Taiwan-CA Inc.
Certification Practice Statement

Version 2.3

臺灣網路認證股份有限公司
TAIWAN-CA INC.

Effective Date: 23 July 2010

Revision History

Version	Effective Date	Released by	Remarks
Ver. 1.0	20 Mar 2000	TaiCA	First release.
Ver. 1.1	1 Mar 2002	TaiCA	Revised according to the integration of TaiCA CA PKI system documents (CPS, CP, etc.) and the EDI (PAA CP) of Trade-VAN.
Ver. 1.2	4 Nov 2002	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) Commercial 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 09102245130.
Ver.1.3	18 Feb 2005	TWCA	1. Revised according to the addition of the electronic stock-affairs certificate, on-line insurance certificate, and certificate multipurpose operations. 2. Revised the applicability of certificate and transaction amount limit. 3. The term Certificate 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	4 Mar 2008	TWCA	1. Deleted the Enterprise EC Certificate section after the service is terminated. 2. Revised Certification Authority to User Certification 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	12 Nov 2008	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	14 Jul 2009	TWCA	1. Added the applicability of online patent/trademark application. 2. Rhetoric changes.
Ver 2.3	23 Jul 2000	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.

Contents

Certification Practice Statement (CPS)

1. Important Statements of Using Certificates

1.1 Approved by Ministry of Economic Affairs

The Certification Practice Statement (CPS) of Taiwan-CA Inc (TWCA) specifies the regulations for managing the following legally established Certificates Service Providers (CSP): (1) Network Banking Certification Authority (NBCA), (2) Commercial EC Certification Authority (EC+) and (3) Commercial XML Certification Authority (CXMLCA), including the issuance, revocation, management and renewal of certificates.

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

Letter Jing-Shang-Zi 09902081770, Ministry of Economic Affairs, dated 23 July 2010.

1.2 Certificates Level of Assurance and Applicability

Types of certificates:

	Types of Certificates	Level of Assurance	Applicability	Note
1	NB Certificate	Level 3	e-Banking transfer, online order transactions, online electronic information security control, online tax declaration, e-invoice and e-voting.	
		Level 2	e-Commerce applications.	
2	EC+ Certificate	Level 3	Online order transactions, financial transactions, e-commerce applications, online tax declaration, e-invoice and e-voting.	
		Level 2	SSL server certificates and information security control.	
3	CXML Certificate	Level 3	Financial transactions, securities transactions, e-commerce applications, online identity verification, online tax declaration, e-invoice, e-voting, online patent/trademark applications, and issue, transaction and application of short-term bill.	
		Level 2	e-Commerce applications, online identify authentication and e-mail applications.	
		Level 1	e-Commerce applications and online	

			identity verification.	
Note: See “Certificate’s Applicability 2.2”, for the details of the level of assurance of certificates. See “Table (1), 2.2.1.2”, for details of the scope using and liability of certificates.				

1.3 Important Statements of Using Certificates

TWCA has been awarded the ISO27001:2005 Certificate in September 2007 and continuously operates the ISO27001:2005 Information Security Management System (ISMS). TWCA also hires private law firms or CPA firms to conduct external audits to ensure its operations meet the requirements of the CPS and the Certification Policy (CP).

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 and/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 shall not disclose and/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. Subscribers 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 subscribers shall have full liability for the damage that is caused.

Liability

When employees of TWCA cause damage to subscribers out of negligence as a result of processing subscriber registration, certificate issuance, certificate suspension and/or 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 “Scope of Using and Liability, Clause 2.2.1.2.” When such damage is caused by TWCA employees out of deliberation or gross negligence, TWCA shall be in full liability for the actual damage that 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 subscriber 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 or the relevant operating procedures

2. Introduction

2.1 Overview

In order to build a secure and reliable network environment where no fabrication, alteration and/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 subscribers 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) and various excellent IT corporations.

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.

2.2 Certificate’s Applicability

2.2.1 Certificate’s Applicability and Liability

2.2.1.1 Level of Assurance

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

(1) Class 1

1. Identity authentication
   The user certification authority (UCA) or RA only conducts limited verification of the user account (ID, such as personal name, registered company name or universal resource location (URL)) and e-mail account through simple procedures.

2. Level of assurance
   The UCA and RA only assure the uniqueness of the user account and e-mail account in the database, and all other information related to the user is considered as unverified.

3. Applicability
   Allows subscribers to send electronic documents by e-mail or protect their own electronic documents; except for business transactions required identity verification.

(2) Class 2

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

2. Level of assurance
   The UCA and RA only assure the uniqueness of the user account and e-mail account in the database, as well as general verification of the relevant subscriber information instead of assurance for absolutely correct subscriber information.

3. Applicability
   It is recommended to use in enterprise intranets, non-financial or non-securities small amount e-commerce transactions or encryption for data transmission.

(3) Class 3

1. Identity authentication
   Apart from checking the information specified in Class 2, the subscriber shall personally apply for the registration. A legal person or corporate subscriber shall apply for registration through an agent holding valid authorization documents and documents that can identify his/her identity (e.g. citizen identity card or passport with a photo of the agent).

2. Level of assurance
   Identity verification higher than the Class 2 certificate is provided through various strict operating procedures to greatly enhance the certificate reliability of subscribers and trustees.

3. Applicability
   It is recommended to use in financial or securities transactions.

(4) Testing certificates

1. Identity authentication
   Testing certificates are intended for testing purpose and neither the UCA nor the RA will run any identity authentication. Therefore, they cannot be used in any applications or businesses.

2. Level of assurance
   No assurance will be made by the UCA or RA.

3. Applicability
   Used by UCA-authorized subscribers for testing only. No use in any applications or businesses other than testing is allowed.

2.2.1.2 Scope of Using and 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 [Level 3 identify verification].[Single usage].[Held by natural person].[For use in financial transactions].

Part 1 [Level of Assurance]	Part 2 [Usage]	Part 3 [Subscriber status]	Part 4 [Business Category]
1. Class 1 2. Class 2 3. Class 3 0. Testing Certificate	1. Single usage 2. Multi-usage in limited category	1. Legal person 2. Natural person 3. Others	1. Financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting and issue and transaction of short-term bills and securities 2. Securities transactions, e-commerce applications, online tax declaration, e-invoice and e-voting 3. e-commerce applications, online identity verification, online tax declaration, e-invoice, e-voting, online patent/trademark application and e-mail applications

1. Part 1: Level of assurance
It falls into 3 classes: (1) Class 1, (2) Class 2, (3) Class 3, and (0) Testing Certificates. The security level is subject to the registration status of subscribers. Please refer to “Level of Assurance, Clause 2.2.1.1” 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 between TWCA and the subscriber or the publishing of TWCA. The followings are the code of limited usage:

a. FXML: For certificate holders to transact with TWCA-approved RAs. However,

certificate holders shall register to counterparty of transactions in advance. Banks are the original RAs of FXML certificates.

b. EC: For certificate holders to transact with TWCA-approved RAs. However, certificate holders shall register to counterparty of transactions in advance, and the transaction shall be limited to online e-commerce transaction.

c. 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: Subscriber status

It falls into (1) legal person, (2) natural person, and (3) others.

(4) Part 4 : Business Category

Business category falls into (1) financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, issue and transaction of short-term bills and securities; (2)securities transactions, e-commerce applications, online tax declaration, e-invoice and e-voting; (3)e-commerce applications, online identity verification, online tax declaration, e-invoice, e-voting and online patent/trademark application, e-mail applications. Certificates for use in financial transactions can also be used in securities transactions, e-commerce applications and online identity verification when they conform to the requirements of the scope of use or approved by TWCA.

Ex. The class code of current EC for network banking is 3.1.1.1, representing:
(3): Class 3 assurance level
(1): Single usage
(1): Legal person
(1): For use in financial transactions

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

1. Transaction amount limit: Different transaction amount limits 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 transaction amount limit of that class code.

2. Indemnity amount limit: Different indemnity amount limits are set according to the level of assurance, usage, and subscriber status of certificates. This limit refers to the maximum amount of indemnity indemnified for a single certificate of subscribers. That is to say, regardless of the counts of transaction, the accumulative amount of indemnity shall not exceed the indemnity amount limit.

3. When a subscriber and TWCA have signed a contract where transaction amount limit, indemnity limit and scope of use are specified individually, the transaction amount limit, indemnity limit and usage of the certificate held by this subscriber shall be subject to the contract terms.

4. Multi-usage in limited category: The scope of use of a subscriber certificate shall be subject to the contract signed between the subscriber and TWCA or the relevant management regulations 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	Business Category	Transaction Amount Limit	Indemnity Amount Limit
1.1.1.3	Class 1	Single Usage	Legal person	e-Commerce applications, online identity verification	3,000	3,000
1.1.2.3	Class 1	Single Usage	Natural person	e-Commerce applications, online identity verification	3,000	3,000
1.1.3.3	Class 1	Single Usage	Other	e-Commerce applications, online identity verification	3,000	3,000
2.1.1.3	Class 2	Single Usage	Legal person	e-Commerce applications, online identity verification, e-mail applications	900,000	300,000
2.1.2.3	Class 2	Single Usage	Natural person	e-Commerce applications, online identity verification, e-mail applications	300,000	100,000
2.1.3.3	Class 2	Single Usage	Other	e-Commerce applications, online identity verification, e-mail applications	900,000	300,000
3.1.1.1	Class 3	Single Usage	Legal person	Financial transactions	Unspecified	2,000,000
3.2.1.1	Class 3	Multi-usage in limited category	Legal person	Financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, issue and transaction of short-term bills and securities	Unspecified	2,000,000
3.1.2.1	Class 3	Single Usage	Natural person	Financial transactions	Unspecified	300,000
3.2.2.1	Class 3	Multi-usage in limited category	Natural person	Financial transactions, e-commerce applications, online tax declaration, e-voting, issue and transaction of short-term bills and securities	Unspecified	300,000
3.1.1.2	Class 3	Single Usage	Legal person	Securities transactions	100,000,000	2,000,000
3.2.1.2	Class 3	Multi-usage in limited category	Legal person	Securities transactions, e-commerce applications, online tax declaration, e-invoice, e-voting	100,000,000	2,000,000
3.1.2.2	Class 3	Single Usage	Natural person	Securities transactions	15,000,000	300,000
3.2.2.2	Class 3	Multi-usage in limited category	Natural person	Securities transactions, e-commerce applications, online tax declaration, e-voting	15,000,000	300,000
3.1.1.3	Class 3	Single Usage	Legal person	e-Commerce applications, online identity verification, online patent/trademark application	20,000,000	2,000,000
3.2.1.3	Class 3	Multi-usage in limited category	Legal person	e-Commerce applications, online identity verification, online tax declaration, e-invoice, e-voting	20,000,000	2,000,000
3.1.2.3	Class 3	Single Usage	Natural person	e-Commerce applications, online identity verification, online patent/trademark application	2,000,000	300,000
3.2.2.3	Class 3	Multi-usage in limited category	Natural person	e-Commerce applications, online identity verification, online tax declaration, e-voting	2,000,000	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.

2.2.1.3 Using and Prohibition

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 in issued certificates, 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.

A. NBCA system

Certificates issued by TWCA with the term “Test” specified in the CN column under the issuer DN (Issuer Distinguished Name) are testing certificates, and TWCA assumes no liability resulting from the use of such certificates.

Certificates issued by TWCA with the term “NBS”, “NSS”, “ERS”, “VOT”, “INS”, “ECB” or “TCA” specified at the beginning of the CN column under the issuer DN (Issuer Distinguished Name) are NB certificates.

