company Uniformed Tax Code" specified in the CN column under the issuer DN column are held by juristic persons; e.g. "CN=16742774-16-A742774". Tariff-and-charge-free certificates issued by TWCA with the "Citizen Identity Card Number" specified in the CN column under the issuer DN column are held by natural persons; e.g. "CN=H145201478-01-001". The scope of use and liability of these certificates are "Class 3.1.1.1, or Class 3.1.2.1, or Class 3.2.1.1, or Class3.2.2.1".

- Certificates issued by TWCA with "CN=TWCA SMIME User CA, OU=User CA, O=TAIWAN-CA Inc., C=TW" specified in the issuer DN (Issuer Distinguished Name) column are S/MIME (Secure/Multipurpose Internet Mail Extensions) certificates.

The scope of use and liability of S/MIME certificates issued by TWCA with the "Usage + Last 4 Numbers of Code + Serial Number" specified in the CN column under the applicant DN column, e.g. "CN=SMIME5678-00-000001", are "Class 2.1.1.3, or Class 2.1.2.3, or Class 2.1.3.3".

2. When the class code of TWCA is specified in the "TerseStatement column of the certificate issuer in the CP of the certificate":

<1> Certificate's applicability: Please refer to Section1.4.

<2> Limits on applicability of certificate: Both the subscribers and parties relying on the certificates shall use the certificates within the scope of businesses indicated by the class code specified in the certificates. They shall also follow the restrictions on the usage and transaction counterparts, and the corresponding transaction amount limit specified in Table 1.

<3> In a transaction, both the subscribers and relying parties of users shall verify the information in specified in the TerseStatement column of the certificate issuer in the CP of the certificate to ensure that the transaction is within the scope of use of the certificate prior to continuing with and completing the transaction.

<4> Vendors supplying system hardware and software for electronic signature and its verification and security controls of decryption shall indicate the scope of use of certificates in the conspicuous places for users to verify. They may also check the certificates with computer programs to ensure that the certificates are within their scope of intended use.

Examples of issuer's TerseStatement:

(Please refer to Table 1, Section 1.4.1.2 for details of the transaction amount limits and indemnity amount limits of certificates.)

- Restriction = 3.1.1.1,Financial,only for the authorized relying party :refer to the 1st OU of this certificate's Subject DN.

  (DN is Distinguished Name for short. OU is Organization Unit Name for short.) The above example is a Class 3 and single usage certificate. The party relying on the certificate is restricted to the first authorized party relying on the certificate described in the first organization unit name (OU) under the Subject DN. The holder of this certificate is an enterprise user (juristic person). The certificate is for use in financial transactions.

- Restriction = 3.1.2.2,Securities,only for the authorized relying party :refer to the 1st OU of this certificate's Subject DN.

  The above example is a Class 3 and single usage certificate. The party relying on the certificate is restricted to the first authorized party relying on the certificate described in the first organization unit name (OU) under the Subject DN. The holder of this certificate is an individual user (natural person). The certificate is for use in securities transactions.

- Restriction = 3.2.1.1,Financial,FXML.

  The above example is a Class 3 and multi-usage in limited category certificate for use in the transactions between the holder and the authorized RAs. However, the holder shall first register to the transaction counterpart. The holder is an enterprise user (juristic person). The certificate is for use in financial transactions.

- (D)Restriction = 1.1.1.3,Non-financial and non-securities, only for the authorized relying party: refer to the 2nd OU of this certificate's Subject DN.

  The above example is a Class 1 and single usage certificate. The party relying on the certificate is restricted to the second authorized party relying on the certificate described in the first organization unit name (OU) under the Subject DN. The holder of this certificate is an enterprise user (juristic person). The certificate is for use in e-commerce applications.

- Restriction = 3.2.2.2,Securities,EC

  The above example is a Class 3 and multi-usage in limited category certificate for use in the transactions between the holder and the authorized RAs. However, The certificate holder shall first register or enroll with the transaction counterparty before using the certificate.. The holder is a natural person user. The certificate is for use in securities transactions.

- Restriction = 1.1.2.3, Non-financial and non-securities, only for the authorized relying party: refer to the 2nd OU of this certificate's Subject DN.

  The above example is a Class 1 and single usage certificate. The party relying on the certificate is restricted to the second authorized party relying on the certificate described in the first organization unit name (OU) under the Subject DN. However, the holder shall first register with the transaction counterpart. The holder of this certificate is a natural person user. The certificate is for use in e-commerce applications.

- Restriction = 1.1.3.3, Non-financial and non-securities, only for the authorized relying party: refer to the 2nd OU of this certificate's Subject DN.

  The above example is a Class 1 and single usage certificate. The party relying on the certificate is restricted to the second authorized party relying on the certificate described in the second organization unit name (OU) under the Subject DN. However, the holder shall first register to the transaction counterpart. The holder of this certificate is a user other than a juristic person or natural person user. The certificate is for use in e-commerce applications.

1.4.2 Prohibited Certificate Uses

Certificates issued by TWCA cannot be used in applications and businesses that may cause physical or mental injuries to or death of human beings or severe damage to social order and public interest; except for the intended uses specified in Section 1.4.1 herein. These certificates also cannot be used in applications and businesses 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 Policy Management Authority (PMA) of TWCA shall be the unit responsible for the establishment, amendment and publishing of the CPS.

1.5.2 Contact Person

Users recommending any revision of the CPS shall email or mail their recommendations in detail, supporting documents and contact information to the contact window below.

Users can contact the following TWCA window for certificate registration, certificate application, certificate renewal, certificate access, reporting a lost key or doubts of security.

Company name	TAIWAN-CA INC. (TWCA)
Contact unit	Customer Service Center
Address	(100) 10TH Floor,85,Yen-Ping South Road, Taipei, Taiwan, R.O.C
TEL	886-2-23708886
Fax	886-2-23700728
E-mail	ca@twca.com.tw
URL	https:// www.twca.com.tw

1.5.3 Person Determining CPS Suitability for the Policy

The PMA shall be the unit responsible for the amendment and establishment of this CPS.

1.5.4 CPS Approval Procedures

This CPS is established by the Certification Authority, and passed upon review of the PMA.

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.

1.6 Definitions and Acronyms

Defined in Appendix 1 and Appendix 2.

2. Publication and Repository

2.1 Repositories

This CA is responsible for managing and maintaining the repository, and for publishing and disclosing the Certificate Policy (CP), Certification Practice Statement (CPS), certificate-related information, and audit reports within the repository.

This CA ensures that the repository is accessible 24/7. The repository URL is: https://www.twca.com.tw/repository

2.2 Publication of Certification Information

The information published in CA includes but is not limited to the following:

- CP;
- CPS;
- CA certificate;
- CA certificate related information, including certificate attribute values and the download link for the Certificate Revocation List (CRL);
- Audit reports.

2.3 Frequency of Publication

The revised CP, once finalized and approved by PMA, will be published in this repository within 7 working days.

This CPS, once finalized and approved by PMA, will be submitted to the regulatory authority for approval. This company will publish it in the repository within 7 working days after receiving the official approval document.

Once a certificate of this CA is signed, its certificate chain and related certificate information will be published in this repository within 7 working days for users or relying parties to access and use. The issuance frequency of the CRL follows the provisions outlined in Section 4.9.7.

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

2.4 Access Controls on Repositories

The repository of this CA is available in a read-only format for users or relying parties to access and query publicly. However, to prevent malicious attacks or tampering, access control shall be implemented when updating repository information or during abnormal traffic conditions.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

When generating or processing the <SubjectName> (e.g. citizen ID card number, company tax code or the interbank e-banking account number of FISC) and expanding the <SubjectAltName> (e.g. banking account number, company Chinese name or personal Chinese name) for users of the X.509 V3 (ISO 9594-8) certificates using the X.501 (ISO 9594-2) Distinguished Name (DN) naming method, the CA shall follow the formats below:

1. Business EC Certificate System (EC+)

<1> Business EC Certificate

Distinguished Name (DN)	Description	Necessity	Example of DN contents
1.Country(C)	Country code of certificate issuing place	Mandatory	C = TW
2.Organization(O)	The Certification Authority's Common Name(CN) or the Certificate Applicant's Organizational Information(1)	Optional	O = TaiCA Secure CA
3.Organization(O)	The Certification Authority's Policy Qualifier Name or the Certificate Applicant's Organizational Information(2)	Optional	O = Certificate Service Provider
4.OrganizationUnit(OU)	The Registration Authority's English Distinguished Name or the Certificate Applicant's Organizational Unit Information(1)	Optional	OU = President Securities Corp.
5.OrganizationUnit(OU)	The Registration Authority's Branch Office or Service Classification, or the Certificate Applicant's Organizational Unit Information(2)	Optional	OU = PSCNET

6.CommonName(CN)	The certificate applicant's distinguished name, or other identifiable name or verified information, such as the subscriber's National Identification Number	Mandatory	CN = TWA123456789-00
7.Email(E)	The certificate applicant's email address	Optional	E= user@sec.com

2. Commercial XML Certificate System

<1> Tariff and fees certificate

Distinguished Name (DN)	Description	Necessity	Example of DN contents
1.Country(C)	Country code of certificate issuing place	Mandatory	C = TW
2.Organization(O)	Information on the Certificate Authority's Policy or the Certificate Applicant's Organizational Information	Optional	O = Finance
3.OrganizationUnit(OU)	Information of the Certificate Authority (issuing entity) or the Certificate Applicant's Organizational Unit Information(1)	Optional	OU = TaiCA Finance User CA
4.OrganizationUnit(OU)	The Registration Authority's English Distinguished Name or the Certificate Applicant's Organizational Unit Information(2)	Optional	OU = 12345678-RA-FINANCE
5.OrganizationUnit(OU)	The Registration Authority's Application or Service Identifier, or the Certificate Applicant's Organizational Unit Information(3)	Optional	OU = TAX
6.CommonName(CN)	The certificate applicant's distinguished name or other identifiable or verified information, such as the business registration number	Mandatory	CN = 12345678-01-000

<2> Commercial XML Certificate

Distinguished Name (DN)	Description	Necessity	Example of DN contents
1.Country(C)	Country code of certificate issuing place	Mandatory	C = TW
2.Organization(O)	Information on the Certificate Authority's Policy or the Certificate Applicant's Organizational Information	Optional	O = Information
3.OrganizationUnit(OU)	Information of the Certificate Authority (issuing entity) or the Certificate Applicant's Organizational Unit Information(1)	Optional	OU = TaiCA Information User CA
4.OrganizationUnit(OU)	The Registration Authority's English Distinguished Name or the Certificate Applicant's Organizational Unit Information(2)	Optional	OU = 12345678-RA-Trade
5.OrganizationUnit(OU)	The Registration Authority's Application or Service Identifier, or the Certificate Applicant's Organizational Unit Information(3)	Optional	OU = Trade
6.CommonName(CN)	The certificate applicant's distinguished name or other identifiable or verified information, such as the business registration number	Mandatory	CN = 12345678-01-000

3.1.2 Need for Names to be Meaningful

The subject distinguished name recorded in the user's certificate shall comply with relevant laws and regulations concerning naming conventions. It shall be sufficient to identify a specific legal entity or natural person and be recognizable by relying parties.For individuals, the identification name based on the National Identification Number shall be processed in accordance with the standards set by the Ministry of the Interior. For enterprises, the identification name based on the Business Registration Number shall be handled according to the standards established by the competent authority.

If, due to business requirements, the subject distinguished name does not pertain to a

National Identification Number or Business Registration Number, prior consent from the company shall be obtained. Before using the certificate, the user and the relying party shall agree upon the user's identification name and verify its accuracy during certificate validation.

3.1.3 Anonymity and 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

The DNs that are used in certificates shall be identifiable and unique in the certificate system. When there are different subscribers using the same registration name of DN, the subscriber first to register the name shall enjoy the priority to use such name. Subscribers registering the same name afterwards shall add a distinguishing column code or serial number to distinguish from the first user.

When there are different users using the same DN, the UCA/RA shall award the priority use of that DN to the first user registered with that DN. Neither the UCA nor the RA is responsible for resolving the disputes arising from or in connection with DN. Users shall refer the claim to the competent authorities of the corresponding business. For example, when the citizen ID card number DN of two or more users is identical, these users shall make the claim to the Ministry of the Interior.

When the DN of a user is owned by another user as proven by the valid documents issued by the competent authorities, the UCA shall immediately cancel the DN registration of that subscriber who shall also need to take the relevant liability. Also, neither TWCA nor the RA is responsible for verifying the legitimacy of the DN registered by that user.