〈”O” is the abbreviation of the first letter of “OrganizationName”; “OU” is the abbreviation of “OrganizationUnitName”; and “CN” is the abbreviation of “CommonName”〉

(1) If the SubjectType (subject type) in the third sub-column under SubjectAltName (subject alternative name) in the NB certificates issued by TWCA is not “B1” (Binary 10000000), these certificates are held by legal persons; e.g. “SubjectType = B1”.
(2) If the SubjectType (subject type) in the third sub-column under SubjectAltName (subject alternative name) in the NB certificates issued by TWCA is “B1” (Binary 10000000), these certificates are held by natural persons.
(3) If the CN column under the issuer DN in the NB certificates issued by TWCA begins with “NBS”, the scope of use and liability of these certificates are “Class 3.1.1.1”, “Class 3.1.2.1”, “Class 3.2.1.1”, or “Class 3.2.2.1”.
(4) If the CN column under the issuer DN in the NB certificates issued by TWCA begins with “NSS”, the scope of use and liability of these certificates are “Class 3.1.1.2 “, “Class 3.1.2.2”, “Class 3.2.1.2” or “Class 3.2.2.2”.
(5) If the CN column under the issuer DN in the NB certificates issued by TWCA begins with “ERS”, the scope of use and liability of these certificates are “Class 3.1.1.3”, “Class 3.1.2.3”, “Class 3.2.1.3” or “Class 3.2.2.3”.
(6) If the CN column under the issuer DN in the NB certificates issued by TWCA begins with “VOT”, the scope of use and liability of these certificates are “Class 3.2.1.3” or “Class 3.2.2.3”.
(7) If the CN column under the issuer DN in the NB certificates issued by TWCA begins with “INS”, the scope of use and liability of these certificates are “Class 3.2.1.3” or “Class 3.2.2.3”.
(8) If the CN column under the issuer DN in the NB certificates issued by TWCA begins with “ECB”, the scope of use and liability of these certificates are “Class 3.2.1.3” and “Class 3.2.2.3”.
(9) If the CN column under the issuer DN in the NB certificates issued by TWCA begins with “TCA”, the scope of use and liability of these certificates are “Class 3.2.1.3” or “Class 3.2.2.3”.

B. EC+ system

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 subject DN column are held by legal persons; e.g. “CN=TW1674277416742774”. EC certificates issued by TWCA with the “Citizen Identity Card

Number" specified in the CN column under the subject DN column are held by natural persons; e.g. "CN=TWH14520147801".

(1) EC certificates issued by TWCA with the "Bank English Name" specified in the "OU" column under the subject DN column; e.g. "OU=Cathay United Bank", the scope of use and liability of these certificates are "Class 3.1.1.1", "Class 3.1.2.1", "3.2.1.1" or "3.2.2.1".
(2) EC certificates issued by TWCA with the "Securities Company English Name" specified in the "OU" column under the subject DN column; e.g. "OU=DASHIN SECURITIES CO. LTD.", the scope of use and liability of these certificates are "Class 3.1.1.2, "Class 3.1.2.2", "3.2.1.2" or "3.2.2.2".
(3) 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 subject 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".

Certificates issued by TWCA with "CN=TaiCA Secure CA,OU=SSL Certification Service Provider,O=TAIWAN-CA.COM Inc.,C=TW" specified in the issuer DN (Issuer Distinguished Name) column are SSL server certificates.

SSL certificates issued by TWCA with the "URL" specified in the CN column under the subject DN column are SSL server certificates; e.g. "CN=WWW.TAICA.COM.TW".

The scope of use of these SSL certificates includes only the encryption of data transmitted among websites. The transaction amount limit of these certificates are NT$10 million, and the indemnity amount limit is NT$2 million.

C. CXML Certificate system

(1) 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 CXML certificates.

CXML certificates issued by TWCA with the "Company Uniformed Tax Code" specified in the CN column under the subject DN column are held by legal persons; e.g. "CN= 16742774-16-A742774". CXML certificates issued by TWCA with the "Citizen Identity Card Number" specified in the CN column under the subject 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", "Class 3.2.2.3", "Class 3.2.1.1" or "Class3.2.2.1".

(2) Certificates issued by TWCA with "CN=TaiCA Finance User CA,OU=User CA,O=TaiCA,C=TW" specified in the issuer DN column are tariff certificates.

Tariff certificates issued by TWCA with the "Company Uniformed Tax Code" specified in the CN column under the subject DN column are held by legal persons; e.g. "CN= 16742774-16-A742774". Tariff certificates issued by TWCA with the "Citizen Identity Card Number" specified in the CN column under the subject 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", "Class 3.1.2.1", "Class 3.2.1.1" or "Class3.2.2.1".

(3) Certificates issued by TWCA with "CN=TWCA SMIME User CA,OU=User CA,O=TAIWAN-CA Inc.,C=TW" specified in the issuer DN 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 subject DN column, e.g. "CN= SMIME5678-00-000001", are "Class 2.1.1.3", "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 "the Certificate's Applicability, Clause 2.2."
(2) Limits on certificate applicability: Both the subscribers and relying parties of 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 counterparties, and the corresponding transaction amount limit specified in Table 1.
(3) In a transaction, both the subscribers and relying parties of certificates 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 customers 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, Clause 2.2.1.2, for details of the transaction amount limits and indemnity amount limits of certificates.)

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

("DN" represents "Distinguished Name". The first letter in the column is an abbreviation, e.g. "OU" is the abbreviation of "Organization Unit Name".)

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

<2> 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 relying party is restricted to the first authorized relying party described in the first organization unit name (OU) under the Subject DN. The holder of this certificate is an individual subscriber (natural person). The certificate is for use in securities transactions.

<3> 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 must first register to the transaction counterparty. The holder is an enterprise subscriber (legal person). The certificate is for use in financial transactions.

<4> 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 relying party is restricted to the second authorized relying party described in the first organization unit name (OU) under the Subject DN. The holder of this certificate is an enterprise subscriber (legal person). The certificate is for use in e-commerce applications or online identity verification.

<5> 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 holder must first register to the transaction counterparty. The holder is an individual subscriber. The certificate is for use in securities transactions.

☆ **Prohibitions of certificate uses: Certificates shall be used and only be used in the said scope of uses, and shall not be used in**: (1) the scope of uses not specified in the CPS, (2) application 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) applications or businesses prohibited in the laws and regulations related to the Electronic Signatures Act and by the competent authorities.

2.3 Identification

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

(1) NB certificates
OID=2.16.886.3.1.1.5

(2) EC+
OID=2.16.886.3.1.3.1

(3) CXML certificates
OID=2.16.158.3.1.8.5

2.3.1 Standards

This CPS is edited and complied according to the following standards:

(1) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF PKIX RFC 3647 November 2003.
(2) Regulations on Required Information for Certification Practice Statements, Ministry of Economic Affairs, 7 July 2004.
(3) PKI Certification Policy V1.5, TWCA.

2.3.2 Definition

Please refer to the Glossary for details of the terms and their meanings that are used in this CPS.

Prior to reading this CPS, subscribers are advised to understand the PKI (public key infrastructure) operation concepts below.

(1) The digital signature is used in the authentication of identity and transaction messages, the integrity of messages, and the non-repudiation of the sending or receiving of transaction messages.
(2) The cryptosystem for message confidentiality, such as symmetric or asymmetric cryptosystems.
(3) Asymmetric cryptosystem: public/private key pairs and public key certificate; e.g. digital signature and digital envelope mechanisms.
(4) The operability of CA and RA under the PKI hierarchical framework.

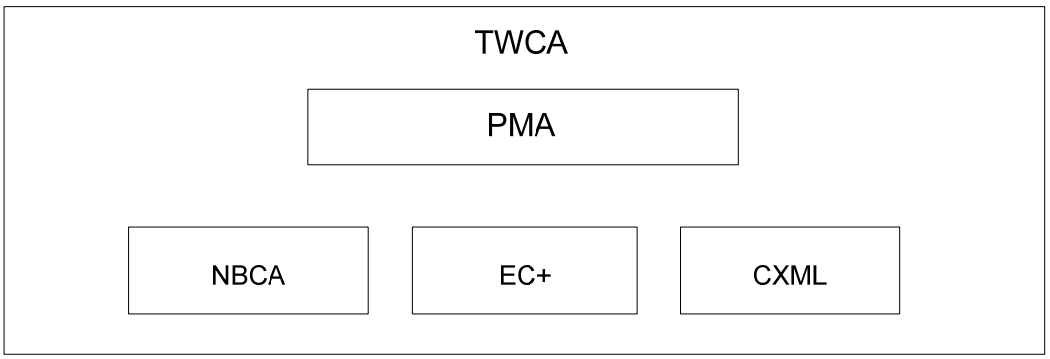
2.4 Community and Applicability

2.4.1 TWCA Certificates Service Provider

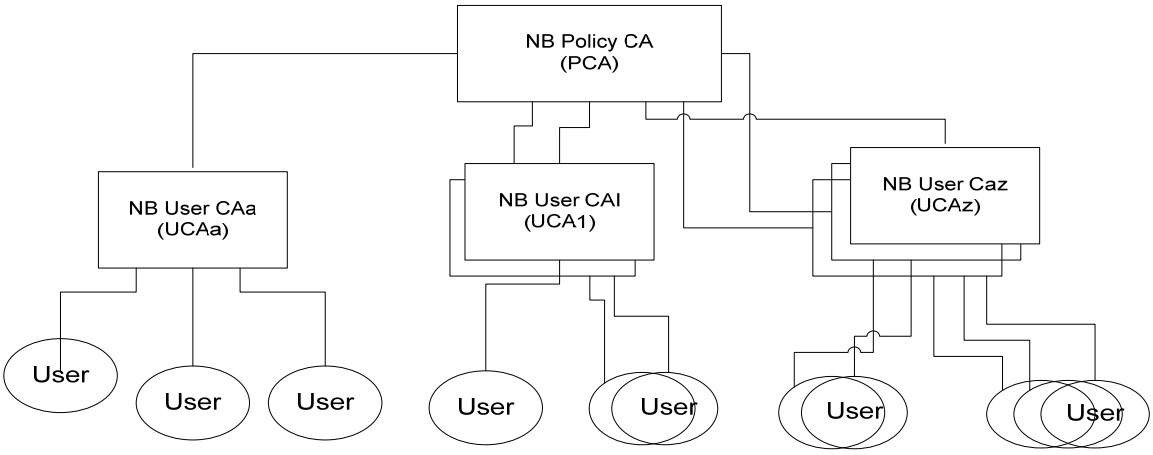
TWCA is an authority issues and manages the following types of certificates: (1) NB certificates, (2) EC+ certificates, and (3) CXML certificates.

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.

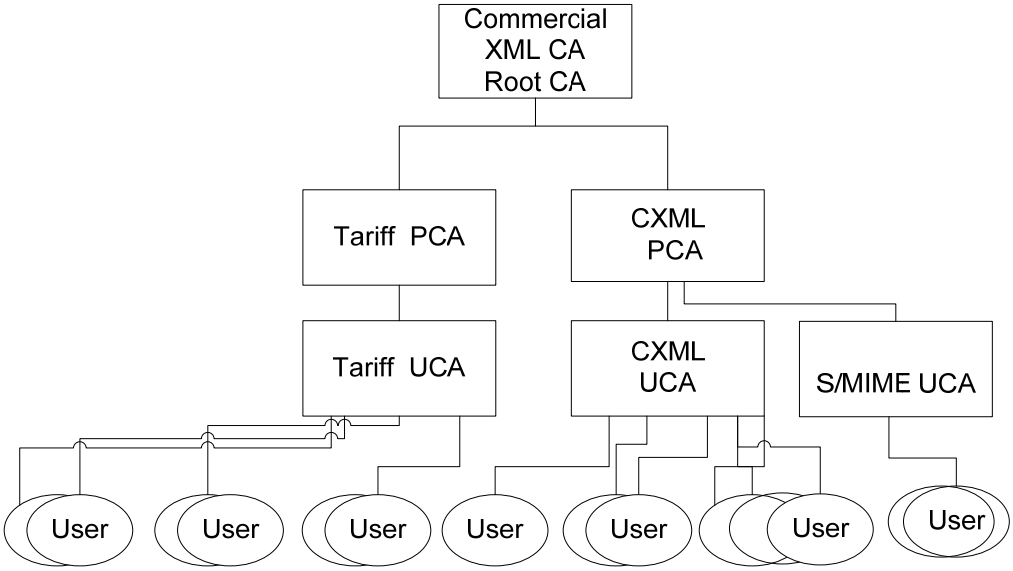
1. The PKI framework and specifications of the Root Certification Authority (RCA), Policy Certification Authority (PCA) and User Certification Authority (UCA).
2. The CP and CPS.
3. The contents of certificates and revoked certificates.
4. The code of operations and procedures of transnational certificate PKI cross certification.



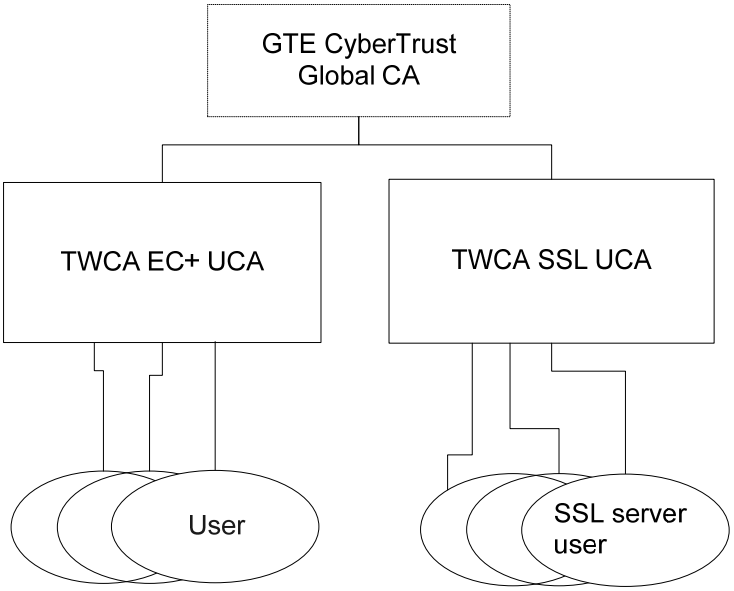
(1) NBCA


NB Policy CA
(PCA)
NB User CAa
(UCAa)
NB User CAI
(UCA1)
NB User Caz
(UCAz)
User
User
User
User
User
User
User

(2) CXML


Commercial
XML CA
Root CA
Tariff PCA
CXML
PCA
Tariff UCA
CXML
UCA
S/MIME UCA
User
User
User
User
User
User
User

(3) EC+



2.4.2 Root Certification Authority (RCA)

- 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 PCA certificates and CRLs.
- Implemented in an independent operating environment with security control where public keys are generated and implemented by at least 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.

2.4.3 Policy Certification Authority (PCA)

- 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 CAs.
- Issues, manages and delivers the CA certificates and CRLs.

2.4.4 User Certification Authority (UCA)

- Follows the instructions established by the PCA.
- Manages and publishes the operating procedures and verification code of operations of subscriber registration, certification and CRLs.
- Accepts the application, renewal, suspension, revocation, access and registration of subscriber certificates.
- Issues, manages and delivers the RA and subscriber certificates, CRLs and subscriber information.

2.4.5 Registration Authority (RA)

An RA manages the UCA registration:

- Selects quality financial institutions or relevant units as RAs; these RAs shall process subscriber registration after signing a contract with TWCA.
- A department dedicated to the registration affairs shall be established.

- Manages and publishes the operating procedures and identity verification code of operations of applications for subscriber registration.
- Verifies the application messages in subscriber registration, certificate issue and revocation, and certificate access; the authenticity of identity and the veracity of messages.
- Delivers the messages of application for subscriber registration, certificate revocation and certificate access to the UCA.
- Processes the certificate registration, certificate application and certificate revocation; and sends reply to subscribers 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.

2.4.6 Repository Authority (RA) or Directory Authority (DA)

- A repository authority or directory authority is a certificate chain managing and publishing certificates, CRLs and allowing subscribers to access to such by means of a directory server or database.
- Manages and publishes the operating procedures and code of operations for identity verification and message security controls for accessing the directory server.
- Manages and publishes the operating procedures and code of operations for identity verification and message security controls for accessing the directory server with online certificate status protocol (OCSP).
- Verifies the identity authenticity and the validity of the message enquired and sends the correct message to subscribers when subscribers making an enquiry.
- Publishes and manages the registration name, URL, e-mail account and contact information of the repository authority or directory authority.

2.4.7 End Entities

2.4.7.1. Subscribers

Subscribers are the holders of certificates issued by the UCA. They include natural persons; legal persons of profit or non-profit businesses; government agencies; financial group legal 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 legal 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.

2.4.7.2. Relying 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 of others (recipients) and sending message to the recipients after encryption to ensure the message confidentiality of both parties.

2.4.8 Policy Management Authority (PMA)

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

1. CP
2. CPS
3. Code of operations

2.4.9 Applicability

Subscribers shall legally and correctly use the private key of certificates specified and issued according to this CPS according to the regulations specified in this CPS and the business application system instructions. Also, subscribers shall not use the private key of these certificates in (1) the scope of uses not specified in the CPS, (2) application 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) applications or businesses prohibited in the laws and regulations related to the Electronic Signatures Act and by the competent authorities. Otherwise, the subscribers shall have full liability for the damage that is caused.

2.4.9.1 Risk and security

The reliability of the public key system of certificates relies on the uniqueness of the public and private keys of the certificate issuing systems, the verifiability of identity, the security of physical facilities and equipment (including hardware and software), the rigor of security control of personnel operating procedures, and the security of information transmission over the Internet.

When selecting the public key for the application system, it is necessary to consider the security problems as well as the risk level of man-induced damage of the internal and external environments and the threat of natural disasters. Security controls appropriate to the security level of application systems shall be established. In the following sections of this CPS, the code of operations and security controls of the TWCA public key certification service system will be described in detail.

2.5 Contact Details

2.5.1 Specification Administration Organization

The Policy Management Authority (PMA) of TWCA shall be the unit responsible for the establishment, amendment and publishing of the CPS.

2.5.2 Contact Person

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

Subscribers 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	10th Floor, 85 Yen-Ping South Road, Taipei, Taiwan 100, R.O.C
Phone	886-2-23708886
Fax	886-2-23700728
E-mail	ca@twca.com.tw
URL	http://www.twca.com.tw

2.5.3 Person Determining CPS Suitability for the Policy

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

3. General Provisions

3.1 Obligations

3.1.1 CSP Obligations

- To establish, publish and manage the CPS and CP within the scope of certification and the code of operations related to certificate operations.
- 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 ensure that the selection of certification system operators (including outsourced personnel) and system operations conform to the CPS.
- Operators shall take due care of the registration and certificate data and the relevant information of subscribers and avoid the leaking, identity fraud, alteration and unauthorized use of the relevant information.
- To accept the certificate application, certificate renewal, certificate suspension, certificate revocation, certificate access and certificate registration of subscribers (RA) according to the CPS; ensure the veracity and integrity of transaction data delivered from the RA and subscribers to the UCA; issue certificates; and correctly and securely deliver the relevant reply messages to subscribers.
- To correctly and securely deliver the subscriber certificates and TWCA CRLs to the repository according to the CPS when offering the DA service.
- To specify in the contracts signed with subscribers and/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.
- The private signature key of UCA shall only be used in the issue and revocation of subscriber certificates. A different and independent private key shall be used for information encryption or other signature purposes.

3.1.2 RA Obligations

- To ensure the rights and obligations of RAs and subscribers according to this CPS, CP and RA code of operations; and to verify the authenticity and integrity of application information in processing subscriber identity verification, certificate application, certificate renewal, certificate suspension, and certificate revocation.
- To ensure that the selection of certification system operators (including outsourced personnel) and system operations conform to the CPS and the code of operations of the RA.
- 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; subscribers (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 subscribers to sign the relevant documents according to the code of operations corresponding to the level of assurance of their registration status.
- To accept the user’s application for registration and cancellation of registration, certificates, certificate renewal, certificate suspension, certificate access and certificate revocation.
- To verify the authenticity and veracity of subscriber 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 subscribers the correct messages replied from the UCA.
- RAs shall take due care to retain the registration data and the relevant information of subscribers and avoid leaks, identity fraud, alteration and unauthorized use of the relevant information.
- To specify in the contracts signed with subscribers and/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/or 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.
- The RA shall be responsible for subscriber registration and management. The UCA shall be responsible for the issue and management of certificates entrusted by the RA. The RA shall provide the subscribers and relying parties the information concerning the above rights and obligations.

3.1.3 Repository Obligations

- To ensure the rights and obligations of repository authority and subscribers and TWCA; and to enquire information and carry out security controls related to subscriber certificates.
- To immediately update the database and inform subscribers of the latest information according to the subscriber 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 subscribers the correct information enquired when subscribers enquire information to the directory server or database; unauthorized subscribers shall not access to other information stored in other repository, except for the information of certificates and CRLs which are open to sunscriber access.
- Both the repository and its operators shall take due care of the registration and certificate data and other information of subscribers and avoid the leaking, identity fraud, alteration and/or unauthorized use of the relevant information.
- In doubts of security, such as identity fraud, exposure and/or 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.

3.1.4 Subscriber Obligations

- To provide detailed and correct documents and data of identity when applying for registration to the RA.
- 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.
- To properly and securely generate and protect the private key and PIN according to this CPS; and to ensure that either the key or the PIN is known or used by any party.
- To verify the authenticity of subscribers and UCA and the integrity and validity of certificate information when accepting the subscriber certificate issued by TWCA.
- To understand and agree to the CPS and relevant code of operations; to legally and correctly use the private key and certificate in the relevant business systems; and to ensure such uses shall neither violate any relevant laws and regulations nor infringe the rights of any third party.
- In doubts of security, such as identity fraud, exposure and/or loss of the private key corresponding to certificates, or when there is a change of the information related to the subscriber in the certificate or desire to stop using the certificate, subscribers shall immediately report to the RA according to the relevant regulations.

3.1.5 Relying Party Obligations

- The replying party shall understand and agree to the CPS and the code of operations and the rights and obligations of the business systems that are used. It shall also ensure that the certificate is used within the scope of use specified in the certificate and the relevant business systems specified in this CPS, and such uses shall neither violate any relevant laws and regulations nor infringe on the rights of any

third party.

- The authenticity and validity of certificates shall be verified by the certificate chain according to the CPS, the regulations of the relevant application and business systems, and the X.509 certificate standards. When the CRL security mechanism is present, the status of certificates, i.e. either revoked or suspended, shall be cleared.
- The relying party shall verify the validity of transaction messages. Apart from the validity and authenticity of certificates, the replying party shall verify the transaction amount limit, liability amount limit, business category and liability of certificates according to the CPS and the regulations of the relevant business systems.

3.2 Liability

The certification service items and contents provided by TWCA are specified in "Certificate's Applicability, Clause 2.2." Service contents not specified in this CPS, such as the transaction systems that used by subscribers and replying parties, shall not be covered in the liability specified in this CPS.