3.1.6 Recognition, Verification and Role of Trademarks

The UCA and RA respect the registered trademark right of the registering company's Chinese and English names in the DN and accept users to use them as their DN. Nonetheless, this shall not guarantee the recognition, verification and uniqueness of the user's registered trademark. Neither TWCA nor the RA is responsible for resolving disputes concerning such matters. Users shall apply for resolution to the competent authorities of the corresponding business.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The UCA or RA shall verify the correctness, integrity and validity of the subscriber private key with any of the following methods:

- When subscriber signing the certificate application contents with the user private key, the UCA or RA shall verify the correctness, integrity and validity of certificate application contents, the protected subscriber identity information, the public key and private key. Also, the public key shall not be the certificate that is currently in use.
- Apart from verifying the correctness, integrity and validity of the private key with the user signature, the UCA or RA can encrypt a message with the user's public key and deliver the encrypted message to the user by the digital envelope. After verifying the message, the user can sign it with the private key and reply the confirmation message to the UCA or RA to verify if the private key is correct.

3.2.2 Authentication of Organization Identity

Assurance Level	Authentication Method of Organization
Class 1	1. The applicant shall submit identification information (e.g., company registered name and email address). The Registration Authority (RA) shall verify the uniqueness of the identification information and confirm the objective existence of the legal entity (refer to Section 3.1.5). 2. The applicant may submit the aforementioned identification information through digital or written means. 3. Once the relevant information is submitted, it indicates that the applicant confirms and agrees to the provided information. The RA will proceed to verify the accuracy of the user's identity proof accordingly.
Class 2	1. In addition to verifying the Level 1 identification information, the applicant shall submit the legal entity's name, Business Registration Number, or other information sufficient to identify the legal entity. The Registration Authority (RA) shall verify the existence and validity of the legal entity through telephone or other means, such as third-party databases. 2. During the initial identity registration and authentication process, the applicant shall submit one piece of identity information issued by a reliable source, which has been verified by a trusted third party. The RA shall verify this credential in accordance with its validation standards. 3. The applicant may submit the aforementioned identification information through digital or written means. 4. Once the relevant information is submitted, it indicates that the

	applicant confirms and agrees to the provided information. The RA will proceed to verify the accuracy of the user's identity proof accordingly. 5. A certificate of this assurance level, when used for digital signature purposes, is presumed to have been signed by the user.
Class 3	In-Person Processing: In addition to verifying Level 2 identification information, legal entities or corporate users shall have their authorized representatives personally handle the application. The representative shall provide authorization documents and identification sufficient to verify the applicant's identity (e.g., a photo-identifiable ID card or passport). Non-In-Person Processing: In addition to verifying Level 2 identification information, one of the following methods shall be employed for user identity verification. If the certificate is intended for use in the financial industry, the process shall also comply with the security regulations set by financial supervisory authorities for non-face-to-face account openings: ● Engaging the user's affiliated financial institution to confirm the user's identity. ● Submitting original certification documents from professionals such as lawyers or accountants, with confirmation via correspondence. ● Conducting account opening through mail and video conferencing, followed by an on-site visit for confirmation. The procedures for this process shall be established within each Registration Authority's internal control system. ● Utilizing other non-face-to-face identity verification mechanisms recognized by the competent authority for certificate relying parties (e.g., standard procedures for banks accepting customers to open digital deposit accounts online). For certificates of this assurance level, when used for digital signatures, they are presumed to have the legal effect of being executed by the certificate holder.
Test Certificate	The UCA and the RA do not perform any user identity verification procedures. The certificates issued are intended solely for testing purposes and shall not be used for any applications or business activities beyond testing.
Note 1: The identity information used during the initial registration and authentication process shall be credentials that comply with a high assurance level as defined by ISO/IEC 29115.	

Note 2: To meet the requirements of Assurance Level 2 for the initial registration and authentication process, mechanisms such as business certificate verification, corporate bank account verification, and company registration amendment application review can be employed.

3.2.3 Authentication of Individual Identity

Assurance Level	Authentication Method of Individuals
Class 1	1. The applicant submits identification information for the application, and the Registration Authority verifies the uniqueness of the identification information and confirms the objective existence of the identity. (Refer to Section 3.1.5). 2. The applicant may submit the aforementioned identification information either digitally or in written form. 3. Once the relevant information is submitted, it signifies that the applicant acknowledges and agrees to the provided information, and the Registration Authority will proceed to verify the accuracy of the user's identity proof accordingly.
Class 2	1. In addition to verifying Level 1 related information, the applicant shall submit the legal entity's name, Uniform Business Number (UBN), or other information sufficient to identify the legal entity. The Registration Authority will verify the existence and validity of the legal entity through telephone or other means (such as third-party databases). 2. For the initial registration identity proofing and authentication process, the applicant shall submit one piece of identity information issued by a reliable source (see Note 1), which will be verified by a trusted third party. The Registration Authority will conduct verification in accordance with the authentication specifications of the credential (see Note 2). 3. The applicant may submit the aforementioned identification information either digitally or in written form. 4. Once the relevant information is submitted, it signifies that the applicant acknowledges and agrees to the provided information, and the Registration Authority will proceed to verify the accuracy of the user's identity proof accordingly. 5. Certificates of this assurance level, when used for digital signatures, are presumed to be executed by the user themselves.
Class 3	In-Person Processing: In addition to verifying Level 2 related information, legal entities or corporate users should have their authorized representatives personally handle the application, providing identification documents sufficient to identify the applicant (e.g., photo-identifiable ID cards, passports, etc.).

	Non-In-Person Processing: In addition to verifying Level 2 related information, the following methods (choose one) should be used for user identity verification; if the certificate applied for is intended for use in the financial industry, it should also comply with the security regulations for non-face-to-face account opening identity verification set by financial supervisory authorities: ● Have the user's affiliated financial institution confirm the user's identity. ● The user provides original certification documents from professionals such as lawyers or accountants, confirmed through correspondence. ● Open an account via communication and video methods, with subsequent verification; the operational procedures are established within the internal control systems of each registration authority. ● Other non-face-to-face account opening identity verification mechanisms recognized by the competent authorities of certificate relying parties (e.g., banks accepting customers to open digital deposit accounts online). For certificates of this assurance level, when used for digital signatures, they are presumed to have the legal effect of being executed by the certificate holder.
Test Certificate	The UCA and the RA do not perform any user identity verification procedures; the certificates issued are intended solely for testing purposes and shall not be used for any applications or business activities beyond testing.
Note1: The identity information used in the initial registration identity proofing and authentication process shall be credentials that meet or exceed the high assurance level as defined by ISO/IEC 29115. Note2: The initial registration identity proofing and authentication process shall satisfy the requirements of Assurance Level 2, such as mechanisms including deposit account verification, verification of original phone numbers retained by financial institutions, and telecom number authentication supplemented by verification of identity data authenticity by other authoritative entities.	

3.2.4 Non-verified Subscriber Information

The user information recorded in the certificates issued by this Certificate Authority shall be verified.

3.2.5 Validation of Authority

The identity documents of natural persons, corporate representatives, corporate agents, and corporations shall be official documents issued by governmental authorities or credentials recognized by this Certification Authority (CA) as adequately representing the original applicant (e.g., business certificates). The Registration Authority (RA) shall verify the authenticity of the authorization documents of corporate agents. If necessary, the RA shall contact the original applicant to confirm that the agent is authorized to apply for the certificate.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication of Rekey Requests

3.3.1 Identification and Authentication for Routine Rekey

When the validity of a subscriber key (certificate) is set to one year, this key shall be renewed in one year; i.e. the validity of the subscriber certificate is one year. Within the certificate renewal period (e.g. one month to expiration), the user shall re-generate a public and private key pair and apply to the UCA or RA to issue a new certificate. This process is known as the “rekey” of certificate and private key.

The maximum validity of the user certificate (the validity of private key is the same as that of the certificate) is 3 years.

If a user performs a certificate and private key renewal before the certificate's expiration date, they shall use their currently valid private key to digitally sign the newly generated public key. The resulting Certificate Signing Request (CSR) in PKCS#10 format should then be submitted to the Registration Authority (RA) to request the issuance of a new certificate. The Certificate Authority (CA) or RA will verify the correctness, integrity, and validity of the signature information before proceeding with the certificate issuance process.

When running the rekey of the certificate and private key after the expiration of the certificate, subscribers shall apply to the RA for certificate renewal over the counter, by mail or other methods that can effectively verify their identity. After obtaining the personal identification data for certificate renewal from the RA, subscriber shall use the certificate application message and user’s personal identification data containing the new private key signature to apply for the issue of a new certificate to the UCA or RA according to the regulations of the RA. After receiving the certificate application message of subscribers, apart from verifying the legitimacy of private key possession, the RA shall verify the legitimacy and integrity the user certificate application message.

3.3.2 Rekey after Certification Revocation

After revoking a certificate, subscribers shall not apply to the UCA/RA for re-issuing the certificate. Instead, users shall run the procedure again. That is, users shall run the personal identification for registration. After obtaining the personal identification data for a certificate renewal from the RA, subscribers may re-generate the new public key pair and sign the certificate application message and subscriber's personal identification data with the new private key to apply to the UCA/RA for issuing a new certificate according to the RA regulations. After receiving the application information from the user, the RA shall verify the legitimacy of the private key and the legitimacy and integrity of the subscriber’s certificate application message.

3.4 Certificate Revocation Request

When a user submits a certificate revocation request, it shall be made in digital or written form. The UCA or RA shall verify the user's identity and authenticate the request data, ensuring compliance with the identity verification requirements outlined in Sections 3.2.2 or 3.2.3. If necessary, the original certificate applicant should be contacted to confirm the specific facts leading to the revocation request. If the request is made through an agent, it shall meet the conditions specified in Section 3.2.5. Detailed revocation procedures should be conducted in accordance with the provisions of Section 4.9.

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.

The individual (Natural person) applying for the certificate shall be either the applicant themselves or their authorized representative.

4.1.2 Enrollment Process and Responsibilities

Subscribers shall apply to the RA for issuing a certificate according to the security control requirements of the business application system. Subscribers shall complete the application for registration to the RA prior to applying for a certificate.

- The RA shall explain in detail to users the use of certificates in the business application systems, the rights and obligations specified in the application form and contract, and the operating procedures of the relevant businesses and provide subscribers with the relevant instructions and subscriber's manual. Customers shall agree to these and confirm the receipt of such documents.
- Subscribers shall complete correct and detailed information in the relevant application forms and provide the relevant supporting documents. The RA shall perform the user's personal identification according to the relevant level of assurance. After verifying the subscriber identity and certificates, the RA shall provide the subscriber his/her identity code and PIN to complete the subscriber registration process.
- The RA shall register to the UCA and apply for a RA certificate according to the UCA operating and management procedures. This certificate shall be used for the secure receiving and delivery of the subscriber certificate between the RA and the UCA.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

1. Application for Business EC Certificate System (EC+)

   - After completing the RA registration procedure, obtaining the user's personal identification data from the RA, generating the public key pair and the certificate application message according to the code of operations, subscribers shall sign the certificate application message with the private key and deliver it to the RA to apply for the issue of certificates.

- After checking the correctness, integrity and validity of the certificate application message, the RA shall sign the certificate application message with the RA private key, if there is no error, and encrypt the message with the server prior to delivering it to the UCA.
- After checking the subscriber certificate application message delivered from the RA, and the correctness, integrity and validity of message of the RA and subscriber identity, the UCA shall issue the certificate and deliver it to the RA if there is no error.
- The RA shall check the correctness, integrity and validity of the user certificate delivered by the UCA. If there is no error, the RA shall send the certificate to the applicant.

2. Commercial XML Certificate application

- The applications for the commercial XML certificate applications for all levels of assurance shall be processed in the following manners.
- After completing the identity verification and PIN verification procedures, subscribers may register to the RA and sign the certificate application message generated with their private key before delivering the message to the RA.
- After verifying the subscriber personal identification code and PIN and the correctness, integrity and validity of subscriber certificate application message, the RA shall sign the subscriber certificate application message with the RA private key if there is no error. After encrypting the message with the server, the RA shall deliver the subscriber certificate application message to the UCA.
- After checking the subscriber certificate application message delivered from the RA, the legitimacy of the RA and user identity, and the correctness, integrity and validity of message, the UCA shall issue the certificate and deliver it to the RA if there is no error.
- The RA shall check the correctness, integrity and validity of user certificate delivered by the UCA. If there is no error, the RA shall send the certificate to the applicant.

In consideration of security control, the RA or the UCA may deliver to the user the interface software for certificate application and private key generation by a reliable and secure method, and the security of such interface software shall be assessed and verified appropriately by the RA or UCA.

4.2.2 Approval and Rejection of Certificate Applications

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

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 Certificate Issuance by the CA

Please refer to Section 4.2, for details of application for certificates.