3.2.1 TWCA CA Liability

- TWCA assumes no liability for any damages, except for damage caused to subscribers as a result of failure to follow this CPS, the CP, and the relevant code of operations when processing subscriber registration data or issuing certificates that are considered as negligence.
- 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.
- When employees of TWCA cause damage to subscribers out of negligence as a result of processing subscriber registration, certificate issuance, certificate suspension and/or 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 "Scope of Use and Liability, Clause 2.2.1.2." When such damage is caused by TWCA employees out of deliberation or gross negligence, TWCA shall be in full liability for the actual damage that is caused to the corresponding subscribers.
- After a certificate subscriber 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, TWCA 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.
- TWCA shall be free from any liability for the damage incurred from the use of illegally faked or incorrect certificates that are not attributable to TWCA.
- The validity for claiming indemnity shall be subject to the regulations of the competent authorities or the relevant laws.

3.2.2 RA Liability

- RAs shall take due care of the registration data and the relevant information of subscribers and avoid leaks, identity fraud, interpolation and unauthorized use of the relevant information. When employees of RAs cause damage to subscribers or others as a result of processing subscriber registration and relevant information or errors occurred from the application for subscriber certificates to the UCA, RAs and their employees shall be in full liability for the direct damage that caused to the corresponding subscribers.
- When employees of RAs cause damage to subscribers out of deliberation or negligence during processing subscriber registration, certificate issuance, certificate renewal, certificate suspension

and/or certificate revocation without following the CPS and other relevant RA operating procedures and regulations or by violating the relevant laws and regulations, RAs shall indemnify the direct damage of subscribers as specified.

- RAs shall be free from any liability for the damage incurred from the use of illegally falsified or incorrect certificates that are not attributable to RAs.
- After a certificate subscriber 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.

3.2.3 Subscriber Liability

- Out of deliberation, negligence and/or indecent intentions, subscribers shall be in full liability for indemnifying RAs, TWCA and/or a third party for the damage incurred from 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 and/or lend them to another party. Out of either deliberation or negligence, subscribers shall be in full liability for indemnifying the damage that caused to RAs, TWCA and/or a third party.
- After a certificate subscriber 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, subscribers 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. When that certificate is used in illegal transactions or there are disputes arising out of or in connection with the transactions made with that certificate, if TWCA and RAs process the request according to the CPS and the relevant code of operations, the relying party shall be in full liability for the damage that caused. During the request of certificate revocation or suspension, if subscribers 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 subscriber shall be in full liability 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 subscriber shall have full liability for the damage caused.

3.3 Financial Responsibility

TWCA shall hire an impartial and objective third party to conduct a financial audit for the certification business every year.

Apart from the earthquake and fire insurance for the building and hardware facilities in and by which certificate management is operated, TWCA is making contact with the relevant insurance companies at home and abroad to apply for the certification business liability insurance in order to disperse the risk of operations. Also, TWCA has appropriated NT$30 million as a financial guarantee for the liability arising out of or in connection with the implementation of certification businesses prior to applying for such insurance in order to protect the rights and benefits of subscribers.

3.3.1 Indemnification by Relying Parties and Subscriber

When it is not the remissness of either TWCA or RAs, TWCA or RAs shall enjoy the immunity of liability for the financial, reputational and/or other damage that caused to a third party out of either the

deliberation or negligence of the relying party or subscriber.
The relying party or subscriber shall be in full liability for financial, reputational and/or other damage that caused to TWCA or RAs or a third party out of negligence that is attributable to the relying party or subscriber. TWCA or RAs may claim the damage from the replying party or subscribers according to the relevant law.

3.3.2 Fiduciary Relationships

The fiduciary relationship does not exist among TWCA, RAs and subscribers.

3.4 Interpretation and Enforcement

3.4.1 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.

3.4.2 Severability of Provisions, Survival, Merger, and Notice

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 “the Contact Details, Clause 2.5”, 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 subscribers within this CPS are still valid and shall not be invalidated following the termination of such relationship. For example, when a subscriber applies for a cancellation of the relevant business relationship to a bank after using the subscriber certificate in the transfer system of that bank’s network banking system, the relevant rights and obligations of that subscriber 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 subscribers or RAs shall be delivered by the following methods:

1. 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.
2. 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 at least 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.

3.4.3 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 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 subscribers and RAs or subscribers 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.

3.5 Fees

3.5.1 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 subscribers shall be specified in the fee calculation regulations of corresponding businesses or contract terms.

3.5.2 Certificate Access Fees

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

3.5.3 Revocation or Status Information Access Fees

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

3.5.4 Other fees

It is free of charge for subscribers to download the CPS or CP from the website. However, when subscribers 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 subscribers. The rates shall be specified in the fee calculation regulations of corresponding businesses or contract terms.

3.5.5 Refund

When a subscriber applies to TWCA or RA for a refund and revocation of a NB certificate, CXML certificate or EC+ certificate issued within 7 days, the fees will be refunded to the subscriber 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.

When a subscriber applies to TWCA for a refund of an SSL server certificate of the EC+ certificate after completing the application process but prior to the issue, the fees will be refunded to the subscriber without interest after deducted the handling fee of NT$3000. When the application for refund is made after the issue of such certificate, the fees will be refunded to the subscriber without interest after deducing the monthly fee for the term of use and the handling fee of NT$3000.

3.6 Publication and Repository

3.6.1 Publication of CA Information

This CPS shall be published in PDF version on the TWCA website at www.twca.com.tw for users to download and access one month prior to its affectivity.

Users requesting a paper version of the CPS or having certification-related problems may contact TWCA through the following window:

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

3.6.2 Frequency of Publication

The new version of the CP shall be published immediately on the TWCA website after the revision is completed and approved by the PMA.

The new version of CPS shall be published on the TWCA website immediately after the revision made according to the up-to-date needs is completed and approved for effectuation by the competent authorities.

The subscriber certificates, UCA certificates and CRLs shall be published immediately after generation on the repository for subscriber access. After the subscriber certificate of the NB certificate is revoked, the CRL shall be generated and published immediately. After the application for revocation of EC+ certificates and CXML certificates, the CRL of such certificates shall be generated and published every 24 hours according to “CRL Issuance Frequency, Clause 5.4.9.”

3.6.3 Access Control

This CPS does not have access control, and users are free to download it from the TWCA website as needed.

Although the directory server or database certificates and information of revoked certificates are open to user access, data modification is controlled. Users shall access such information according to the security controls of the UCA repository.

3.6.4 Repositories

The UCA repository allows subscriber access for enquiring about subscriber certificates, UCA certificates and CRLs via the TWCA database and directory server. Such access is limited to only the certificate and CRL information, and unauthorized access to other repository information shall be controlled.

3.7 Compliance Audit

3.7.1 Frequency of Compliance Audit for Each Entity

According to the TWCA internal audit specification (edited and compiled according to the ANS X9.79-2001 Certification Authority Control Object (CACO) and ISO 27001:2005 Information Technology – Code of Practice for Information Security Management), TWCA shall conduct an internal audit on the security controls of the operations of its certification systems at least once a year.

3.7.2 Identity/Qualifications of Auditor

Auditors performing the audits shall be equipped with at least the knowledge of certification authority and information security audit, at least 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 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.

3.7.3 Auditor's Relationship to Audited Party

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.

3.7.4 Topics Cover by Audit

Auditors shall audit:

1. if the CPS and relevant codes of operations have been established;
2. if the relevant businesses are carried out according to the CPS and the relevant codes of operations;
3. if RAs establish the registration-related codes of operations according to the CPS; and
4. if RAs carry out the relevant businesses according to the CPS and the RA's codes of operations.

The major auditing items shall include:

1. Announcement of business implementation: If certificate management is implemented according to this CPS and the relevant codes of operations.
2. Service integrity: The security management of the lifecycle of CA private keys and the relevant certificates (generation, entry, 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).
3. 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.

3.7.5 Action Taken as a Result of Deficiency

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.

3.7.6 Communication of Results

After the audit results are determined through discussions with the relevant personnel of the audited party, they shall be classified to the audited party and the relevant auditors only. The audit unit shall not disclose these results to any party without the prior permission from the audited party.

3.8 Confidentiality

3.8.1 Type of Information to be keep Confidential

TWCA protects the subscriber information according to the Computer-Processed Personal Data Protection Law 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 managing or using subscriber information, neither the UCA nor shall the RA disclose the registration basic data and identity authentication data of subscribers (e.g. citizen ID card number, except when it is used as the information for identifying the subscriber identity in the certificate) without prior subscriber permission or approval of the competent authorities, except the information in the subscriber certificate. This shall include the following information that is used in registration or certificate application:

1. Subscriber information for identity verification (e.g. user name, DOB, PIN, user password or passphrase, user account, and contact information).
2. The private information in subscriber registration, certificate application, certificate renewal, certificate suspension or certificate revocation transaction.
3. Subscriber information that subscribers completed in the registration-related application forms and contracts and the private information in the identity documents (or their photocopy) shall be securely and confidentially protected.

Any private key that a CA uses in the certification system shall be properly and confidentially protected and shall not be displayed in plain text other than in the hardware security module (HSM).

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

Neither CAs nor RAs shall make pubic, sell and/or lease the registration basic data and identity authentication data of subscribers without prior subscriber permission when managing or using subscriber information.

3.8.2 Type of Information Not considered Confidential

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.

3.8.3 Disclosure of Certificate Revocation/ Suspension Information

When processing certificate revocation or suspension according to the relevant codes of operation, the UCA shall immediately generate and publish the complete CRL on the certificate database or directory server for subscriber access according to “the CRL Issuance Frequency, Clause 5.4.9.”

3.8.4 Release to Law Enforcement Officials

Unless otherwise meeting any of the following requirements, the registration basic data and identify verification data of subscribers shall not be disclosed to the competent management authorities or any other party without prior permission:

1. Government laws and regulations with the legal authorization of the competent authorities.
2. Legal request from a court of law for resolving a dispute or arbitration.

3.8.5 Release as Part of Civil Discovery

Under no circumstances shall the registration basic data and identity verification data of subscribers be disclosed to a third party. When the transactions using the relevant certificates involve civil litigations that it is necessary to access the relevant registration and certificate information of the corresponding subscribers, the request shall comply with the following:

1. The official request made by a litigation or arbitration authority with legal jurisdiction.
2. The request shall be authorized by the corresponding subscribers with an electronic signature or personal signature.

3.8.6 Disclosure upon Owner’s Request

Except for the information in the certificate that can be disclosed, the related registration and certificate information of users shall only be disclosed to a third party with the application made by the subscriber with an electronic signature or identity documents signed by the subscriber in person. Unless otherwise authorized by the subscriber, under no circumstances shall TWCA or RAs disclose the subscriber registration and/or certificate information upon the request of a third party.

3.8.7 Other Information Release Circumstances

There is no other circumstance for releasing the subscriber information, except at the request made according the government laws and regulations, by the authorization of the subscriber, or for legal application through official applications.

3.9 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 subscribers are owned by their subscribers. 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 subscribers 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 subscriber certificate status information and the CRLs generated and issued by TWCA, and their subscribers and relying parties are licensed by TWCA to use such certificates, status information and CRLs.

TWCA respects the subscriber registration name stored in the registration name column reproduced in the X.509 V3 certificate without guaranteeing the ownership of the intellectual property rights of the subscriber registration name. If the registration trademark of a subscriber has been preoccupied by a prior subscriber, TWCA assumes no responsibility for resolving the disputes arising out of or in connection with the intellectual property rights of such registration trademark and registration name. Subscribers shall apply for resolution of such disputes to the competent authorities of the relevant businesses.

4. Identification and Authentication

4.1 Initial Registration

When receiving an application for subscriber registration, the UCA and RA shall verify the identity documents that subscribers used in the application and correctly verify their identity according to the regulations specified in “Level of Assurance, Clause 2.2.1.1.”

Prior to applying for the issue of certificates to the UCA or RA, subscribers shall complete the registration procedure specified in “Certificates Application, Clause 5.1.”

4.1.1 Type 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 subscribers 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.