After generating the subscriber certificate, apart from delivering it to the applicant, the UCA shall immediately update the certificate information in the database or directory server for user access.

4.3.2 Notification of Certificate Issuance by the CA to Subscribers

Upon completion of issuance of the user certificates, the UCA and RA shall notify the subscribers to download the certificates immediately.

When the subscriber certificate application message is rejected by the UCA, the UCA and the RA shall immediately notify the user of the message failure. Also, the UCA reserves the right to hold the reason(s) of transaction failure; except for reason(s) complying with this CPS, the CP or the relevant laws and regulations of the competent authorities.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

After the certificate is issued and obtained from the UCA, users shall process the certificate as shown below:

- Verify if the subscriber-related information in the certificate is consistent with that in the subscriber registration and is the correct information of the subscriber.
- The public key and the corresponding private key of a certificate shall come in a pair and possessed by the subscriber. Check if the validity in the certificate is valid and correct.

- Subscribers shall verify the certificate chain of that certificate, examine the correctness, integrity and validity of every certificate, and check if the certificate has been revoked, the validity has expired, and the certificate is legally and correctly issued by the UCA.
- When verifying the certificate contents, if the above problems or other problems recognized by the UCA occur, subscribers may request the UCA or RA to re-issue a certificate within 7 days from the issuance.
- When subscribers activate a certificate, this also means that they have also accepted the rights and obligations specified in this CPS, the CP and the contract.

4.4.2 Publication of the Certificate by the CA

Upon completion of the certificate issuance, the subscriber certificates will be published 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 scope of certificate uses shall be subject to the scope of use specified in this CPS and the contract signed between the subscriber and TWCA. When using the certificate, subscribers shall:

- properly retain and store the private key related to the certificate to prevent loss, exposure, alteration or unauthorized use or theft by a third party;
- verify the certificate chain; check every certificate and the correctness, integrity and validity of that certificate (if it is revoked, expired, legally and correctly issued by the UCA, and legally and correctly possessed by the user); check the veracity of the relevant columns in the certificate according the security control regulations of respective businesses; and check if the possessor of this certificate is a legal and correct trader;
- check the correctness, integrity and validity of certificate stored in the business application system in the form of a public key apart from the identity verification of access when using the certificate; and
- understand and accept the rights and obligations concerning the business category, transaction amount limit, liability amount limit of the certificate in the relevant business systems when using the certificate to sign and encrypt the transaction message; and

legally use the certificate within the scope of use specified in the CP, this CPS and the relevant business regulations.

4.5.2 Relying Party Public Key and Certificate Usage

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

- To obtain the self-signed certificate of the RCA issuing the certificate of this CA via proper and secure channels.
- To check if the RCA self-signed certificate, PCA certificate, UCA certificate and subscriber certificate are expired.
- To verify if the digital signatures of the RCA self-signed certificate, PCA certificate and UCA certificate are valid and not revoked.
- To verify the digital signature used in the subscriber certificate with the public key of the UCA certificate.
- To check if the subscriber certificate is not revoked by the UCA.

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

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

No certificate renewal is available.

4.6.2 Who May Request Renewal Certificate

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of Renewal Certificate Issuance to Subscribers

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 the Renewal Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate and Private Key Renewal

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

4.7.1 Circumstances for Certificate Key Renewal

Subscribers may rekey a certificate prior to its expiration. When the certificate has expired, subscribers shall apply to the RA for certificate renewal over the counter, by mail or other methods that can verify their identity.

4.7.2 Who May Request Renewal Certificate Key

Subscribers may renewal the certificate key.

4.7.3 Certificate Key Renewal Procedure

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

4.7.4 Notification of Renewal Certificate Key Issuance to Subscribers

Subject to Section 4.3.2.

4.7.5 Acceptance Procedure of Renewal Certificate Key

Subject to 4.4.

4.7.6 Publication of the Renewal Certificate Key by the CA

Subject to Section 4.4.2.

4.7.7 Notification of Renewal Certificate Key Issuance by the CA to Other Entities

Subject to Section 4.4.3.

4.8 Certificate Modification

Certificate modification refers to the issuance of a certificate 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 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 Certificate Modification Procedure

Not applicable.

4.8.4 Notification of the Modified Certificate Issuance to Subscribers

Not applicable.

4.8.5 Acceptance Procedure of the Key Certificate Modification

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of the Modified Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation

A subscriber may revoke a certificate during its validity under any of the following circumstances:

1. Certificates revoked by users:
   - 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. Certificates revoked by TWCA 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.
   - A certificate shall be revoked when the RA (UCA) announces that its subscriber has failed to perform its obligations specified in the contract or code of operations, such as paying the relevant fees, or the subscriber illegally uses the certificate and he/she breaks the law, the relevant regulations or the scope of certificate uses.
   - A certificate shall be revoked when the subscriber information in the certificate does not comply with the CP, this CPS or the scope of certificate uses; such as discrepancies between the certificate contents and registration data or discrepancies out of negligence in registration data input.
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.

4.9.2 Who May Request Certificate Revocation

The RA related to the subscribers, TWCA, competent authorities, an authorized third party or subscribers can revoke a certificate.

1. Certificates revoked by subscribers:

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

2. Certificates revoked by RA (TWCA):

   - When applying for revoking a certificate, RA (TWCA) shall follow Section 4.9.3, and contract signed with the user and the relevant codes of operations.

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 shall verify the death status and the identity of the legal successor according to the relevant SOPs.
   - Applications submitted by the RA in accordance with formal and lawful procedures, arising from court litigation or arbitration.
   - A certificate is revoked when the competent authorities apply to revoke a certificate according to the relevant operating procedures.

4.9.3 Procedure for Certificate Revocation

1. Business EC Certificate (EC+) Revocation

   - After a subscriber registers with the RA according to the RA or TWCA security controls (PIN, protection password, etc.) or completes the revocation application form to apply for certificate revocation, the RA shall identify the user's identity and run the certificate revocation process when there is no error. The RA shall encrypt the user's certificate revocation request message with its private key before delivering it to the UCA to apply for revoking the certificate.
   - After receiving the certificate revocation request message from RA, UCA shall check the legitimacy and integrity of the status of RA and user and the message. When there is no error, UCA shall revoke the certificate according to the relevant codes of operations and send the certificate revocation reply message to RA.
   - After receiving the certificate revocation reply message from URA, RA shall check the legitimacy and integrity of the reply message and deliver it to the applicant when there is no error.

2. Commercial XML Certificate Revocation

- After a subscriber registers to RA according to the RA or UCA security controls (PIN, protection password, etc.) or completes the revocation application form to apply for certificate revocation, RA shall identify the subscriber’s identity and run the certificate revocation process when there is no error. RA shall sign the subscriber’s certificate revocation request message with its private key before delivering to UCA to apply for revoking the certificate.
- After receiving the certificate revocation request message from RA, UCA shall check the legitimacy and integrity of the status of RA and user and the message. When there is no error, UCA shall revoke the certificate according to the relevant codes of operations and send the certificate revocation reply message to RA.
- After receiving the certificate revocation reply message from UCA, RA shall check the legitimacy and integrity of the reply message and deliver it to the applicant when there is no error.

Competent authorities, courts, arbitration institutions, and other authorized entities shall also follow the operational regulations of the RA and complete the certificate revocation application form to request the revocation of the certificate from the RA.

When a CA terminates its operations for whatever reasons, it shall revoke its subscriber certificate according to the code of operations prescribed in the Electronic Signatures Act announced by the competent authorities and the terms and conditions specified in the contract signed with RA.

During the validity of a certificate, when subscribers have doubts about certificate security or do not wish to use the certificate anymore, apart from applying for revoking the certificate to RA (or UCA), they shall immediately inform the relevant business subscribers to suspend that certificate. Also, neither TWCA nor RA assumes any liability for the disputes arising out of or in connection with the use of that certificate during the grade period, i.e. the period the application for revocation to the validation of revocation; except for business negligence attributed to UCA or RA.

4.9.4 Revocation Request Grace Period

Subscribers requesting the revocation of certificates shall apply to RA (UCA) immediately. When there is an alleged or proven compromise or security concerns of the certificate key, subscribers should make a revocation request within 24 hours.

4.9.5 Time Within Which CA Shall Process the Revocation Request

After receiving the request message of certificate revocation from the user, RA (or UCA) shall finish processing of the request within 24 hours, provided that the request should be processed immediately if it is received during the business or office hours.

According to the code of certificate system operations of UCA, UCA shall generate the CRL for business EC certificates and C-XML certificates within 24 hours. Therefore, the grace period for the request of certificate revocation for business EC certificates and C-XML certificates shall be 24 hours.

4.9.6 Revocation Checking Requirements for Relying Parties

When using a certificate on a business application system, either the subscriber or the relying party shall verify the validity of the certificate and also check whether the certificate is a revoked certificate. In consideration of business risk factors, the relevant business application systems may voluntarily request or enquire about the CRL status from UCA at planned intervals according to the security level.

4.9.7 CRL Issuance Frequency

Given that the CRL should be issued within 24 hours, the frequency of issuance of CRL is 24 hours.

4.9.8 Maximum Latency for CRLs

Not specified.

4.9.9 Online Certificate Revocation/Status Enquire Service

Online Certificate Status Protocol (OCSP) services are not provided; therefore, users shall verify the certificate status using the Certificate Revocation List (CRL).

4.9.10 Online Revocation/Status Enquire Checking Requirements

Not applicable.

4.9.11 Other Forms of Publishing Revocation

No stipulation.

4.9.12 Special Requirements of Rekey Compromise

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

- To generate a new key pair for the signature and the corresponding new certificate.
- 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).
- To notify subscribers.
- To securely deliver new certificates to subscribers.
- To issue new certificates to subscribers with the new signature key.

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

4.9.13 Circumstances for Certificate Suspension

"Suspension" refers to temporary inactivation. "Suspension revocation" refers to re-activation. The suspension of user certificates shall be processed according to the business requirements and code of operations of UCA and RA. A subscriber may suspend a certificate during its validity under any circumstance of the Suspensions:

1. Subscribers:

    - When there are doubts of private key loss and exposure, users may apply to suspend their certificates 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 or TWCA:

    - A certificate shall be suspended when the RA or TWCA announces that its user has failed to perform its obligations specified in the contract or code of operations, such as paying the relevant fees, or the user illegally uses the certificate that he/she allegedly breaks the law, the relevant regulations, this CPS or the scope of certificate uses.

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.

If the private key is compromised, the procedure of certificate suspension shall not be used. The matter shall be handled in accordance with the provisions of Section 4.9.12.

4.9.14 Who Can Request Certificate Suspension

The RA related to the subscribers, or TWCA, competent authorities, or authorized third party or subscribers can suspend certificates.

1. Subscribers:
   - Subscribers may apply for suspending their certificates as needed according to the RA's code of operations.
2. RA (TWCA):
   - When applying for suspending a certificate, the RA (TWCA) shall follow Section 4.9.13, and the contract signed with the user and the relevant codes of operations.
3. Authorized Third Parties:
   - The authorized person of an organization may request certificate suspension with legal authorization from the organization.
   - Applications submitted by the RA in accordance with formal and lawful procedures due to court litigation or arbitration.
   - A certificate is revoked when the competent authorities apply to revoke a certificate according to the relevant operating procedures.

4.9.15 Procedure for Certificate Suspension

The certificate suspension service of business EC certificates is unavailable from the UCA.

- After a subscriber registers with the RA according to the RA or UCA security controls (PIN, protection password, etc.) or completes a Suspension application form to apply for certificate suspension, the RA shall identify the subscriber's identity and run the certificate suspension process if there is no error. The RA shall sign the user's certificate suspension request message with its private key before delivering it to the UCA to apply for suspending the certificate.
- After receiving the certificate suspension application message from the RA, the UCA shall check the legitimacy and integrity of the status of the RA and user and the message. If there is no error, the UCA shall suspend the certificate according to the relevant codes of operations and send the certificate suspension reply message to the

RA.

- After receiving the certificate suspension reply message from UCA, RA shall check the legitimacy and integrity of the reply message and deliver it to the applicant when there is no error.

From sending of the request of certificate suspension from the user or other authorized parties until the publishing of the suspension notice within 24 hours, users shall immediately stop using the certificate according to the regulations of the business system and notify the relying party to stop using the certificate. When that certificate is used in illegal transactions or when there are lawful disputes arising from or in connection with such transactions, the relying party shall be liable to indemnify the damages that are caused when UCA and RA process the request of certification suspension in compliance with this CPS and the relevant codes of operations. When the user fails to stop using that certificate according to the regulations of the business system and immediately notify the relying party to stop using that certificate during the grace period, they shall be liable for indemnifying the damages caused.

If a subscriber wishes to continue to use that certificate after the suspension is over and the certificate is still valid, he/she may apply to revoke the suspension to the RA. The RA shall identify the subscriber’s identity and run the certificate suspension revocation process if there is no error. The RA shall sign the user’s certificate suspension revocation request message with its private key before delivering to UCA to apply for revoking the suspension in order to re-validate the certificate for further use.

4.9.16 Limits on Certificate Suspension Period

As the certificate suspension service of business EC certificates is unavailable from the UCA, there is no Suspension period available.

After suspending a certificate, if a subscriber does not revoke the suspension prior to the expiration of the certificate, this certificate will be listed in the CRL and become an invalid certificate.

The suspension period of C-XML certificates begins from the listing of a C-XML certificate in the CRL after completing the suspension procedures until the subscriber applies for revoking the suspension. Therefore, the period between the listing the C-XML certificate in the CLR until the revalidation of the C-XML certificate shall mean the suspension period. If the certificate expires before its revalidation, this certificate is considered as an expired certificate and is invalid as a revoked certificate.

The maximum suspension period of certificates shall be the validity of the certificate.

4.10 Certificate Status Service

4.10.1 Operational Characteristics

- Subscribers may verify certificate status via the CRL and OCSP services provided by this Certificate Authority.
- The download location of the Certificate Revocation List (CRL) is specified in the cRLDistributionPoints extension field of the certificate.
- Revocation information for a revoked certificate will be removed from the CRL and OCSP services only after the certificate has expired.

4.10.2 Service Availability

This CA provides 24/7 access to the Certificate Revocation List (CRL) download service. The CRL issuance frequency is specified in Section 4.9.7.

4.10.3 Additional Features

Not specified.

4.11 Termination of Certificate

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 Policy and Practices of Key Escrow and Recovery

The private keys of this CA are not allowed to be escrowed, while the private keys of subscribers are not prohibited from being escrowed.

4.12.2 Encryption 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 CA data center(CADC) is equipped with shock-resistance, water-resistance, fire-resistance, an access control system, anti-invasion access monitoring, and anti-damage alarm system and, therefore, meets the standards for control facilities dedicated to storing highly important and sensitive information to prevent any person from accessing the equipment of the CA without authorization.

5.1.2 Physical Access

Operators' access to the CADC shall be subject to verification with three IC-card-protected entrances. One of the entrances shall be equipped with a biometric device (including but not limited to, fingerprint, face or hand-shape recognition). The CADC shall also be equipped with the physical access control available to identify two persons' identity. A CCTV system with moveable cameras and recording equipment working 24 hours and an IR anti-invasion alarm system shall be equipped at the access to record the access to the data center and prevent any person from accessing the data center without authorization.

The private keys and backup data related to CA operations shall be properly and securely stored in the safety vault protected with CCTV system inside the CA. When operating certificate management, certificate system operators shall be monitored by the CCTV system.

The software and hardware for CA operations and HSM shall be placed in an environment protected with CCTV systems. When operating key management, certification system operators shall be monitored by the CCTV system.

5.1.3 Power and Air Conditioning

The CA shall be equipped with a diesel generator and Uninterruptible Power Supply (UPS). When the general power supply fails, the power supply shall be automatically switched to the diesel generator. The UPS shall maintain power supply stability during the switch.

An independent air-conditioning system shall be furnished to ensure the stability of system operations and provide an optimal work environment. The air-conditioning system shall be maintained and tested at planned intervals.

5.1.4 Water Resistence

The CADC shall be a closed reinforced concrete building to resist rainwater, except for the entrances. The floor shall be elevated to avoid water exposure.

5.1.5 Fire Resistence

The CADC shall be built with fire-resistance materials and equipped with the fire extinguishing equipment with central monitoring system. When a fire is detected, the system shall automatically activate the fire extinguishing function. Manual switches shall be installed at major entrances for onsite personnel to activate the system in case of emergency.

5.1.6 Media Storage

Magnetic media shall be stored in anti-magnetic and antistatic interference equipment and environments. Important data media shall be stored in a vault with high fire resistance. A copy of information media shall be stored in an offsite data center with security controls. Backup and archive information storage media shall be tested and verified for validity and usability at planned intervals.

5.1.7 Waste Disposal

The hardware devices used by the Certificate Management Center in the certificate system shall be destroyed upon decommissioning, and the destruction process shall be verified by the audit unit, with relevant audit records retained.

When documents and media contain commercially sensitive or confidential information, they shall be securely destroyed during the disposal process to ensure that the information is completely irretrievable and inaccessible. The destruction process shall also be verified by the audit unit, and audit documentation shall be retained.

5.1.8 Offsite Backup

The backup copy of media information, documents and specifications related to the operations of the certification system shall be stored in a highly secured offsite backup environment equipped with central air-conditioning, humidity control, antimagnetic and antistatic interference, CCTV monitoring and recording, and controls of access by only authorized personnel.

The backup copy of the daily transaction records of the certification system and the system backup records made every week shall be stored in a highly secured offsite environment. Backup and archive information storage media shall be tested and verified for validity and usability at planned intervals.

5.2 Procedural Control

5.2.1 Trusted Roles

Under the PKI framework, TWCA certificates are issued with the certification system according to a well-laid and secure operating procedure by a trusted and authoritative role played by TWCA and RA in an impartial and rigorous manner.

Duties are assigned to TWCA operators according to competent and trusted personnel with independent responsibility according to the code of operations. These operators shall carry out their duties in a certification system with security controls according to the TWCA code of operations and operation manual for certification and the internal code of operations and operation manual of RAs.

In operating the certification system, in order to distinguish duties from responsibility and authority and ensure that the backup function of duties shall not compromise the overall system security and the integrity of system operations, the trusted operators and their duties of individual businesses are specified below.

5.2.1.1 Certification Authority (CA)

- The CA manager shall manage and supervise the operations of the entire certification system.
- Auditors (TWCA personnel other than CA operators) shall audit and supervise the operation of the TWCA certification system. Please see Section 8.4 for details.
- Supervising personnel of certification system operations shall work in a pair to manage and authorize system operation resources, e.g. operator authorization and implementation, system resource change and adjustment, etc, except businesses related to the issue of certificates.
- Administrators of certification system operations shall work in a pair to set the relevant system parameters and manage the relevant specifications, e.g. CA key and certificate change; except for the issue of user certificates and creation of user data.
- Operators of certification system operations shall create user data, issue certificates, produce reports and implement batch tasks.
- The maintenance personnel of other hardware and software systems, HSM operators, system resource controllers shall carry out the duties assigned to them.

5.2.1.2 Registration Authority (RA)

- The RA supervisor shall manage and supervise user registration.
- Administrators shall work in a pair to set the relevant system parameters and manage the relevant specifications, e.g. RA key and certificate change and RA operator implementation.
- Operators shall create user registration data; review and verify registration contracts, identity documents and applicant identity; and deliver user registration data to UCA. Where double verification is required, user registration data validation of administrators shall be included prior to delivering user registration data to UCA.
- The maintenance personnel of other hardware and software systems, HSM operators, supervising personnel and auditors shall carry out the duties assigned to them.

5.2.2 Number of Persons Required Per Task

TWCA operators of individual businesses shall be assigned with independent responsibility and authority. The number of persons for individual roles, such as supervising personnel, administrators, operators, auditors, maintenance personnel of other hardware and software systems, HSM operators, shall be assigned according to the characteristics of individual businesses. For example, CA key creation and change and user data change shall be operated by two operators; the keys shall be created by 2 security administrators according to the operation security control procedures. Also, these personnel shall support one another when carrying out their duties.

5.2.3 Identification and Authentication for Each Role

In using system resources, supervising personnel, administrators, operators, system maintenance personnel and system resource controllers shall be assigned with a unique role identification codes, an IC card and a PIN (or fingerprint recognition) in order to identify and verify the identity of system resource users. When operators run a function according to the business needs, every action shall be recorded in detail to ensure the accountability of system resource use and to control system security threats and risk assessments.

5.2.4 Roles Requiring Separation of Duty

Subject 5.2.2.

5.3 Personnel Controls

5.3.1 Background, Qualifications, and Experience

TWCA operators shall be honest, trustworthy and faithful in work and shall not engage in sideline jobs that will affect TWCA operations. These operators shall have clean negligence or irresponsibility records and have no criminal record.

- Operational personnel shall possess practical experience in Certification Authority (CA) operations or have completed relevant CA operational training and passed the required examinations. In cases of internal human resource shortages, the Company may assign such duties to outsourced personnel who have practical experience in CA operations.
- The administrators and supervising personnel shall have the practical experience in CA operations, preferably with experience in computer system planning, development, operation and administration. These personnel shall be assigned by TWCA and must not be outsourced to any third party.

5.3.2 Background Check Procedures

The departments related to HR management shall perform an identity security check on the supervising personnel, administrators and operators of the certification system according to the review regulations established. These personnel shall only be employed after passing the practice and experience check conducted by the relevant departments. A security, practice and experience check on these personnel shall be conducted every year according to the characteristics of their duties to ensure if they are qualified for their duties and to provide a reference for duty adjustment or transfer.

5.3.3 Training Requirements

Training on required for certification system operations are given to system operators according to their duties. This includes the required hardware and software skills, the relevant operating procedures and security control procedures, the code of operations for disaster recovery, PKI public key operations, CP, CPS and the relevant codes of operations for information security. Suitable education and training is also provided when there is a change in the certification system or a new system is added.

A complete set of education and training instructions for certification system relevant hardware and software, application system and security management system shall be established to provide education and training of the relevant skills for newcomers or when there is a system change. A record of the efficacy of education and training shall be maintained in detail as a reference for duty assignment.

5.3.4 Training Frequency and Requirements

The relevant knowledge and skills for operating the certification system of operators shall be reviewed once a year, and re-training shall be provided appropriately.

Education and training shall be provided to the relevant system operators when there is a system function update, a new system is added to the original system, or there is a progress or update in the relevant knowledge and technology.

5.3.5 Job Rotation Frequency and Sequence

To meet the needs of system operations and ensure the suitability of operational personnel, the Company will assign qualified personnel to rotate into appropriate roles for professional development. Prior to reassignment, appropriate knowledge and skill training shall be provided.

- A system administrator may be reassigned to a certificate supervisory or audit role only after being away from the original position for one year.
- A certificate supervisory personnel may be reassigned to a system administrator or audit role only after being away from the original position for one year.
- An audit personnel may be reassigned to a system administrator or certificate supervisory role only after being away from the original position for one year.
- An operational personnel may be reassigned to a system administrator, certificate supervisory, or audit role only after serving in the operational role for two years, having received the relevant training, and successfully passing the required evaluation.

5.3.6 Sanctions for Unauthorized Actions

Out of either deliberation or negligence, operators of the certification system carrying out operations not specified in their duties shall be reported to the supervisor and administrator and handled according to the relevant code of operations, whether or not such operations have caused security problems to the certification system.

5.3.7 Independent Contractor Requirements

When it is necessary to outsource work to external personnel due to HR shortage, apart from signing the non-disclosure agreement according to the work contents, the rights and obligations of contracting personnel shall be the same as that of TWCA employees. They shall also receive the education and training relevant to their duties and follow the relevant codes of operation and laws and regulations.

5.3.8 Documentation Supplied to Personnel

To ensure the normal and smooth operations of the certification system, it is necessary to supply documents related to system operations to the relevant personnel. These documents shall include:

- Operation documents of hardware and software operating platforms, network systems and websites, and HSMs.
- The relevant operation documents of the CA and RA certification systems and UCA certification system.
- CPS, CP and the relevant codes of operation.
- Internal system operation documents, such as system backup and recovery operating procedures, offsite backup and DR operating procedures, and routine operating procedures.

5.4 Audit Logging Procedure

5.4.1 Types of Events Recorded

An audit log shall include the following information:

- the registration and cancellation of registration information of users, including contracts, registration documents, application forms and messages related to registration transactions;
- the records of success and failure of the generation, entry and change of the public key and mac key for operating the certification system or other key part;
- the records of success and failure of the generation, entry and change of the CA key and certificate;
- the records of success and failure of the processing and reply of users certificate application transactions;
- audit records and e-mail logs of certification system operations;
- the records of the processing and reply of certificate revocation transactions and CRLs;
- CA data center access application forms, operator IC card CA data center access records, CA data center logs, operator business function entry records, and operator CA data center access CCTV records;
- operation change application forms and system change records of CA host system hardware and software, application systems and certification systems, and operator

system parameter change records; and

- transaction records concerning certification and access to system resources in the certification system via the Internet.