A. NBCA

Network Banking Certificate

Distinguished Name (DN)	Description	Example of DN contents
1. Country(C)	Country code of certificate issuing place	C = TW
2. Organization(O)	Certificate issuing authority	O = TAIWAN-CA.COM Inc.
3. OrganizationUnit(OU)	RA distinguished name	OU = Taiwan Bank
4. CommonName(CN)	Certificate applicant distinguished name; e.g. citizen ID card number	CN = A123456789-00

B. EC+

(a) EC certificates

Distinguished Name (DN)	Description	Example of DN contents
1. Country(C)	Country code of certificate issuing place.	C = TW
2. Organization(O)	CA general DN	O = TaiCA Secure CA
3. Organization(O)	CA policy class name	O = Certificate Service Provider
4. OrganizationUnit(OU)	RA English DN	OU = President Securities Corp.
5. OrganizationUnit(OU)	RA branch or service class	OU = PSCNET
6. CommonName(CN)	Certificate applicant DN, e.g. citizen ID card number	CN = TWA123456789-00
7. Email(E)	Certificate applicant e-mail account	E= user@sec.com

(b) SSL server certificate

Distinguished Name (DN)	Description	Example of DN contents
1. Country(C)	Country code of certificate applicant’s location	C = TW
2. State(S)	Location certificate applicant	S = TAIWAN
3. Locality(L)	Location certificate applicant	L = TAIPEI
4. Organization (O)	English DN of certificate applicant	O = TAIWAN-CA.COM Inc.
5. OrganizationUnit(OU)	English DN or service class of certificate applicant	OU = IT
6. CommonName(CN)	DN of certificate applicant; e.g. URL	CN = www.twca.com.tw

C. CXML

(a) Tariff certificate

Distinguished Name (DN)	Description	Example of DN contents
1. Country(C)	Country code of certificate issuing place.	C = TW
2. Organization(O)	CA policy information	O = Finance
3. OrganizationUnit(OU)	CA (issuance unit) information	OU = TaiCA Finance User CA
4. OrganizationUnit(OU)	RA English DN	OU = 12345678-RA-FINANCE
5. OrganizationUnit(OU)	RA application and service DN	OU = TAX
6. CommonName(CN)	Certificate applicant DN; e.g. company tax code	CN = 12345678-01-000

(b) CXML certificate

Distinguished Name (DN)	Description	Example of DN contents
1. Country(C)	Country code of certificate issuing place.	C = TW
2. Organization(O)	CA policy information	O = Information
3. OrganizationUnit(OU)	CA (issuance unit) information	OU = TaiCA Information User CA
4. OrganizationUnit(OU)	RA English DN	OU = 12345678-RA-Trade
5. OrganizationUnit(OU)	RA application and service DN	OU = Trade
6. CommonName(CN)	Certificate applicant DN; e.g. company tax code	CN = 12345678-01-000

(c) S/MIME certificate

Distinguished Name (DN)	Description	Example of DN contents
1. Country(C)	Country code of certificate issuing place.	C = TW
2. Organization(O)	CA information	O = TAIWAN-CA Inc.
3. OrganizationUnit(OU)	CA (issuance unit) information	OU = TWCA SMIME User CA
4. OrganizationUnit(OU)	RA English DN	OU = 12345678-RA-SMIME
5. OrganizationUnit(OU)	RA application and service DN	OU = SMIME
6. CommonName(CN)	Certificate applicant DN; e.g. application class+ last 4 digit of code + S/N	CN = SMIME5678-00-000001

The e-mail shall be indicated in the <SubjectAltName> column.

4.1.2 Need for Names to be Meaningful

Only meaningful user ID information shall be input in the DN column (e.g. citizen ID card number, company tax code, AP DN etc). Every subscriber DN in every certification system shall be identifiable and unique, and no anonymous or unidentifiable user ID shall be allowed.

4.1.3 Rules for Interpreting Various Name Forms

The regulations governing the user distinguished name of individual business systems shall be subject to the competent authorities of the corresponding business. The DN using the citizen ID card number shall be subject to the regulations specified by the Ministry of the Interior. The DN using the company tax code shall be subject to the regulations specified the competent authorities. The DN for non-ROC resident shall be subject to the uniformed number formed with the number of passport issued by individual countries or the general number that the FDC used to identify aliens in Taiwan. The domain name of servers shall be subject to the domain management regulations specified by the TWNIC. The domain name of transnational servers shall be subject to the international domain management regulations.

If it is necessary to use other forms of coding, apart from obtaining an approval from TWCA, subscribers and relying parties shall make prior arrangement of the DN and verify the veracity of DN while verifying the certificate.

4.1.4 Uniqueness of Names

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 subscriber.

4.1.5 Name Claim Dispute Resolution Procedures

When there are different subscribers using the same DN, the UCA/RA shall award the priority use of that DN to the first subscriber registered with that DN. Neither the UCA nor the RA is responsible for resolving the disputes arising from or in connection with DN. Subscribers 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 subscribers is identical, these subscribers shall make the claim to the Ministry of the Interior.

When the DN of a subscriber is owned by another subscriber as proven by the valid documents issued by the competent authorities, the UAC 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 subscriber.

4.1.6 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 subscribers to use them as their DN. Nonetheless, this shall not guarantee the recognition, verification and uniqueness of the subscriber’s registered trademark. Neither TWCA nor the RA is responsible for resolving disputes concerning such matters. Subscribers shall apply for resolution to the competent authorities of the corresponding business.

4.1.7 Method to Prove Possession of Private Key

The UCA or RA shall verify the legitimacy and veracity of the subscriber private key with at least any of the following methods:

1. When subscribers signing the certificate application contents with the subscriber private key, the UCA or RA shall verify the veracity, uniqueness and legitimacy 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.
2. Apart from verifying the legitimacy and veracity of the private key with the subscriber signature, the UCA or RA can encrypt a message with the subscriber’s public key and deliver the encrypted message to the subscriber by the digital envelope. After verifying the message, the subscriber 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.

4.1.8 Authentication of Organization Identity

If a company registers its level of assurance to Class 3, when TWCA and the RA verify its registration status and DN, this company shall provide the relevant supporting documents (the company stamp and signature of the statutory representative shall appear in each photocopy) issued by the competent authorities or legally authorized units or the relevant legal documents if it is an overseas company. If the registration is

made by an agent, the agent shall apply for the registration in person. Also, the identity documents of this agent shall be verified. The level of assurance for registration is specified in “Level of Assurance, Clause 2.2.1.1.”

4.1.9 Authentication of Individual Identity

If individual registers his/her level of assurance to Class 3, this individual shall apply for registration in person and submit the relevant identity documents (an ID or passport with his/her photo) for the RA to verify. No application shall be made by an agent. When the applicant is an alien, the verification shall be conducted according to the relevant business regulations (e.g. verification of passport with photo). The level of assurance for registration is specified in “Level of Assurance, Clause 2.2.1.1.”

4.2 Routine Rekey

When the validity of a subscriber key (certificate) is set to one year, this key must 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 subscriber 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 subscriber certificate of NB certificates, EC certificates and CXML certificates (the validity of private key is the same as that of the certificate) is 3 years.

The maximum validity of the SSL server certificate is 4 years and is subject to extension with the approval of PMA when there is a special need.

Prior to the expiration of the certificate, subscribers of EC certificates and CXML certificates shall sign the certificate application message of the newly generated public key with the valid private key and deliver the message to the RA to apply for the issue of the new certificate. When running the rekey of the private key prior to the expiration of the certificate, subscribers of NB certificates shall apply for the issue of new certificate to the RA either over the counter or by mail. Subscribers can also sign the certificate application message of the newly generated public key with the valid private key and deliver the message to the RA to apply for the issue of the new certificate.

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 identity verification data for certificate renewal from the RA, subscribers shall use the certificate application message and subscriber identity verification 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 subscriber certificate application message.

4.3 Rekey after Revocation

After revoking a certificate, subscribers shall not apply to the UCA/RA for re-issuing the certificate. Instead, subscribers shall run the procedure again. That is, subscribers shall run the identity verification for registration. After obtaining the identity verification 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 identity verification 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 subscriber, the RA shall verify the legitimacy of the private key and the legitimacy and integrity of the subscriber’s certificate application message.

4.4 Revocation Request

Please refer to Certificate Suspension and Revocation, Clause 5.4, for the regulations of certificate revocation.

5. Operation Requirements

5.1 Certificate Application

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.

1. The RA shall explain in detail to subscribers 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.

2. Subscribers shall complete correct and detailed information in the relevant application forms and provide the relevant supporting documents. The RA shall perform the subscriber identity verification according to the relevant level of assurance. After verifying the subscriber identity, the RA shall provide the subscriber his/her identity code and PIN to complete the subscriber registration process.

3. 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.

A. Application for NB certificates

1. After completing the RA registration procedure, obtaining the subscriber identity verification 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.

2. Before subscribers applying for the certificate, the RA shall securely and confidentially deliver the subscriber identity verification data for certificate application to the UCA.

3. When subscribers send the certificate application message to the RA to apply for the issue of certificate, the RA shall check the legitimacy and integrity of the certificate application message. If there is no error, the RA shall sign the certificate application message with the RA private key and encrypt the information prior to delivering it to the UCA.

4. The UCA shall verify the legitimacy and integrity of the subscriber certificate application message received from the RA. If there is no error, the UCA shall issue the certificate to the subscriber.

B. Application for EC+ certificates

(1) EC certificates

1. After completing the RA registration procedure, obtaining the subscriber identity verification 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.

2. After checking the legitimacy and integrity 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.

3. The UCA shall check the subscriber certificate application message received from the RA, the legitimacy of the RA and subscriber identity, and the integrity of message. If there is no error, the UCA shall issue the certificate and deliver it to the RA.

4. The RA shall check the legitimacy and integrity of subscriber certificate delivered by the UCA. If there is no error, the RA shall send the certificate to the applicant.

(2) SSL server certificates

1. All assurance levels of SSL server certificates shall use following procedure to verify subscriber's information.
2. Subscribers shall prepare the "photocopy of the profit business registration"; "domain name authorization"; "SSL Server Digital Certificate Application Form"; and the check or draft of the service fees; and send them to the RA to apply for the SSL server certificate.

3. After entering the SSL server certificate application website via the Internet, subscribers shall generate the subscriber certificate application file according to the regulations for SSL server certificate application and registration. Then, subscribers shall complete the information of the technical contact person, business contact person and accounting contact person based on the information completed in the "SSL Server Digital Certificate Application Form" and the password to complete the certificate application.

4. If the domain name is registered in Taiwan (*.com.tw), RA must query the TWNIC WHOIS database to verify the ownership of domain name which filled in the certificate application form. If the domain name is not registered in Taiwan, RA must use the global WHOIS service (Network Solutions or others) to verify the ownership of the domain name.

5. After checking the subscriber's application documents and certificate application message, operators shall issue the subscriber certificate if there is no error and deliver a notice to the subscriber to download the certificate from the TWCA website by e-mail.

C. Application for CXML certificates

1. All assurance levels of CXML certificates shall use following procedure to verify subscriber's information.

2. After completing at least 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.

3. After verifying the subscriber identity identification code and PIN and the integrity 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.
4. If certificate applicant applies the S/MIME certificate, RA must verify the applicant's email address. When verify the email address of S/MIME certificate, RA must verify the domain name ownership of mail address which is filled in certificate application form. After verify the ownership of domain name, RA operator will manually send email to applicant's mailbox to notify the certificate applying procedure is under process, and ask subscriber to reply to verify that the email address is correct and subscriber did do the certificate application. If certificate applicant replies using the same mail address and confirms the certificate application request, the verification of email address will be success,

otherwise it will be fail.

5. After checking the subscriber certificate application message delivered from the RA, the legitimacy of the RA and subscriber identity, and the integrity of message, the UCA shall issue the certificate and deliver it to the RA if there is no error.