5.4.2 Frequency of Processing Log

When a new system is added to the operations, the relevant operation records of the certification system shall be checked every day. After the system is adjusted or modified to normal status, only the records of abnormal system operations shall be checked. Also, the records of normal system operations shall be checked in detail at planned intervals (once a week) according to the business needs.

The audit records of abnormal events that may affect system security shall be checked in detail according to the relevant system and document record audit regulations of TWCA, including the checking, management process and follow-up of the improvement of events.

When checking the operation records of the certification system, whether or not the audit records have been altered by unauthorized shall be audited, including the checking, management process and follow-up of the improvement of events.

5.4.3 Retention Period for Audit Log

The relevant audit logs and reports and media data shall be retained for 7 years. The records and reports of abnormal system operations shall be retained for 9 years. Video recordings shall be reused every 3 months, except for recordings that shall be retained for special reasons.

5.4.4 Protection of Audit Log

The audit logs of all TWCA certification systems shall be protected according to the security controls established for protecting audit logs of individual certification systems. Such controls shall be protected with resource control and identity authentication.

The backup copy of audit logs shall be made by independent personnel authorized with the read-only authority of audit logs. The backup copy of audit logs shall be made once a week, and one backup copy shall be retained at the offsite backup center equipped with security controls.

The audit logs of certification systems shall be protected by a security control system with read-only function and no writing or clearing of any audit logs shall be allowed. Also, only authorized personnel shall read the relevant audit logs.

The retention of document audit logs shall be protected with security controls. A copy of such logs shall be retained at the offsite backup center equipped with security controls.

5.4.5 Audit Log Backup Procedures

The audit logs and documents of certification systems shall be collated and a backup copy shall be made every week according to the Audit Record Backup Operating Procedure. A copy of the audit logs shall be retained at the offsite backup center equipped with security controls.

5.4.6 Audit Log Collection System

The collection of audit logs shall begin from the startup of the certification system and end at the shutdown of the certification system. The audit logs of certification systems shall be collected automatically by the operating system or certification system or manually by CA personnel. When the automatic audit log collection fails and the CA certification system shall continue to provide service, audit logs shall be collected manually. The events collected shall include:

Type of event	Log collection (automatically by the computer or manually by personnel)	Collected by
1. Change of OS security parameters	Automatic	OS.
2. Startup and shutdown of certification systems	Automatic	OS.
3. System login and logoff	Automatic	OS.
4. Creation, modification and deletion of system users	Automatic	OS.
5. Implementation and change of user CA system	Automatic	CA and RA certification systems
6. Generation, issue and revocation of keys and certificates	Automatic	CA and RA certification systems
7. Creation, modification and deletion of user information	Automatic	CA and RA certification systems
8. Information of transactions via	Automatic	Internet system

the Internet		
9. Backup and recovery	Automatic and Manual	System and personnel
10. Change of system environment parameters	Manual	Operator
11. Update of hardware and software systems	Manual	Operator
12. System maintenance	Manual	Operator
13. Personnel adjustment	Manual	Operator
14. Relevant forms of certification system operations	Manual	Operator

5.4.7 Notification to Event-Causing Subject

When an anomaly affecting security controls occurs during certification operations, operators shall notify the security administrator to take appropriate actions according to the system anomaly handling standards.

5.4.8 Vulnerability Assessment

The following vulnerability assessments should be performed once a year:

- OS vulnerability assessments
- Physical facility vulnerability assessments
- Certificate management system vulnerability assessments
- Network vulnerability assessments

5.5 Records Archival

5.5.1 Types of Records Archived

TWCA shall make and retain the backup copy of system environment files, contracts signed with users, information concerning user registration data, user certificate and revoked certificate data files, transaction data files, audit data files, information of UCA key and certificate change, CPS, CP and CA system data to ensure the stable operations of the certification system.

5.5.2 Retention Period for Archive

Apart from the archive retention period specified by the competent authorities, the retention period of public-key-related information specified by TWCA is as follows:

- The CPS, CP and relevant operation manuals; user registration application forms and relevant contract terms; and user identity documents shall be retained for 10 years from their expiration.
- Information of user certificate application, renewal and extension; and revoked or expired certificates shall be retained for 10 years from certificate expiration.
- The record of transaction messages concerning the application, access and revocation of certificates shall be retained for 10 years from certificate expiration.
- The data related to the PCA and UCA key changes shall be retained for 10 years from key certificate expiration.
- The data related to the Root CA key changes shall be retained for 15 years from key certificate expiration.

5.5.3 Protection of Archive

Archive data, such as keys, certificates, transaction data, audit information, CPS and registration documents shall be stored in a moisture-proof environment with central air-conditioning and protected by security controls. Unauthorized personnel shall not access such archive. No data shall be obtained in any way, except at the request of the law and the relevant codes of operations.

A copy of such data shall be stored in moisture-proof RD center with central air-conditioning and protected by security controls.

Under no circumstance shall TWCA disclose to a third party the basic data and personal identification data of users stored and protected by TWCA or RA, except at the request of the competent authorities and a court of law according to the relevant laws and regulations for resolving disputes arising from or in connection with such data.

5.5.4 Archive Backup Procedures

Keys, certificates and transaction data shall be collated, filed and backed up every day, every week and every month according to the backup and disaster recovery operating procedures. A copy shall be kept by TWCA in an environment with security controls, and another copy shall be stored in the RD center with security controls. When the certification system is unable to start up due to system anomalies, TWCA shall perform the system anomaly recovery with the backup copy it retains according to the system backup and recovery manual.

5.5.5 Requirements for Time-Stamping of Records

Changes of hardware and software facilities and systems, system parameters or system resources shall be remarked by a time-stamp during the operation of the certification system. When it is generated automatically by the operating system or certification system, the system will retrieve the time-stamp and automatically add the time to the time-stamp. When it is generated manually by operators, operators shall input the time-stamp in the relevant forms and records as a reference for future trace.

When users register to RA, apply for or renew (rekey) a certificate, revoke a certificate, suspend a certificate or access to a certificate, a time-stamp will be remarked in the transaction messages. The time-stamp is generated automatically by the operating system or certification system according to the system clock and added to the record automatically.

5.5.6 Archive Collection System

Archive records concerning certification system operations shall be retained by TWCA personnel. Such records shall be produced by the relevant TWCA systems with independent resources and security controls. Collected audit logs shall also be retained by TWCA internal control system. The records of the retained documents of certification system operations shall be collected and managed by the relevant personnel.

5.5.7 Procedures to Obtain and Verify Archive Information

According to the code of operations of TWCA internal control, the archive information of certification systems shall be verified once a year or irregularly according to business needs. When verifying and auditing the archive records, the responsible auditor shall verify these records according to the code of operations for internal audit, including the test of offsite DR.

5.6 Key Changeover

5.6.1 Key Changeover of Subscriber

UCA shall specify the lifecycle of the subscriber key at the same length as the certificate issued to subscribers by CA. That is to say, when the user certificate expires, the corresponding shall also be invalidated.

Before the expiration of the subscriber's key validity period, the subscriber shall complete the Certificate Renewal Application Form and submit it to the RA to proceed with the subscriber key replacement process. Once the process is completed, the subscriber may generate a new key pair and apply for the issuance of a new certificate from the UCA or the RA. The relevant procedures shall follow the provisions of Section 3.3.1.

If the old key is deemed insecure while still within its validity period, the subscriber shall first apply for the revocation of the old certificate through the UCA or theRA. Only after the revocation can a new key pair be generated. The subscriber shall then complete the Certificate Issuance Application Form in accordance with the operational procedures of the RA and apply for the issuance of a new certificate. The certificate revocation procedures shall refer to the provisions of Section 4.9.

5.6.2 Key Changeover of UCA

UCA may generate a new key pair to apply for a new certificate after the existing key has expired. After the new certificate is issued, UCA shall sign the user’s applications for new certificates and certificate revocation with the new private key and continue to sign with the old key the CRLs of UCA certificates issued with that key until it is expired. Also, UCA shall immediately notify RAs.

When there are doubts about key security prior to the key’s expiration, UCA shall first apply for certificate revocation to PCA before generating the new key pair to apply for a new certificate. After the new certificate is issued, UCA shall sign the user’s applications for new certificates and re-sign the CRLs with the new key. UCA shall immediately notify users and RAs of with the fastest method that user certificates and CRLs issued with the old UCA private key are invalid and users shall generate a new key pair to applying for a new certificate to UCA.

5.6.3 Key Changeover of PCA

When the key has expired, PCA shall generate the next key pair to apply for a new certificate to Root CA according to the certificate chain. After that, PCA shall sign the UCA’s application for new certificates and certificate revocation with the new private key and continue to sign with the old key the CRLs of UCA certificates issued with that key until it is expired. CA shall also immediately notify UCAs.

When there are doubts about key security prior to the key’s expiration, PCA shall first revoke the old certificate before generating the new key pair to apply for a new certificate to RCA. After the new certificate is issued, PCA shall sign the UCA’s applications for new certificates and re-sign the CRLs with the new key. Also, PCA shall immediately notify UCAs with the fastest method that UCA certificates and CRLs issued with the old PCA private key are invalid and UCAs shall generate a new key pair to apply for a new certificate to PCA.

5.6.4 Key Changeover of RCA

Prior to the key expiration, RCA shall generate a new key pair, self-issued certificate and the fingerprint ID of the new certificate. RCA shall continue to sign with the old key the CRLs of PCA certificates issued with that key until it is expired and immediately publish the fingerprint ID of this new self-issued certificate and notify PCAs.

When there are doubts about key security prior to the key's expiration, RCA shall first revoke the old certificate before generating the new key pair, self-issued certificate and the fingerprint ID of the new certificate. After that, RCA shall immediately notify PCAs with the fastest method that all old certificates are invalid and PCAs shall generate a new key pair to apply for a new certificate to RCA.

When the private key is cracked, RCA shall immediately revoke all PCA certificates and notify UCAs according to the certificate chain to immediately revoke all user certificates and business application systems to stop using all certificates issued by the certification system.

5.7 Key Cracked and Disaster Recovery Procedures

5.7.1 Key Cracked and Emergency Handling Procedures

This CA has established an Emergency Response Procedure and Disaster Recovery Plan, documented in writing as part of its Business Continuity Plan and Disaster Recovery Procedures. These documents include notification procedures for users and relying parties in the event of a disaster, security breach, or service disruption. The aforementioned procedures shall be reviewed or revised by this CA on an annual basis.

5.7.2 Corrupted Computing Resources, Software and Data Handling Procedures

When software computing resources of the certification system or data related to system operations are corrupted, system recovery can be implemented with the internal media backup data or backup mediate data stored in the offsite RA center according to the system backup and recovery manual to resume normal system operations.

When hardware computing resources of the certification system are corrupted, the certification system can be re-installed, re-implemented and recovered with the internal backup hardware equipment, the relevant software computing backup resources and system operation backup data according to the system backup and recovery manual to resume normal system operations.

5.7.3 Entity Private Key Cracked Handling Procedures

If the Certificate Management Center's key is suspected to be compromised or lost (even if the compromise is not yet confirmed), the following procedures shall be undertaken:

- The RA shall promptly notify all users via email, written notice, or other appropriate means.
- A new key pair shall be generated in accordance with the provisions of Section 6.1 and submitted to the superior Certificate Management Center for the issuance of a new certificate.
- All valid certificates shall be revoked. A new Certificate Revocation List (CRL) shall be issued using the new signing key, and this CRL shall include all unexpired certificates.
- New certificates shall be issued to users in accordance with the procedures outlined in Section 4.3.

The Certificate Management Center shall immediately investigate the incident and report to the Policy Management Authority the reasons for the key compromise or loss, as well as the measures taken to prevent recurrence.

If a user's key is suspected of being compromised, the procedures outlined in Section 4.9.3 shall be followed.

5.7.4 Business Continuity Capabilities after a Disaster

After a natural or other type of disaster, the relevant secure facilities of the certification system shall be:

- Repaired or updated to normal status as soon as possible when system operations will not be affected during system recovery in order not to affect normal system operations;
- Shut down immediately and repaired or updated to normal status as soon as possible when system operations will be affected prior to restarting system operations; the DA plan shall be initiated if such facilities shall not be recovered or updated within the time specified in the code of operations in order to restart system operations at the offsite DR center;
- Shut down and the DR plan shall be initiated immediately to recover system operations when the relevant secure facilities are severely damaged.

To avoid business discontinuity as a result of natural and other type of disasters, TWCA has planned an offsite DR plan and implemented an offsite DR system to implement systems, storage media and documents in an offsite DR center at an appropriate distance from the TWCA's operation systems. These systems, storage media and documents include the software and hardware system and facilities required for system operations, media and documents related to certificate information, code of operations and business system recovery documents.

An exercise and test of the contingency and DR plan for the business recovery systems for offsite disaster recovery shall be conducted once a year according to the business needs. The code of operations and system recovery documents shall be updated constantly according to the changes in the actual operating environment. The testing records shall be maintained for audit. By doing so, the operations of the certification system shall be recovered within 24 hours from a natural or other type of disaster to ensure and minimize the risk on business continuity.

5.8 CA Service Termination

When terminating the service of any system for whatever reasons, TWCA shall minimize the impacts on business continuity and reliably transfer the relevant certification business to a secure and objective CA to continue the relevant business.

In case of normal termination of service, contract expiration or organization restructuring without threat of security, TWCA shall:

- notify the competent authorities 30 days prior to termination of service;
- notify the users of the service termination and that such service shall be overtaken by other CA 30 days prior to termination of service;
- arrange the other CA overtaking the relevant business to overtake the rights of valid users certificates;
- revoke the certificate of the CA to be terminated and all user certificates it issues and transfer to the CA overtaking the business the relevant private keys and certificates, all user certificates and CRLs of the CA to be terminated in a highly secure operating environment without any doubt of security;
- transfer to the overtaking CA the CP, CPS and relevant operating manuals and documents of TWCA; user contracts and registration data; audit records; archive data; certificate status data and the documents required for overtaking the business to securely retain such documents and data for 7 years;
- expunge the relevant private keys of the CA to be terminated, officially announce to users that the certification business has been transferred to the overtaking CA, and assist the overtaking CA to run the certification business as much as possible; and

- announce the fact to users as soon as possible when the service is terminated as a result of abnormal situations (bankruptcy or illegal operations announced by a court of law) and terminate the service according to the normal service termination procedures in order to minimize the impacts on the operations of the user business system.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

When generating the CA key pair, two key administrators shall log-in the HSM at the same time to generate the key pair directly from the HSM. Under no circumstance shall the key pair be generated by a single person. Also the key pair generated by the HSM shall be directly encrypted and stored in the HSM.

The user's key pair shall be generated under the control of the user.

6.1.2 Private Key Delivery to Subscriber

As TWCA does not provide key pair generation service for users, there is no need for security controls for private key delivery.

6.1.3 Public Key Delivery to Certificate Issuer

When a subscriber applies for a certificate to RA or directly to UCA with his/her public key, apart from protecting the user’s signature, the public key in the request message shall protect the integrity of message encryption.

In the reply message for certification application success, the UCA signature and message integrity are protected.

6.1.4 CA Public Key Delivery to Trusted Certificate Parties

When the CA public key is delivered to the users after a change or user enquiry, the CA signature and message integrity in this public key are protected.

6.1.5 Key Sizes

The length of the RSA public key of RCA is 2048 bits, and the bit length shall be divisible by 8; the security strength of the curve used by the ECC public key is P-256.

The length of the RSA public key of PCA is 2048 bits, and the bit length shall be divisible by 8; the security strength of the curve used by the ECC public key is P-256.

The length of the RSA public key of UCA is 2048 bits, and the bit length shall be divisible by 8; the security strength of the curve used by the ECC public key is P-256.

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

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

6.1.7 Key Usage Purposes

Subscribers shall use the certificate issued by TWCA to subscribers for use as electronic signature, encryption and other purposes according to the level of assurance specified in the CPS and business application systems. Also, subscribers shall use their certificates in the relevant business systems according to the usage specified in the Key Usage column in the standard expansion column of the X.509 V3 certificates.

Apart from electronic signature and encryption, users requesting certificates for other purposes shall apply to UCA for the key and certificate that meets their intended use.

6.1.8 Subscriber Key Generation Equipment

The key pair generation device of subscribers usually refers to the key generation device built in the operating system.

6.2 Private Key Protection and Cryptographic Module Engineering Control

6.2.1 Cryptographic Module Standards

Use hardware cryptographic modules that comply with CNS 15135, ISO 19790, or FIPS 140-2 Level 3 standards.

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

The UCA private key shall be generated, implemented and changed by 2 key administrators at the same time. Under no circumstance shall the said key be generated, implemented and changed by a single person. Also, the relevant information of the private key, such as the IC card and PIN, shall be controlled by different administrators with independent duties and stored in an environment with security controls.

If the backup and retention of the private key is stored by means of m of n key parts, it shall be backed up and stored independently by different key administrators in media with security controls. If the private key is backed up and stored in plain text, the key administrator shall encrypt the private key with the key part of the HSM before storing it in media with security controls, and audit records shall be maintained.

6.2.3 Private Key Escrow, Recovery and Storage

Not applicable.

6.2.4 Private Key Backup

The CA private key shall be encrypted before storing in the HSM. The backup of the key shall be performed by 2 authorized personnel and stored in media after encryption. Personnel may also store the m of n key parts of the private key in an IC card and store the m of n key parts in the secure vault with dual control and a copy of the control the offsite DR center with security controls.

6.2.5 Private Key Archival

After encryption, the CA private key may be stored in an IC card by means of key component with security controls or in the interface media and placed in a secure vault with dual control. The retention of the private key after its expiration is the same as the security controls for private keys in use. The storage operations related to the private key shall be the same as those specified in Section 5.6.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The CA private key shall be generated, implemented or changed directly from the HSM by 2 key administrators. Under no circumstance shall the key be implemented or changed by a single person. After encryption and storing in the HSM, the private key shall be unable to output outside of the HSM in plain text.

When it is necessary to compute with that private key, the computing shall be done directly in the HSM via the functional interface of the HSM. After the computing, the results shall be output, and the private key shall not be output in plain text outside of the HSM.

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 CA private key stored in the HSM shall be activated by 2 authorized key administrators (e.g. IC card and fingerprint or password verification) prior to use. Unauthorized personnel shall not activate or access the CA private key.

The subscriber private key shall be protected by password or pass-phases possessed by the subscriber, and no one else can access such password or pass-phases.

6.2.9 Method of Deactivating Private Key

The private key stored in the HSM shall be deactivated by 2 authorized key administrators logging in the system (e.g. IC card and password verification) prior to implementation. Unauthorized personnel shall not access the private key.

After deactivation, either the HSM or the private key shall be stored in an environment with security control. Unauthorized personnel shall not access.

6.2.10 Method of Destroying Private Key

After the expiration of the private key or when the corresponding public key becomes invalid or is revoked, the Certificate Authority shall erase the private key from software cryptographic modules using data overwriting methods. For hardware cryptographic modules or IC cards, the private key shall be erased using zeroization techniques.

When hardware cryptographic modules are decommissioned, all private keys stored on the devices shall also be erased using the aforementioned methods.

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The procedures and security requirements of public key archival shall be the same as that of certificate archival. Public keys and certificates shall be retained for 10 years. If the retention period specified by the competent authorities is longer, such retention period shall prevail.

6.3.2 Public Key and Private Key Validity Periods

Unless otherwise specified in the business requirements of CA and RA, the validity periods of users public key and private key shall be the same.

The maximum validity of the user public and private keys shall be 3 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

The activation data of subscriber private keys, such as IC card PIN, pass-phase, etc., shall be generated directly inside the HSM in a environment with security control. It shall be a randomly generated number (recommended length of a password is 6 characters and pass-phase 8 characters). When it is delivered to the user over the Internet, it shall be protected with appropriate security controls. If it is delivered to the user by mail, it shall be delivered in a sealed password envelope. The delivery method is subject to change according to the user requirement during implementation.

6.4.2 Activation Data Protection

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

Subscriber activation data shall be properly retained or destroyed after memorizing them and shall not be disclosed to others. If it is needed to retain them in paper format, the data shall be stored in a secure environment and shall not disclose them to others. Activation data shall be changed anytime according to the security requirements of business systems.

6.4.3 Other Aspects of Activating Data

In consideration of security, the frequency of change of the lifecycle of the activation data for subscriber certificates is as follows:

- Low protection:

  The length of the activation data is 4-6 numbers. The activation data are stored in the system in plain text. They can be selected by the user. There is no need of special security controls when delivering by mail. The recommended lifecycle for the activation data used in non-confidential or general data delivery or low amount transactions shall be one year, and such data shall be changed after one year.

- Medium protection:

  The length of the activation data is 4-8 numbers. The activation data are stored in the system after encryption. Special security controls are needed when they are mailed to users. They can be selected by users or generated by the system. The recommended lifecycle for the activation data used in the delivery of generally important data or general amount transactions shall be six months, and such data shall be changed after six months.

- High protection:

  The length of the activation data is 6-8 numbers. The activation data are stored in the system after encryption. Special security controls are needed when they are mailed to users. They are randomly generated directly inside the HSM in an environment with security control. The recommended lifecycle for the activation data used in the delivery of rather important data or transactions at a certain amount shall be one month, and such data shall be changed after one to three months.

For the security reason, subscribers are recommended to change the activation data issued by TWCA for protecting the private key or IC card of users according to the security requirements of the business system.

The lifecycle specifications of the activation data that users use to apply for certificates to TWCA are specified in the relevant codes of operation of certificates.

Subscribers are recommended to change frequency of change of the activation data (e.g. IC card PIN, disk password) issued by RA to users according to the security level requirements of the business (e.g. users are recommended to change the activation data for connecting to the RA every 3 or 6 months).

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The certificate system and relevant supporting systems provide the following security controls with operating systems, or by integrating with operating systems, software and physical protection.

- System login with identification authentication.
- User-defined access control.
- Security audit ability.
- Restrictions on various certificate services and the access control of trusted roles.
- Identification and authentication of trusted roles and identity.
- Assurance of communication and database security.
- Secured and reliable channels for the identification of trusted roles and relevant identity.
- Protection for procedural integrity and security controls.

6.5.2 Computer Security Rating

The computer systems used to perform authentication operations shall meet the security requirements of either the Common Criteria (CC, ISO/IEC 15408) certification for the General Purpose Operating Systems Protection Profile (GPOSPP), or be certified at EAL4+ level, or be approved for use through internal security evaluation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

This follows the ISO 27001 specifications in CA system development.

Both hardware and software of the CA are dedicated, only components complying with the security policy are used, and no irrelevant hardware devices, network connection or software components are installed.

6.6.2 Security Management Controls

This CA operates in accordance with the standards of ISO/IEC 27001 and WebTrust for

Certification Authorities (CA) as established by AICPA/CICA.

Prior to software installation or update, CA validates that the correct version is provided by developers, and the software is unmodified. After system installation, the CA verifies its integrity when running the system.

6.6.3 Life Cycle Security Level

This CA conducts an annual review to assess whether the current cryptographic algorithms or keys are at risk of being compromised.

6.7 Network Security Controls

The certification systems of RCA and PCA are independently operated off-line management systems that are operated manually only by business-related personnel after authorization.

Only authorized personnel of the relevant business can implement management work with the certificate management system. These personnel shall pass the personal identification by accessing 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 the certificate system are connected only to the intranet and segregated from outside by means of a firewall. Connections with the internal hosts shall pass the identity verification, and only authorized personnel or systems can access to the internal host.

Update patches, system vulnerability scan, intrusion defense system and the firewall system are applied to protect the repository of the certificate system against denial of service (DoS) and instructions.

6.8 Time-stamp

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

- Time of certificate issuance;
- Time of certificate revocation;
- Time of CRL issuance.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The details of the certificate that used by the UCA certification systems shall be specified in the certificate-related code of operation for certificate profiles.

7.1.1 Version Number(s)

The CA certification systems currently issue X.509 V3 certificates. The version number is indicated in the certificate version format column.

7.1.2 Certificate Extension Columns

In addition to the basic columns and standard extension columns, CA uses the X.509 V3 certification system with private extension columns. Please refer to the certificate-related code of operation for certificate profiles for the details of columns.

7.1.3 Algorithm Object Identifiers

Based on the specification announced by the ISO OID management unit, the algorithm object identifier that used in individual certification systems is as follows:

Algorithm Security Mechanism	Algorithm	Object Identifier (OID)
Key Algorithm	RSAEncryption	1.2.840.113549.1.1.1
Key Algorithm	ecPublicKey	1.2.840.10045.2.1
Signature Algorithm	sha-256WithRSAEncryption	1.2.840.113549.1.1.11
Signature Algorithm	sha-1WithRSAEncryption	1.2.840.113549.1.1.5
Signature Algorithm	sha384WithRSAEncryption	1.2.840.113549.1.1.12
Signature Algorithm	ECDSAWithSHA256	1.2.840.10045.4.3.2
Signature Algorithm	ECDSAWithSHA384	1.2.840.10045.4.3.3
Hash Function	SHA-256	2.16.840.1.101.3.4.2.1
Hash Function	SHA-1	1.3.14.3.2.26

7.1.4 Name Forms Identification

The identifier name forms of the user certificates issued by the certification systems comply with the X.500 Distinguished Name(DN) naming formats.