6. After checking the legitimacy and integrity of the subscriber certificate reply message from the UCA, the RA shall deliver the certificate to the applicant if there is no error.

For the reason of security control, the RA or the UCA may deliver to the subscriber 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.

5.1.1 Certificate Application Policy

- New certificate application: Subscriber shall apply for the issue of a new certificate after completing the registration procedure.
- Certificate extension/renewal: Please refer to the Certificate Renewal (Extension) Policy, Clause 5.1.2.
- Certificate rekey/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.
- After a subscriber certificate is suspended, subscribers shall not apply for certificate re-issue to the UCA.
- After a subscriber certificate is revoked, subscribers shall complete the Certificate Application Form and run the subscriber identity verification before applying to the RA for issuing a new certificate.
- After cancelling the subscriber registration, the rights and obligations between the subscriber and RA are terminated. In this case, subscribers shall apply for registration to the RA again before they can apply for issuing a new certificate to the RA.

5.1.2 Certificate renewal(Extend) Policy

Neither the EC certificates nor the CXML certificates are subject to extension. Also, NB certificates are valid for only one extension.

When subscribers apply to the RA or UCA for issuing a new certificate with the old registration data and public key prior to the expiration of a subscriber certificate, it is known as an extension. Neither the certificate distinguishing data nor the key will be changed, except the validity and serial number of the certificate.

Subscribers shall be noted that no extension shall be allowed for expired or invalid subscriber certificates.

5.1.3 Certificate Suspension Policy

Neither the NB certificates nor the EC certificates are valid for suspension.

When subscribers wish to suspend a certificate or when there are doubts of theft, marauding or security of the private key, subscribers shall immediately apply for certificate suspension to the RA according to the code of operations of the relevant business systems and the RA.

If subscribers do not release a suspended certificate before the certificate expiration, this certificate shall be added to the CRL and becomes invalid. If subscribers apply for releasing a suspended certificate to the RA before the certificate expiration, this certificate shall be removed from the CRL and becomes valid until its expiration.

No suspension or release of an expired or invalid certificate shall be allowed.

5.2 Certificates Issuance

Please refer to “Certificates Application, Clause 5.1”, 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 subscriber access.

When the subscriber certificate application message is rejected by the UCA, the UCA and the RA shall immediately notify the subscriber 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.

The RA and subscribers can only sign and encrypt a message and shall not issue certificates of any kind.

5.3 Certificates Acceptance and Using

5.3.1 Certificates Acceptance

After the certificate is issued and obtained from the UCA, subscribers 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 validity and legitimacy 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 accepted a certificate, this also means that they have also accepted the rights and obligations specified in this CPS, the CP and the contract.

5.3.2 Certificates Using

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 and/or unauthorized use or theft by a third party;
- verify the certificate chain; check every certificate and the validity and legitimacy of that certificate (if it is revoked, expired, legally and correctly issued by the UCA, and legally and corrected possessed by the subscriber); 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 validity and integrity 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.

5.4 Certificate Suspension and Revocation

5.4.1 Circumstances for Revocation

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

1. Certificates revoked by subscribers
   - When a subscriber wishes to revoke a certificate, for example for security consideration after the termination of employment or transfer of an employee or when the subscriber does not want to use the certificate anymore.
   - A subscriber shall revoke a certificate when the contents and subscriber registration data in the certificate have been changed, such as a change of registration data after a restructuring or merger or for any special reasons.
   - A subscriber shall 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
   - A certificate shall be revoked as the certification system key changes, becomes invalid or out of system integration needs.
   - A certificate shall be revoked when a CA terminates its 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. Certificates revoked by competent authorities
   - A certificate is revoked when the competent authorities or a court of law apply to revoke a certificate according to the relevant procedures.

5.4.2 Who can Request 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 apply to revoke their certificates as needed according to the RA's code of operations.

2. Certificates revoked by RA (TWCA)
   - When applying for revoking a certificate, RA (TWCA) shall follow the Circumstances for Revocation, Clause 5.4.1, and contract signed with the subscriber and the relevant codes of operations.

3. Certificates revoked by an authorized third party
   - The authorized person of a corporation may revoke a certificate under legal authorization.
   - When a legal legacy successor of a subscriber applies to revoke a certificate, RA shall verify the death status and the status of the legal successor according to the relevant codes of operations.
   - A court of law or arbitration institution shall apply to revoke a certificate to RA according to the relevant codes of operations of TWCA.
   - When applying to revoke a certificate, the competent authorities shall follow the relevant laws and regulations.

5.4.3 Procedure for Revocation Request

A. Revocation of NB certificates

1. Subscribers shall complete the Certificate Revocation Application Form according to the RA/TWCA code of operations. Or, after the identity verification of RA, subscribers shall sign the certificate revocation application message with their private key and deliver the message to the RA to apply for certificate revocation.

2. After receiving the certificate revocation message from the subscriber, RA shall check the legitimacy and integrity of the revocation message, sign it with the RA private key and encrypt the entire message if there is no error before delivering it to the UCA to apply for revocation.

3. After receiving the certificate revocation message, UCA shall check the legitimacy and integrity of the identity message of the RA and subscriber applying for the revocation. When there is no error, UCA shall revoke the certificate and notify RA of the revocation reply message and update the CRL immediately.

4. After receiving the revocation reply message UCA, RA shall check the legitimacy and integrity of the message and reply to the applicant when there is no error.

According to the RA code of operations for certificate revocation, when subscribers are allowed to apply to revoke their certificates to the UCA:

1. After signing the certificate revocation message with the private key, the subscriber shall deliver the message back to the UCA to apply for certificate revocation.

2. After receiving the certificate revocation application message from the subscriber, UCA shall check the legitimacy and integrity of the message and revoke the certificate if there is no error. Then, UCA shall send a revocation reply to the subscriber and immediately update the CRL.

B. Revocation of EC+

1. Business EC certificates

(1) After a subscriber registers to RA according to the RA/TWCA security controls (PIN, protection password etc) or completes the revocation application form to apply for certificate revocation, RA shall verify the status of the subscriber 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.

(2) After receiving the certificate revocation request message from RA, UCA shall check the legitimacy and integrity of the status of RA and subscriber 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.

(3) 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.

2. Revocation of SSL server certificates

(1) Application by mail

After completing and signing the "SSL Server Certificate Revocation Application Form", subscribers shall mail the application form to TWCA to apply to revoke the certificate. After checking the subscriber identity, TWCA operator shall revoke the certificate when there is no error.

(2) Online application

After logging on to the TWCA SSL server certificate system website, TWCA shall check the subscriber identity. When there is no error, subscribers may select the Certificate Revocation item. The TWCA certification system will immediately revoke the certificate. Also, subscribers shall complete and sign the "SSL Server Certificate Revocation Application Form" to TWCA for reference.

C. Revocation of CXML certificates

1. After a subscriber registers to RA according to the RA/TWCA security controls (PIN, protection password etc) or completes the revocation application form to apply for certificate revocation, RA shall verify the status of the subscriber 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 to revoke the certificate.

2. After receiving the certificate revocation application message from RA, UCA shall check the legitimacy and integrity of the status of RA and subscriber 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.

3. 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.

When the competent authorities, a court of law, an arbitration institution and/or any authorized third-party requests the revocation of certificates, it shall complete an application form to apply for certificate revocation according to the relevant codes of operations of 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 grace period, i.e. the period the application for revocation to the validation of revocation; except for business negligence attributed to UCA or RA.

5.4.4 Revocation Request Grace Period

Subscribers requesting the revocation of certificates shall apply to RA or UCA immediately.

After receiving the request message of certificate revocation from the subscriber, RA or UCA shall process the request immediately during the business or office hours and shall finish processing the request within 24 hours.

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

The CRL for NB certificates shall be generated immediately after receiving the request of certificate revocation from subscribers. Therefore, there is no grace period for the revocation of NB certificates.

5.4.5 Circumstances for Suspension

The suspension of subscriber 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 of the following circumstances:

1. Certificates suspended by subscribers

- When there are doubts of private key loss and exposure, subscribers may apply to suspend their certificates without revoking them in order to reserve the right of certificate use.
- Subscribers may apply to suspend their certificates when they do not wish to use them for a period of time.

2. Certificates suspended by RA/TWCA
   - A certificate shall be suspended 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 that he/she allegedly breaks the law, the relevant regulations, this CPS or the scope of certificate uses.

3. Certificates suspended by competent authorities
   - A certificate shall be suspended when the competent authorities or a court of law apply to suspend a certificate according to the relevant procedures.

5.4.6 Who can Request Suspension

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

1. Certificates suspended by subscribers
   - Subscribers may apply for suspending their certificates as needed according to the RA's code of operations.

2. Certificates suspended by RA (TWCA)
   - When applying for revoking a certificate, RA (TWCA) shall follow the "Circumstances for Suspension, Clause 5.4.5", and contract signed with the subscriber and the relevant codes of operations.

3. Certificates suspended by an authorized third party
   - The authorized person of a corporation may suspend a certificate under legal authorization.
   - A court of law or arbitration institution shall apply for suspending a certificate to RA according to the relevant codes of operations of TWCA.
   - When applying to suspend a certificate, the competent authorities shall follow the relevant law and regulations.

5.4.7 Procedure for Suspension Request

The certificate suspension service of NB certificates and EC+ certificates is unavailable from the UCA.

1. After a subscriber registers to RA according to the RA/TWCA security controls (PIN, protection password etc) or completes the suspension application form to apply for certificate suspension, RA shall verify the status of the subscriber and run the certificate suspension process when there is no error. RA shall sign the subscriber's certificate suspension request message with its private key before delivering to UCA to apply to suspend the certificate.

2. After receiving the certificate suspension application message from RA, UCA shall check the legitimacy and integrity of the status of RA and subscriber and the message. When there is no error, UCA shall suspend the certificate according to the relevant codes of operations and send the certificate revocation reply message to RA.

3. 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 revocation from the subscriber or other authorized parties until the publishing of the suspension notice within 24 hours, subscribers 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 subscriber 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 RA in order to re-validate the certificate for further use.

5.4.8 Limits on Suspension Period

As the certificate suspension service of NB certificates and EC+ certificates is unavailable from the UCA, there is no limit on the suspension period.

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 CXML certificates begins from the listing of a CXML certificate in the CRL after completing the suspension procedures until the subscriber applies for revoking the suspension. Therefore, the period between the listing the CXML certificate in the CRL until the revalidation of the CXML 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.

5.4.9 CRL Issuance Frequency

According to the code of operations of the certification system, the UCA of EC+ certificates and CXML certificates shall generate the CRL within 24 hours. Therefore, the CRL issuance frequency shall be 24 hours.

When a subscriber applies to revoke a NB certificate, the UCA of NB certificates shall immediately revoke that certificate and generate the CRL.

5.4.10 CRL Checking Requirements

When using a certificate on a business application system, either the subscriber or the relying party shall verify the validity and status (if it is revoked) of the certificate. This is because not until a subscriber applies for revoking a certificate will UCA generate the CRL according to the frequency of CRL issuance. The frequency of issuance of the CRL for EC+ certificates and CXML certificates is once every 24 hours. However, when revoking an NB certificate, the certificate shall be revoked and CRL generated immediately. In consideration of business risk, the relevant business application systems may voluntarily request or enquire the CRL status from UCA at planned intervals according to the security level.

When the OCSP enquiry is used in the security mechanism of the business application systems, the subscriber or relying party may skip the CRL check.

5.4.11 On-line Revocation/Status Checking Availability

While the online revocation/status check service is unavailable for NB certificates and EC+ certificates, the status of these certificates shall be verified by means of CRL check.

The online revocation/status check service is available in the security mechanism of CXML certificates. If the online revocation/status check is selected, subscribers will not need to check the CRL.