7.1.5 Name Constraints Identification

The “nameConstraints” extension column is added to the certificates issued by CA where appropriate.

7.1.6 Certificate Policy Object Identifier

The CP object identifier defined in the CP is used in the “certificatePolicies” extension column of the certificates issued by CA.

The CP-related OIDs of user certificates issued by the certification systems according to the X.509 V3 specification are stored in the CP-related columns in the certificate. The OID distinguished value is specified in the certificate-related CP and the code of operation for certificate profiles.

7.1.7 Usage of CP Constraints Extension Columns

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

7.1.8 CP Qualifiers Syntax and Semantics

When the policy constraint extension column is used in the certificate, its syntax and semantics is specified in the certificate-related code of operations for certificate profiles. The CP terse statement is stored in the CP extension column of C-XML certificates, and it is the constraint code of applicability of certificate usage. The syntax and semantics of the constraints are: Part 1 is the level of assurance of personal identification; Part 2 is the usage; Part 3 is the user status; and Part 4 is the business category. Please refer to Section 1.4 for details.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension Column

When the policy constraint extension column is used in the certificate, the required code of operation is specified in the business-system-related code of operations. The CP terse statement is stored in the CP extension column of C-XML certificates, and it is the constraint code of applicability of certificate usage. This shall be checked and processed when using the certificate in business application systems.

7.2 CRL Profile

7.2.1 Version Number(s)

Certification systems currently issue X.509 V2 CRLs. The version value is indicated in the version format column in the CRL.

7.2.2 CRL and CRL Entry Extension Columns

For each certificate system, when using certificate revocation list (CRL) extension fields during certificate revocation operations, the detailed contents of each field shall refer to the CRL profile.

7.3 OCSP Profile

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

The audit of the operational security controls for this company's certificate system is conducted in accordance with this company's internally established self-audit guidelines, which reference the WebTrust Principles and Criteria for Certification Authorities and the ISO/IEC 27001 standards. An internal audit shall be performed once annually.

8.2 Identity and Qualifications of Assessors

Auditors performing the audits shall be equipped with the knowledge of certification authority and information security audit, two years of relevant audit experience and the relevant knowledge of application system businesses and computer software systems and experience in system planning, design and development, and are familiar with the regulations of this CPS. When the requirements and qualifications of auditors are specified in the regulations of relevant national management authorities, these requirements and qualifications shall prevail. Holders of national auditor qualifications or internationally recognized auditor qualifications with the relevant practical audit experience are also qualified auditors.

8.3 Assessor's Relationship to Assessed Entity

Either the internal or external auditors shall have no involvement in the business of the parties being audited. That is to say, auditors shall have no business or financial connections with the parties being audited or any interest with these parties that shall interfere with the objectivity of the audit. Auditor shall perform the audit and assessment with an independent, impartial and objective attitude.

When there are inadequate qualified auditors, professional, impartial and objective third-party auditing organization shall be hired to conduct the audit.

8.4 Topics Covered by Assessment

The major auditing items shall include:

- Announcement of business implementation:

  If certificate management is implemented according to this CPS and the relevant codes of operations.

- Service integrity

  The security management of the lifecycle of CA private keys and the relevant certificates (generation, implementation, use, cancellation of registration, retention and destruction); the security management of the lifecycle of certificates, revoked certificates and expired certificates; and the security management of the lifecycle of interface media (e.g. IC cards).

- Security control of CA environment:

  Information security management complied with the information security policy, CP and CPS; risk assessment and security control of assets; security control of operators; security control of the secure facilities in the physical environment; security control of hardware and software equipment and media; security control of system or network access; security control of system development and maintenance; system DR management; System Offsite RD Management complied with the relevant laws and regulations and international standards; and security management of audit events and records.

When auditing regulations and standards are specified by the competent authorities, the internal audit shall comply with and pass the verification and certification of the competent authorities. When there is an integration of transnational or transborder certification systems, the internal audit shall comply with and pass the transnational or transborder audit standards.

8.5 Actions Taken to Deficiency of the Result of Assessment

When nonconformities to the CPS or regulations concerning operational security are detected in the detailed assessment, auditors shall list the defects detected in detail by severity and notify the audit unit and the audited party.

The audited party shall propose the corrective and preventive actions and plans according to the defects detected. The relevant auditors of the audit unit shall review the reasonability and applicability of these corrective and preventive actions and follow up the improvement.

8.6 Publication of Results

The CA will publish the results of the latest external audit in the repository.

9. Other Business and Legal Regulations

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The fee structure and rates for the registration, certificate application and certificate renewal services between the UCA and RA or users shall be specified in the fee calculation regulations of corresponding businesses or contract terms.

9.1.2 Certificate Access Fees

The fee structure and rates for the certificate access service between the UCA and RA or users shall be specified in the fee calculation regulations of corresponding businesses or contract terms.

9.1.3 Certificate Revocation or Status Information Access Fees

The fee structure and rates for the certificate revocation provided by the UCA shall be specified in the fee calculation regulations of corresponding businesses or contract terms.

9.1.4 Fees for Other Services

It is free of charge for users to download the CPS or CP from the website. However, when users request a paper version of the CPS or CP or other relevant documents, TWCA shall charge a processing fee and the postage from the requesting users. The rates shall be specified in the fee calculation regulations of corresponding businesses or contract terms.

9.1.5 Refund Policy

When a subscriber applies to TWCA or the RA for a refund and revocation of a certificate issued within 7 days, the fees will be refunded to the user without interest after deducting a handling fee of NT$100. However, when the application for refund and certificate revocation is made after 7 days from the issue, no fees will be refunded.

9.2 Financial Responsibility

9.2.1 Liability Coverage

In risk management related to certificate management operations, in addition to having insurance coverage for earthquakes and fire damage for buildings and hardware facilities, the company has secured US$2 million in general liability insurance and US$5 million in professional liability insurance to protect user rights and mitigate business operational risks.

9.2.2 Other Assets

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

9.2.3 Liability for End-Entities

Subject to Section 9.2.1.

9.2.3.1 Liability of the TWCA certification

- The certification services and operations provided by this CA are defined in Section 1.4.1 of this CPS. Any content not specified in this statement is excluded from liability for compensation.
- 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.
- This CA assumes no responsibility for indemnifying any damages arising from or in connection with losses as a result of an act of God or natural disasters (e.g. earthquakes) and/or events (e.g. wars) beyond the reasonable control of this CA.
- This CA shall 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 CPS, the CP and/or the relevant codes of operations; or violation of the relevant laws and regulations. The upper limit of compensation is in accordance with the provisions of 9.8 Limitation of Liability.
- This CA assumes no responsibility for indemnifying any damages arising from or in connection with legal disputes over the use of a subscriber certificate from receiving a revocation request made by this CA or persons who can make a revocation request until the publication of certificate revocation listed in CRLs, provided that this CA processes the revocation request according to this CPS and the relevant codes of operations.
- This CA assumes no responsibility for indemnifying any damages arising from or in connection with the use of illegal, fabricated or erroneous certificates.
- The statue of repose of the subscriber's claim for damages is subject to the relevant laws and regulations.

9.2.3.2 RA Liability

- RA shall take due care of the registration data and the relevant information of users and avoid leaks, identity fraud, interpolation and unauthorized use of the relevant information. When employees of RA cause damage to users or others as a result of processing user registration and relevant information or errors occurred from the application for user certificates to the UCA, RA and their employees shall be in full liability for the direct damage that caused to the corresponding subscribers.
- When employees of RA cause damage to users out of deliberation or negligence during processing user registration, certificate issuance, certificate renewal, certificate suspension and certificate revocation without following the CPS and other relevant RA operating procedures and regulations or by violating the relevant laws and regulations, RA shall indemnify the direct damage of users as specified.
- RA shall be free from any liability for the damage incurred from the use of illegally falsified or incorrect certificates that are not attributable to RA.
- After a certificate user or any person entitled to make a request of certificate revocation or suspension makes a request of certificate revocation or suspension and before the UCA publishes the revocation or suspension (CRL) of that certificate, if that certificate is used in illegal transactions or there are disputes arising out of or in connection with the transactions made with that certificate, RAs shall be free from any liability when the request of certificate revocation or suspension is processed according to this CPS or the relevant operating procedures.
- The liability of RAs shall not cover the illness, mental or emotional troubles incurred from the use of certificates.

9.2.3.3 Subscriber Liability

- Out of deliberation, negligence or indecent intentions, users shall be fully liable for the damages caused to another person by the provision of false or untrue data for registering to the RA.
- Subscribers shall properly retain the private key and PIN of their certificates and shall not disclose for lend them to another party. Out of either deliberation or negligence, users shall be in full liability for indemnifying the damage that caused to RAs, TWCA or a third party.
- After a certificate user or any person entitled to make a request of certificate revocation or suspension makes a request of certificate revocation or suspension and before the UCA publishes the revocation or suspension (CRL) of that certificate, users shall immediately revoke the use of that certificate according to the regulations of the business system and notify the relevant relying parties to stop using that certificate.

During the request of certificate revocation or suspension, if users do not revoke the use of that certificate according to the regulations of the business systems and immediately notify the relevant relying parties to stop using that certificate, the user shall be fully liable for the damage that caused.

- If a subscriber violates this CPS and the relevant code of operations when applying for the use of certificate or the use of a relying party certificate, or uses the certificate in other scope of uses not specified in this CPS or scope prohibited by the competent authorities, or violates the relevant laws and regulations, the user shall have full liability for the damage caused.

9.2.3.4. Relying Party's Liability

If that certificate is used in illegal transactions or there are legal disputes arising out of or in connection with the transactions made with that certificate, users, TWCA and the RA shall be free from any liability when the request of certificate revocation or suspension is processed according to this CPS and the relevant operating procedures.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Confidential information includes:

- The private key and password for operating CA.
- The multi-person control data for controlling the private key of CA.
- The personal data of the representative and agent applying for certificates.
- Records valid for audit and traceability generated or held in custody by CA.
- Audit records and documents generated by auditors during the audit.
- 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:

- Disclosure made by the law with the authorization of the competent authorization given according to the regulatory procedures.

- Courts or arbitration institutions with lawful jurisdiction may handle disputes and arbitration arising from certificates, provided that the request is made in accordance with legal procedures.

9.4 Privacy of Personal Information

9.4.1 Privacy Protection Plan

TWCA protects the subscriber information according to the Personal Information Protection Act of the Republic of China and the regulations and code of operations specified by other government units in compliance with the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data published by the Organization for Economic Co-operation and Development (OECD).

When using or accessing to user information for certificate management, CAs/RAs shall access to such information by authorized personnel according to the business requirements under strict security control.

Neither CA nor RA shall make pubic, sell or lease the registration basic data and personal identification information of users without prior user permission when managing or using user information.

This company obtained the BS 10012 certification for Personal Information Management Systems (PIMS) in November 2013. In July 2018, it upgraded to BS 10012:2017 and simultaneously obtained certification for ISO/IEC 27701 (Privacy Information Management System), which remains valid to date.

9.4.2 Types of Personal Privacy Information

- Basic registration data and personal identification information of subscribers;
- The subscriber's personal identification information that is used in registration or certificate application;
- The private information in subscriber registration, certificate application, certificate renewal, certificate suspension or certificate revocation transaction.
- Subscriber information that users completed in the registration-related application forms and contracts and the private information in the identity documents (or their photocopy).

9.4.3 Types of Non-personal Privacy Information

The subscriber certificate information, certificate status information (for certificate validity enquiry) published on the directory server or database; and the certificate information, CRL, CP and CPS of the UCA are non-confidential information that can be disclosed.

9.4.4 Responsibility to Protect Personal Privacy Information

Subject to the relevant laws and regulations.

9.4.5 Notice and Consent to Use Personal Privacy Information

Subject to the relevant laws and regulations.

9.4.6 Disclosure Pursuant to Judicial or Administrative Requirement

Subject to Section 9.3.3.

9.4.7 Other Information Disclosure Circumstances

Subject to Section 9.3.3.

9.5 Intellectual Property Rights

TWCA warrants that the hardware and software systems and the relevant equipment and operating manuals thereof that are used in the certification system are legally licensed for its use by their intellectual property right proprietors. TWCA further warrants that it shall not infringe the right of any third party. All rights of systems independently developed by TWCA and their operating manuals shall be reserved to TWCA.

TWCA shall be the proprietor of the intellectual property rights of this CPS, CP and other documents written for carrying out other operations for certificate management.