5.4.12 On-line Revocation Checking Requirement

Please refer to “CRL Checking Requirements, Clause 5.4.10”, and “On-line Revocation/Status Checking Availability, Clause 5.4.11”, for details.

5.4.13 Other Forms of Revocation Advertisements Available

The certificate status check is available from the TWCA certification system. However, the other forms of revocation advertisements are currently unavailable, except for the X.509 V2 CRL.

5.4.14 Checking Requirements for Other Forms of Revocation Advertisements

As other forms of revocation advertisements are currently unavailable from TWCA, there is no checking requirement for other forms of revocation advertisements.

5.4.15 Special Requirements ReKey Compromise

As there is no special requirement, when there are doubts a rekey compromise shall be processed according to “Key Changeover, Clause 5.7” .

5.5 Security Audit Procedures

From physical equipment operations to certification system implementation, both TWCA and RAs shall retain the relevant operational documents and transaction and audit records as a reference for performing the security audit of the certificate systems. Also, the operation of the certification systems shall be audited according to the TWCA and RA audit regulations.

5.5.1 Types of Events Recorded

An audit log shall include at least the following information:

1. the registration and cancellation of registration information of subscribers, including contracts, registration documents, application forms and messages related to registration transactions;
2. the records of success and failure of the generation, entry and change of the RSA key and 3DES key for operating the certification system or other key part;
3. the records of success and failure of the generation, entry and change of the CA key and certificate;
4. the records of success and failure of the processing and reply of certificate application transactions;
5. audit records and e-mail logs of certification system operations;
6. the records of the processing and reply of certificate revocation transactions and CRLs;
7. 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;
8. 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

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

5.5.2 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 for 3 months, 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 (at least 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 and RA, 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.

5.5.3 Retention Period for Audit Log

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

5.5.4 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 at least once a week, and at least 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.

5.5.5 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.

5.5.6 Audit 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 must continue to provide service, audit logs shall be collected manually. The events collected shall at least include:

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

5.5.7 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.

5.5.8 Vulnerability Assessments

The potential threat and risk, both internal and external, of certification system operations shall be assessed at least once a year by checking and following up the audit logs and making constant adjustments and modification of the security controls of system operations in order to minimize the risk on system operations.

5.6 Records Archival

5.6.1 Types of Event Records

TWCA shall make and retain the backup copy of system environment files, contracts signed with users, information concerning user registration data, subscriber 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.

5.6.2 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; subscriber registration application forms and relevant contract terms; and subscriber identity documents shall be retained for at least 10 years from their expiration.
- Information of subscriber certificate application, renewal and extension; and revoked or expired certificates shall be retained for at least 10 years from certificate expiration.
- The record of transaction messages concerning the application, access and revocation of certificates shall be retained for at least 10 years from certificate expiration.
- The data related to the PCA and UCA key changes shall be retained for at least 10 years from key

certificate expiration.

- The data related to the Root CA key changes shall be retained for at least 15 years from key certificate expiration.

5.6.3 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 DR center with central air-conditioning and protected by security controls.

Under no circumstance shall TWCA or RA disclose to a third party the basic data and identify authentication data of subscribers 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.

5.6.4 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 DR 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 recover manual.

5.6.5 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 system time and automatically add the time to the time stamp. When it is generated manually by operators, operators shall input the system time in the relevant forms and records as a reference for future trace.

When subscribers 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.

5.6.6 Archive Collection System

Archive records concerning certification system operations shall be retained by TWCA operators. 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.

5.6.7 Procedure 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 at least once a year or irregularly according to business needs according to the code of operations for internal management. 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.

5.7 Key Changeover

5.7.1 Key Changeover of Subscriber

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

When the key has expired, subscribers may generate a new key pair to apply for a new certificate to UCA/RA by completing the certificate renewal application form to apply for a key changeover to RA. When there are doubts about the security of a valid key, subscribers shall first apply for certificate revocation to UCA/RA before generating a new key pair to apply for a new certificate to RA by completing the certificate application form according to the RA code of operations.

5.7.2 Key Changeover of UCA

A. NB certificates

1. When the key has expired, UCA may generate a new key pair to apply for a new certificate to PCA. After the new certificate is issued, UCA shall sign the subscriber's applications for new certificates and re-sign the UCA CRLs with the new key. Also, UCA shall immediately notify subscribers and RAs of with the fastest method.

2. 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 subscriber's applications for new certificates and re-sign the CRLs with the new key. UCA shall immediately notify subscribers and RAs of with the fastest method that subscriber certificates and CRLs issued with the old UCA private key are invalid and subscribers shall generate a new key pair to applying for a new certificate to UCA.

B. EC+ certificates and CXML certificates

1. 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 subscriber'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.

2. 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 subscriber's applications for new certificates and re-sign the CRLs with the new key. Also, UCA shall immediately notify subscribers and RAs with the fastest method that subscriber certificates and CRLs issued with the old UCA private key are invalid and subscribers shall generate a new key pair to apply for a new certificate to UCA.

5.7.3 Key Changeover of PCA

A. NB certificates

1. A NB PCA is also a Root CA.

2. When the key has expired, PCA may generate the next key pair and issue the next PCA self-issued certificate according to the certificate chain. After that, PCA shall sign the UCA's application for new certificates and certificate revocation with the next private key pair, and re-issue the PCA's UCA CRL with the next certificate. PCA shall also immediately notify UCAs.

3. When there are doubts about key security prior to the key's expiration, PCA shall first revoke the old certificate before generating the next key pair and issuing a new self-issued sub-certificate according to the certificate chain. After that, PCA shall sign the UCA's application for new certificates and certificate revocation with the new sub-private key pair and notify UCAs with the fastest method that certificates and CRLs issued with the old PCA key are invalid, and UCAs shall generate a new key pair to apply for a new certificate to PCA.

B. CXML certificates

1. 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.

2. 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 Root CA. 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.

5.7.4 Key Changeover of RCA

CXML certificates

1. 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.

2. 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 subscriber certificates and business application systems to stop using all certificates issued by the certification system.

5.8 Compromise and Disaster Recovery

To ensure that the certificate system can be re-implemented and operations re-opened within the shortest time after abnormal situations or natural disasters, in addition to a complete set of network and software/hardware equipment backup systems and a certification system DR plan, TWCA has planned the offsite certification recovery and operations to ensure business continuity when a situation or disaster occurs.

5.8.1 Computing Resources, Software, and/or Data are Corrupted

When software computing resources of the certification system and/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 DR 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 recover manual to resume normal system operations.

5.8.2 Entity Public Key is Revoked

The revocation of entity public keys shall be processed according to “Certificate Suspension and Revocation, Clause 5.4.”

5.8.3 Entity Private Key is Compromised

When there are doubts about the damage, loss, exposure, interpolation or third-party theft of the entity private key, the entity shall immediately report to RA and apply for revocation. The entity shall also apply for cancelling the use that private key (certificate) to the relevant business application systems of the private key. The entity shall follow “Certificate Suspension and Revocation, Clause 5.4,” to process other relevant affairs.

5.8.4 Secure Facility after a Natural or Other Type of Disaster

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

1. 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;

2. 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 DR 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;

3. shut down and the DR plan shall be initiated immediately to recover system operations when the relevant secure facilities are severely damaged.

5.8.5 Contingency and Disaster Recovery Plan

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 at least 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.

5.9 CA 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 subscribers 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 subscribers certificates;
- revoke the certificate of the CA to be terminated and all subscriber certificates it issues and transfer to the CA overtaking the business the relevant private keys and certificates, all subscriber 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; subscriber 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 at least 7 years;
- expunge the relevant private keys of the CA to be terminated, officially announce to subscribers 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 subscribers 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 subscriber business system.

6. Physical、Procedural and Personnel Security Control

6.1 Physical Control

The certification system shall be implemented in a safe and robust building and independent hardware and software operating environment. Only authorized personnel shall access the certification system to implement certificate management according to the code of operations for security control. HSMs shall also be placed in an environment with security controls to avoid deliberate damage or unauthorized access and uses.

6.1.1 Site Location and Construction

A CA shall be an independent data center equipped with shock-resistant, water-resistant, fire-resistant and temperature control systems, independent power supply, independent uninterrupted power supply (UPS), access control system, anti-invasion access monitoring and anti-damage alarm system as specified below.

6.1.2 Physical Access

The access control for the CA data center shall include identity check and verification with three IC-card-protected entrances and fingerprint recognition. Access shall be available for at least two personnel at the same time (no one can get in and out of the data center alone). CCTV system with moveable cameras and recording equipment working 24 hours and IR anti-invasion alarm system shall be equipped at the access.

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.

6.1.3 Power and Air-Condition

The CA shall be equipped with a diesel generator and 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.

6.1.4 Water Exposures

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

6.1.5 Fire Prevention and Protection

The CA shall be built with fire-retardant materials and equipped with the FM2000 fire 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.

6.1.6 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.

6.1.7 Waste disposal

Prior to disposing hardware equipment, disk drives and HSMs that are used on the certification system, sensitive and confidential business information shall be securely expunged and destroyed. The process shall be verified by the audit unit and records shall be maintained.

Documents and storage media containing sensitive and confidential business information shall be securely destroyed prior to disposing of to ensure that such information shall be neither recovered nor accessed. The process shall be verified by the audit unit and records shall be maintained.

6.1.8 Off-Site 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 secure offsite environment. Backup and archive information storage media shall be tested and verified for validity and usability at planned intervals.

6.2 Procedure Control

6.2.1 Trusted Role

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 and RA 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.

6.2.1.1 CA

- The CA manager shall manage and supervise the operations of the entire certification system.
- Auditors (non-CA TWCA operators) shall audit and supervise the operation of the TWCA certification system. Please see “Security Audit Procedures, Clause 5.5,” for details.
- Supervising personnel of certification system operations shall work at least 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 at least 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 subscriber certificates and creation of subscriber data.
- Operators of certification system operations shall create subscriber 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.

6.2.1.2 RA

- The RA supervisor shall manage and supervise user registration.
- Administrators shall work at least 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.

6.2.2 Number of Persons Required per Role

TWCA and RA 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 at least two operators; the RSA key and 3DES key shall be created by at least 2 security administrators according to the operation security control procedures. Also, these personnel shall support one another when carrying out their duties.

6.2.3 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.

6.3 Personnel Control

6.3.1 Background, Qualifications, Experience, and clearance requirements

TWCA and RA 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.

- Operators shall at least have the practical experience in CA operations or receive the relevant training related to CA operations and pass the test. When TWCA is in short of human resources in a business, it shall outsource such business to a third party.

The administrators and supervising personnel shall at least 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 shall not be outsourced to any third party.

6.3.2 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.

6.3.3 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 hardware and software and ISMS 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.

6.3.4 Retraining Frequency and Requirement

The relevant knowledge and skills for operating the certification system of operators shall be reviewed at least 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.

6.3.5 Job Rotation Frequency and Sequence

TWCA shall transfer eligible candidates to different jobs and provide them with necessary and appropriate education and training prior to the transfer in order to cope with the system requirements and ensure the suitability of work for operators.

6.3.6 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.

6.3.7 Contracting Personnel 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.

6.3.8 Document 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 at least include:

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

7. Technical Security Control

7.1 Key Pair Generation and Installation

7.1.1 Key Pair Generation

When generating the UCA key pair, at least 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.

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.

7.1.2 Private Key Delivery to Entity

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

7.1.3 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 subscriber’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.

7.1.4 CA Public Key Delivery to Users

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.

7.1.5 Key Sizes

The size of the CA signature and encrypted RSA key and the RCA key shall at least be 2048 bits. The size of the PCA key shall at least be 1024 bits. The size of the UCA key shall at least be 1024 bits. The size of the subscriber key shall at least be 1024 bits. The size of these keys is subject to adjustment according to the system security requirements and the progress in cryptographic analysis technology and computer hardware technology.

7.1.6 Public Key Parameters Generation

Generation and selection of TWCA RSA public key parameters:

The optimal key parameters for EC+ certificates and CXML certificates shall be generated by CNS15135, ISO19790 or FIPS 140-2 accredited random number generators (RNG).

7.1.7 Parameter Quality Checking

Quality check of TWCA RSA public key parameters:

The CNS15135, ISO19790 or FIPS 140-2 accredited HSMs shall be applied to check the quality of the key parameters for EC+ certificates and CXML certificates.

7.1.8 Hardware/Software Key Generation

EC+ certificates and CXML certificates shall be generated by CNS15135, ISO19790 or FIPS 140-2 accredited HSMs**.**

7.1.9 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, subscribers requesting certificates for other purposes shall apply to UCA for the key and certificate that meet their intended use.

7.2 Private Key Protection

7.2.1 Standards for Cryptographic Module

EC+ certificates and CXML certificates shall be generated with FIPS 140-1 Level 3 accredited HSMs.

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

The UCA private key shall be generated, implemented and changed by at least 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.

7.2.3 Private Key Escrow

No private key escrow, recovery and storage service is available for NB certificates, EC+ certificates and CXML certificates.

7.2.4 Private Key Backup

The CA private key shall be encrypted before storing in the HSM. The backup of the key shall be performed by at least 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 backup media in the offsite DR center with security controls.

7.2.5 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. Please refer to “Record Archival, Clause 5.6 for details.”

7.2.6 Private Key Entry into Cryptographic Module

The CA private key shall be generated, implemented or changed directly from the HSM by at least 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.

7.2.7 Method of Activating Private Key

The CA private key stored in the HSM shall be activated by at least 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 passphrase possessed by the subscriber, and no one else can access such password or passphrase.

7.2.8 Method of Deactivating Private Key

The CA private key stored in the HSM shall be deactivated by at least 2 authorized key administrators logging in the system (e.g. IC card and fingerprint or 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.

7.2.9 Method of Destroying Private Key

When the private key is not in use, or the corresponding public key is failed or revoked, their software cryptographic modules shall be destroyed by means of data overwriting, and the HSM or IC card shall be destroyed by means of zeroization.

When a HSM is scraped, all private keys inside shall be destroyed with the above methods.

7.3 Other Aspects of Key Pair Management

7.3.1 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 at least 10 years. If the retention period specified by the competent authorities is longer, such retention period shall prevail.

7.3.2 Usage Periods for Public Keys and Private Key

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

The maximum validity of the public and private keys of NB certificates, business EC certificates and CXML certificates shall be 3 years.

The maximum validity of the public and private keys of SSL server certificates shall be 4 years. However, the validity shall be extended with the approval of PMA.

7.4 Activation Data

7.4.1 Activation Data Generation and Installation

The activation data of subscriber private keys, such as IC card PIN, passphrase 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 at least 6 characters and passphrase at least 8 characters). When it is delivered to the subscriber over the Internet, it shall be protected with appropriate security controls. If it is delivered to the subscriber by mail, it shall be delivered in a sealed password envelope. The delivery method is subject to change according to the subscriber requirement during implementation.

7.4.2 Activation Data Protection

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.

7.4.3 Other Aspects of Activation Data

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

1. 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 subscriber. There is no need of special security controls when delivering by mail. The recommended lifecycle for the activation data used in non-private or general data delivery or low amount transactions shall be one year, and such data shall be changed after one year.

2. 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 subscribers. They can be selected by subscribers 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.

3. 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 subscribers. 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 subscribers according to the security requirements of the business system.

The lifecycle specifications of the activation data that subscribers 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 subscribers according to the security level requirements of the business (e.g. subscribers are recommended to change the activation data for connecting to the RA every 3 or 6 months).

7.5 Computer Security Controls

7.5.1 Specific Computer Security Technical Requirements

The certification system shall operate the following tasks in an operating system environment protected by security controls: the identification and verification of user identity, the defining and control of system resource access right, and the audit and recording of security control events. Databases shall be protected by security controls.

Security controls for the confidentiality, integrity, non-repudiation shall be provided when delivering transaction messages. Strict security controls shall be applied to backup and archive data. The management responsibility and authority of personnel and internal operating procedures shall be clearly defined and controlled. A well-laid business continuity recovery mechanism shall be implemented. Computer security rating accredited platforms and certification systems shall be used. The ISMS environment for certification system operations shall be implemented and operated according to the ISO27001:2005 ISMS Standard and comply with the security management codes of CA.

7.5.2 Computer Security Rating

The computer software system security rating of the software systems used for certification and important certification systems shall at least comply with the ISO/IEC 15408 CC security standard or its equivalents.

The certification system for EC+ certificates and CXML certificates shall pass the ITSEC E3 security certification.

7.6 Life Cycle Technical Controls

7.6.1 System Development Controls

The controls of the planning and development of relevant systems shall implemented according to the software development control specifications for certificate systems, ISO15048 Common Criteria or equivalent software development control specifications.

7.6.2 Security Management Controls

The ISMS environment for operating the certification systems shall comply with the standards of the WebTrust program for CA (AICPA/CICA)

The certification system shall be used with strict controls. Systems shall be strictly tested and verified prior to installation and use. Version control, functionality testing and recording shall be applied to system modification or update. The integrity of the certification system shall be checked and tested at planned intervals.

Security controls shall be applied to hardware and software equipment from purchasing to acceptance. Auditable security mechanism, e.g. seal, password and signature, shall be applied to identify the integrity of equipment, i.e. without intrusion or change. The verification, system installation and acceptance of HSMs shall be performed in an operating environment with security control.

When software and hardware is updated and the old equipment is scraped, no data with security concern shall be contained in such equipment.

7.6.3 Life Cycle Security Ratings

The code of operations for the security rating of lifecycle has not yet been specified.

7.7 Network Security Control

The certification systems of Root CA and PCA are independently operated offline management systems that are operated manually only by business-related personnel after authorization.

UCA is protected by the firewall and network resource security control systems. Only the CA system related functions are open for users to run certificate-related functions at UCA over the Internet. Users are unable to use functions or communication interfaces not provided by UCA. The instruction detection and antivirus management system are installed to enhance the security controls of network management in order to enhance the anti-intrusion and anti-damage security functions of the network. Also, the version of the firewall, IDS, antivirus and network resource security control systems is updated constantly to minimize the threat and risk of network systems.

7.8 Cryptographic Module Engineering Controls

FIPS 140-1 Level 3 accredited HSMs are used for EC+ certification system and CXML certification system.

8. Certificate and Certificate Revocation List(CRL) Profiles

8.1 Certificates Profile

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

8.1.1 Version Number(s)

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

8.1.2 Certificate Extension

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.

8.1.3 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 Control	Algorithm	OID
Encryption	RSAEncryption	1.2.840.113549.1.1.1
Encryption (signature)	sha-1WithRSAEncryption	1.2.840.113549.1.1.5
Encryption	desCBC	1.3.14.3.2.7
Encryption	3desEDE-CBC	1.2.840.113549.3.7
Hash Function	MD5	1.2.840.113549.2.5
Hash Function	SHA-1	1.3.14.3.2.26

8.1.4 Name Forms

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

8.1.5 Name Constraint

No anonyms or pseudonyms are allowed in the DN of the subscriber certificates issued by the certification systems. Only unique DNs are allowed in the subscriber DN.

8.1.6 Certificate Policy Object Identifiers

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.

8.1.7 Usage of Policy Constraints Extension

When the policy constraint extension is used in the certificate, the code of operation is specified in the certificate-related code of operation for certificate profiles. Apart from the URL for users to obtain the CP, the terse statement of the CP is indicated in the CP extension column in CXML certificates. This is the

applicability of certificate usage.

8.1.8 Policy Qualifiers Syntax and Semantics

When the policy constraint extension 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 CXML 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 identity certification; Part 2 is the usage; Part 3 is the user status; and Part 4 is the business category. Please refer to “Certificate’s Applicability, Clause 2.2,” for details.

8.1.9 Processing Semantics for the Critical Policy Extension

When the policy constraint extension 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 CXML certificates, and it is the constraint code of applicability of certificate usage. This must be checked and processed when using the certificate in business application systems.

8.2 CRL Profile

8.2.1 Version number(s)

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

8.2.2 CRL and CRL Entry Extensions

When the CRL entry extensions are used in the CRL, the code of operation is specified in the certificate-related code of operation for certificate profiles.

9. Specification Administration

9.1 Specification Change Procedure

As the competent authorities of this CPS, the Policy Management Administration (PMA) of TWCA shall review the CPS at least 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.

When relevant OIDs are specified in this CPS, when the contents of the CPS are updated, the corresponding OIDs remain unchanged, except the version serial number.

Should there be suggestions for updating this CPS, please send the details to the Contact Person, Clause 2.5, by mail or e-mail for PMA review.

9.2 Publication and Notification Policies

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 http://www.twca.com.tw.

9.3 CPS Approval Procedures

This CPS shall be approved by 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.

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 and qualification of the person signing the electronic document and the authenticity of the electronic document.

(4). Encrypt/Encipher
It refers to use of mathematical algorithms or other means to encipher an electronic document.

(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 identify and interpret by humans.

(6). Digital Signature
It refers to the computing of an electronic document with mathematical algorithm or other means into a digital message of a particular size and encrypted with the private key of the signor to form an electronic signature. A digital signature can be verified by a public key.

(7). Private Key
It refers to the pair-wise digital data possessed by the signor for producing the digital signature.

(8). Public Key
It refers to the pair-wise digital data open to the public for verifying the digital signature.

(9). <Public Key>Certification or Certificate
It refers to an electronic certificate containing a signature and verification data for conforming to the identity and qualification of the signor.

(10). Certificate Service Provider; CSP
It refers to a certificate issuer or legal person.

(11). Certification Practice Statement; CPS
It refers to the code of operation published by the CA to specify the issue of certificates and processing of other certification businesses of the CA.

(12). Asymmetric Cryptosystem
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 connect a long message (containing many bytes) into a fixed size message. The output of the same message after compression function computing must be identical, and it is absolutely impossible to reduce the input message from the output message.

(14). Issue a Certificate:

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

Appendix 2: Acronyms and Abbreviations

AICPA	American Institute of Certified Public Accountants, Inc.
ANS	American National Standard
BCA	Brand Certification Authority
CA	Certification Authority
CC	Common Criteria
CCA	Cardholder Certification Authority
CCITSE	Common Criteria for Information Technology Security Evaluation
CMA	Certification Management Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CSP	Certificate Service Provider
CRL	Certificate Revocation List
DA	Directory Authority
DN	Distinguished Name
EAL	Evaluation Assurance Level
EB	Electronic Banking
EC	Electronic Commerce
FEDI	Financial Electronic Data Interchange
FIPS	Federal Information Processing Standard
HMAC-SHA1	Hash Message Authentication Code – Security Hash Algorithm 1
ISO/IEC	the International Organization for Standardization, The International Electrotechnical Commission
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
MCA	Merchant Certification Authority
NB	Network Banking
OCSP	Online Certificates Status Protocol
OID	Object Identifier
OECD	Organization for Economic Co-operation and Development
PAA	Pan-Asian e-Commerce Alliance
PMA	Policy Management Authority
PCA	Policy Certification Authority
PIN	Personal Identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RA	Repository Authority(Directory Authority)
RCA	Root Certification Authority
RSA	Rivest, Shamir, Adleman(encryption algorithm)
SET	Secure Electronic Transactions
SSL	Secure Socket Layer
TCSEC	Trusted Computer System Evaluation Criteria
TSA	Time Stamp Authority
TTP	Trusted Third Party
UCA	User Certification Authority
URL	Universal Resource Location