The private and public keys generated by users are owned by their users. However, after the public key is issued in the form of a certificate by the UCA and stored in the directory server or database, TWCA shall be the proprietor of the intellectual property rights of such certificates, and their users and relying parties are licensed by TWCA to use such public key certificates.

TWCA shall be the proprietor of the intellectual property rights of the CA certificates, CA and user certificate status information and the CRLs generated and issued by TWCA, and their users and relying parties are licensed by TWCA to use such certificates, status information and CRLs.

TWCA respects the user’s registered name stored in the subject distinguished name field of the X.509 V3 certificate, but does not guarantee the ownership of the intellectual property rights associated with the registered name. If a registered trademark submitted by a user during registration has already been used by a prior user, any legal disputes or arbitration related to the intellectual property rights of the registered trademark or registered name fall outside the jurisdiction and responsibility of the company. Users should submit such matters to the relevant competent authority.

9.6 Responsibility and Obligation

9.6.1 CA Responsibilities and Obligations

- To establish, publish and manage the CPS and CP for certificate issuance and the SOPs related to certification.
- To ensure the rights and obligations of UCAs and RAs and the RA practice is operated according to this CPS, the CP and relevant standards.
- To confirm the selection of certification system personnel (including independent contractors) and ensure that system operation conforms to the CPS.
- Operators should take good care of the registration and certificate data and related information of subscribers to prevent leakage, marauding, interpolation and unintended use of such data and information.
- To accept the certificate application, certificate renewal, certificate suspension, certificate revocation, certificate access and certificate registration of users (RA) according to the CPS; ensure the veracity and integrity of transaction data delivered from the RA and users to the UCA; issue certificates; and correctly and securely deliver the relevant reply messages to users.
- To correctly and securely deliver the user certificates and TWCA CRLs to the repository according to the CPS when offering the DA service.
- To specify in the contracts signed with users or relevant operating documents the code of operations for certificate application, certificate renewal, certificate suspension, certificate revocation, certificate registration and certificate uses; and the relevant rights and obligations.
- Private signature key of UCA shall only be used in the issue and revocation of user certificates. A different and independent private key shall be used for information encryption or other signature purposes.

9.6.2 RA Responsibility

- To ensure the rights and obligations of RA and users according to this CPS, CP and RA code of operations; and to verify the authenticity and integrity of application information in processing user personal identification, certificate application, certificate renewal, certificate suspension, and certificate revocation.

- To confirm the selection of RA certification system personnel (including independent contractors) and ensure that system operation conforms to the CPS and RA SOP.
- To ensure that subscribers have understood and agreed to the rights and obligations and the business-related code of operations specified in the application form and contract when applying for registration; users (or the legal agent of a legal person) sign in the application form or contract in person to confirm their understanding and agreement of such rights and obligations; or to request users to sign the relevant documents according to the code of operations corresponding to the level of assurance of their registration status.
- To accept the subscriber's application for registration and cancellation of registration, certificates application, certificate renewal, certificate suspension, certificate access and certificate revocation.
- To verify the authenticity and veracity of user identify in processing applications for registration or cancellation of registration and certificates; to notify the UCA to issue certificates to the applicants; and to securely deliver to users the correct messages replied from the UCA.
- RA and its workers shall take due care to retain the registration data and the relevant information of users and avoid leaks, identity fraud, alteration and unauthorized use of the relevant information.
- To specify in the contracts signed with users or relevant operating documents the code of operations for certificate application, certificate renewal, certificate suspension, certificate revocation, certificate registration and certificate uses; and the relevant rights and obligations.
- In doubts of security, such as identity fraud, exposure and loss of the RA private key corresponding to certificates, or when there is a change of the information related to the RA in the certificate, the RA shall immediately report to the UCA issuing the certificate according to the relevant regulations.
- RA assumes the representations and warranties relating to subscriber registration. This UCA assumes the responsibilities and obligations relating to the issuance of certificate commissioned by RA. RA shall provide the information regarding the above representations and warranties to users and relying parties.

9.6.3 Subscriber Responsibilities and Obligations

- When registering to RA, subscribers shall submit detailed and correct documents and data of identity.
- To understand and agree to the rights and obligations specified in the application form

and contract and the code of operations concerning the application for certificates, renewal of certificates, suspension of certificates, revocation of certificates, registration of certificates and the use of certificates; and to sign in the code when applying for registration to the UCA.

- Subscribers shall generate and protect their private key and the corresponding private key protection password securely and in full compliance with the provisions of this Practice Statement. No one other than the user or a designated custodian shall have knowledge of or access to the private key and its protection password.
- Subscribers shall verify the authenticity of users and UCA and the integrity and validity of certificate information when accepting the user certificate issued by TWCA.
- Subscribers shall 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.
- In doubts of security, such as identity fraud, exposure and loss of the private key corresponding to certificates, or when there is a change of the information related to the user in the certificate or desire to stop using the certificate, users shall immediately report to the RA according to the relevant regulations.

9.6.4 Relying Party's Responsibilities and Obligations

- When using certificates, relying parties shall understand and agree to the CPS and the rights and obligations 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.
- The use of a certificate shall comply with the provisions of the Certification Practice Statement, the operational regulations of the applicable business systems, and the X.509 certificate standard. The certificate shall be validated step-by-step through the certificate chain to ensure its correctness and validity. When a Certificate Revocation List (CRL) or equivalent security mechanism is available, it shall be checked to determine whether the certificate has been revoked or suspended.
- When verifying the validity of transaction information, apart from verifying the validity and legitimacy of subscriber certificates, underlying parties shall 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 Repository Representations and Warranties

- To ensure the responsibilities and obligations of repository authority and subscribers and TWCA according to this CPS and the code of repository operation; and to enquire information and carry out security controls related to user certificates.

- To immediately update the database and inform users of the latest information according to the user certificates and CRLs delivered by the UCA; and to provide 24-hour normal services, except for system maintenance.
- To verify the authenticity of identity, enquire the validity of messages and securely and effectively send to users the correct information enquired when users enquire information to the directory server or database; unauthorized users shall not access to other information stored in other repository, except for the information of certificates and CRLs which are open to user access.
- Both the repository and its operators shall take due care of the registration and certificate data and other information of users and avoid the leaking, identity fraud, alteration and unauthorized use of the relevant information.
- In doubts of security, such as identity fraud, exposure and loss of the repository private key corresponding to certificates, or when there is a change of the information related to the repository in the certificate, the repository shall immediately report to the UCA issuing the certificate according to the relevant regulations.

9.7 Disclaimers of Responsibilities

- TWCA assumes no responsibility for indemnifying any damages arising from or in connection with the processing of user registration data and certificate issuance; except for losses caused by TWCA’s failure to follow this CPS, the CP or the relevant codes of operations as a result of negligence attributable to TWCA.
- When loss is caused to subscribers and relying parties as a result of an interruption of Internet transmission, failure of equipment or any other force majeure (e.g. war or earthquake), or other circumstances not attributed to TWCA, TWCA shall be free from any liability for indemnifying such loss.
- TWCA 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 certificate data of subscribers as a result of the failure to keep such data in custody with due faith and due care of TWCA.
- After receiving a request of certificate revocation, TWCA shall finish revoking the requested certificate within one workday and issue and complete publishing the CRL to the repository within one day from the revocation. Prior to the publication of the status of certificate revocation, subscribers shall take actions appropriate to minimize the effect on the relying parties of their certificates, and shall be fully liable for the consequences of the use of such certificates.

9.8 Limitation of Liability

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

9.9 Indemnities

Subject to Section 9.2.1.

9.10 Term and Termination

9.10.1 Term

This CPS shall be effective after being approved by the competent authorities according to the Electronic Signatures Act and published by TWCA 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 Users

TWCA will establish contact channels with subscribers with appropriate methods. These will include, but are not limited to, telephone, fax or contact-mail.

9.12 Amendments and Publications

9.12.1 Procedure for Amendment

This CPA shall be approved by TWCA PMA according to the Electronic Signatures Act, Enforcement Rules of the Electronic Signatures Act, Regulations on Required Information for Certification Practice Statements and the code of management related to CA and by the competent authorities.

The Policy Management Administration (PMA) of TWCA shall review the CPS once a year to ensure if it complies with the security specifications in international standards, the code of operation of the competent authorities, the framework and functional adjustment of the certification management system, the suitability of business system requirements, in order to make constant amendments, updates or adjustments according to the business requirements, international standards, user suggestions and known errors.

Unless otherwise specified, this CPS or its updates shall be validated when posted on the TWCA website after the PMA review and approval of the competent authorities. Users may download the latest version from our website at https://www.twca.com.tw.

9.12.2 Amendments Notification Mechanism

When updates to this Practice Statement are proposed, detailed related documents shall be submitted by mail or email to the contact point specified in Section 1.5.2, for review by the TWCA Policy Management Authority.

9.12.3 Circumstances Under Which OID Shall 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 Procedures

According to the description of this CPS, the dispute resolution procedures or dispute arbitration procedures incurred from problems about the public or private key are covered by the General Provisions. Disputes arising from or in connection with other businesses shall be subject to the code of operations of individual businesses.

Both parties shall endeavor to reasonably resolve any disputes with due faith.

If the disputing parties are unable to reasonably resolve a dispute within 14 days, they shall initiate a negotiation and appoint a qualified and competent third party to be the mediator to mediate and resolve the dispute. Both parties shall agree to the mediation and resolution made by the mediator.

If the disputing parties do not accept the mediation and resolution made by the mediator and reasonably resolve the dispute within one month, both parties may refer the dispute to the Taipei District Court of Taiwan to seek resolution through litigation.

Subscribers , RAs and TWCA shall agree to resolve disputes between users and RAs or users and TWCA with due faith through negotiations and that the Taipei District Court of Taiwan shall be the jurisdiction court for the first instance of any disputes requiring a resolution through litigation.

RAs and TWCA shall agree to resolve disputes with due faith through negotiations and that the Taipei District Court of Taiwan shall be the jurisdiction court for the first instance of any disputes requiring a resolution through litigation.

All parties shall agree to share the cost incurred from the negotiation or litigation of any disputes through negotiations or the relevant laws and regulations.

Transnational or transborder disputes that cannot be resolved through the above methods shall be resolved according to the relevant transnational or transborder dispute arbitration process.

9.14 Governing Law

This CPS is established according to the relevant laws and regulations of the government and within the jurisdiction and governance of the relevant laws and regulations of the Republic of China, including the relevant laws and regulations of the competent authorities, such as the Electronic Signatures Act, Enforcement Rules of the Electronic Signatures Act and the Regulations on Required Information for Certification Practice Statements. When transnational or transborder business integration is required, apart from the regulations governing business integration, the relevant laws of the Republic of China shall be the governing law.

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.

This Practice Statement and the Certificate Authority shall comply with the provisions of the Electronic Signature Act and its Enforcement Rules of this country..

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Survival

When it is needed to revise some clauses of this CPS when they are obsolete, other clauses remain valid and unaffected by those obsolete clauses. When the revision of the CPS is completed and published, those obsolete clauses shall be updated according to Section 1.5 of this CPS.

When the relationship of subscribers and relying parties have expired or been interrupted for whatever reasons, the rights and obligations of the relevant users within this CPS are still valid and shall not be invalidated following the termination of such relationship. For example, when a user applies for a cancellation of the relevant business relationship to a bank after using the user certificate in the transfer system of that bank's network banking system, the relevant rights and obligations of that user and that bank are still valid due to the transaction and shall not be invalidated as this relationship is terminated.

According to this CPS and the regulations of the relevant businesses, the notification between the UCA and users or RAs shall be delivered by the following methods:

- Electronic messages:

  The sender shall sign the message with the electronic signature before sending it to the recipient. The recipient shall verify the signature when receiving the message.

- Paper documents:

  The name and mailing address of the relevant operators of the sender and recipient shall be indicated in the documents and forms. Documents shall be delivered by mail to the recipient 3 days in advance (7 days in advances for overseas recipients). When delivering such documents by fax, apart from the detailed contact information of both the sender and the recipient, the detailed fax ID and the signature of the relevant personnel shall be required.

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

This CPS is amended according to Section 9.12.

9.16.4 Enforcement

No stipulation.

9.16.5 Act of God

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

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

(4). Encrypt/Encipher

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

(5). Decrypt/Decipher

It refers to the reduction of an encrypted or enciphered message that is unable to be identified or interpreted 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 (Encryption System)

It refers to a computer-based mathematical algorithm for generating and using a mathematically 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 transfer a long message (containing many bytes) into a fixed size message. The output of the same message after compression function computing shall 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 Authority (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.

(15). Elliptic Curve Cryptography (ECC)

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

(16). ECC P-256 Curve

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

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
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standard
ISO/IEC	the International Organization for Standardisation, 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