TAIWAN-CA INC.

Root Certification Authority

Certification Practice Statement

(Version 1.0)

Effective Date: 31 December 2008

Revision Record

Rev	Effective Date	Issuer	Note
1.0	31 Dec 2008	TWCA PMA	First Issue

Contents

Summary

Important notices of the Certification Practice Statement (CPS) established by the Root Certification Authority (RCA), TAIWAN-CA INC. (TWCA) are as follows:

1. Approval of Competent Authorities

This CPS is established pursuant to the Required Items in Certification Practice Statements promulgated by **the Ministry of Economic Affairs (MOEA) and approved by the Letter** Jingshangzi **09702430830 issued by the MOEA dated 31 December 2008.**

2. Certificates Issued

(1) Types of Certificates

The RCA of the TWCA issues certificates to subordinate certification authorities (Sub-CA) for verifying their identity.

(2) Assurance Level

The RCA operates according to the Class 4 assurance level specified in its certificate policy (CP) and issues to the Sub-CAs certificates of the following 5 assurance level as defined in the CP:

Assurance Level:

Testing Class: Guarantee for the certificate testing of subscribers or relying parties, and usage other than certificate testing is prohibited.

Class 1: Basic guarantee for identifying data integrity in network environments of very low threat of malicious interpolation.

Class 2: Preliminary guarantee for basic identity authentication suitable for use in network environments of lower risk of malicious interpolation but still with the potential threat of information interpolation.

Class 3: Intermediate guarantee suitable for use in network environments of higher risk of malicious information interception or interpolation.

Class 4: High guarantee suitable for use in network environments of high risk of malicious information interpolation requiring a high recovery cost.

(3) Appropriate Certificate Uses

The RCA issues Sub-CA certificates for establishing the trust relationship between the RCA and Sub-CAs in order to establish the required certification trust path for constructing the PKI

The certificates issued by the RCA are intended for use as the security control for identity verification.

The Sub-CA certificates issued by the RCA according to this CPS are intended for Organizations playing the role as a Sub-CA after approved by the RCA. With the Sub-CA certificate, these Organizations can verify the mutual trust relationship between the RCA and Sub-CA. When verifying the certificate of a Sub-CA with the RCA public key, it can validate the trust relationship between the Sub-CA and the RCA.

3. Liability and Important Notices

(1) When a cause of certificate revocation occurs, e.g. private key discloser or loss, a Sub-CA shall immediately notify the RCA and apply for certificate revocation; provided that the Sub-CA shall be responsible for the risk and liability arising from or in connection with the use of such certificate prior to the publication of certificate revocation.

(2) The RCA shall assume no liability for processing the registration data and certification for Sub-CAs, except for the negligence attributable to the RCA.

(3) The RCA shall assume no liability for the damage that caused Sub-CAs due to the certificates issued to the SCAs as a result of an act of God, e.g. wars and earthquakes, or any event that is beyond the reasonable control of the RCA.

(4) The RCA shall be responsible for the damage that was caused to a third party as a result of the leakage, fraud, interpolation or unauthorized use of the relevant information due to its negligence in retaining the registration and certification data of Sub-CAs.

(5) After receiving an application for certificate revocation, the RCA shall complete the revocation within one workday and issue the certificate revocation list (CRL) and publish it to the repository within one day. A Sub-CA shall take proper action to minimize the effect on relying parties and shall take full responsibility for the use of such certificate prior to the publication of the CRL.

(6) When damages arises between the RCA and a Sub-CA as a result of the issue or use of the certificate, the liability of both parties shall be limited to the scope specified in the relevant laws and regulations and the contract.

(7) When a relying party accepts a certificate issued by the RCA, this means that the relying party has understood and agreed to the liability terms of the RCA and shall trust the certificate within the scope specified in this CPS.

4. Other Important Notices

(1) When a Sub-CA has doubts about the loss or compromise of the private key, or the relevant information of the Sub-CA has been changed, the Sub-CA shall report to the RCA according to the relevant regulations.

(2) Sub-CAs shall properly generate, retain and use their private keys and follow the restrictions on the use of keys and certificates.

(3) When applying for a certificate, Sub-CAs shall provide detailed and correct information. When accepting the Sub-CA certificate issued by the RCA, Sub-CAs shall validate the correctness of the certificate contents and that the public and private keys are in a pair.

(4) Sub-CAs shall store their certificates and CRL in a secure repository and ensure the availability of repository for relying parties to enquire at any time.

(5) When verifying a certificate, relying parties shall use the self-issued certificate of the RCA in order to verify if the digital signature in the Sub-CA certificate is signed with the RCA private key. Relying partiess shall also verify of the certificate has been revoked with the CRL.

(6) When using the CRL issued by the RCA, relying parties shall first verify the digital signature to validate if the CRL is valid.

(7) The RCA shall conduct an internal audit and an external audit at least once a year. Please refer to Audit and Other Assessments, section 8, for details of the audit operations.

1. Introduction

1.1 Overview

TAIWAN-CA INC. (TWCA) is a joint-venture company formed by Taiwan Stock Exchange Corporation (TWSE), Taiwan Depository and Clearing Corporation (TDCC), Financial Information Service Corporation (FISC), and HiTrust Inc (HiTrust).

The TWCA Root Certification Authority Certification Practice Statement (CPS) is established according to the TWCA Public Key Infrastructure Certificate Policy (CP) and the Required Items in Certification Practice Statements promulgated by the Ministry of Economic Affairs (MOEA), the competent authority of the Electronic Signature Law. The aim of this CPS is to describe how the Root Certification Authority (RCA) issue and manage the certificates for the subordinate certification authorities (Sub-CA) according to this CPS.

In order to build a secure and trustable network transaction environment; to ensure information transmitted over the network is not fabricated, interpolated or marauded; to verify the identify of both parties of the transactions and to prevent the repudiation of transactions afterwards, TWCA has established a public key infrastructure (PKI) and RCA as the trust anchor to issue certificates to Sub-CAs.

1.2 Document Name and Identification

The full name of this CPS is TWCA Root Certification Authority Certification Practice Statement.

This CPS is established in accordance with the CP, and its object identifier (OID) is: {joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) CP(5) id-TWCA-PKI-CP-policy(5) }.

1.3 PKI Participants

1.3.1 Root Certification Authority (RCA)

The RCA is the highest level certificate authority playing the role of the trust anchor. The RCA is operated and managed by the TWCA and is responsible for the following work:

(1) to issue and manage Sub-CA certificates;

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

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

1.3.1.1 Policy Management Authority (PMA)

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

(1) CP;

(2) CPS; and

(3) SOP.

1.3.2 Registration Authority (RA)

The duty of RA is to verify the identity and the required information for issuing certificates of Sub-CAs for the RCA to issue Sub-CA certificates.

The RCA shall be the RA, and there is not another RA under the RCA.

1.3.3 Subscriber

The subscriber is the individual specified in the certificate subject and the holder of the private key corresponding to the certificate public key.

The subscriber of this RCA shall be the Organization applying for becoming a Sub-CA or the Sub-CA established by the TWCA.

1.3.4 Relying party

A relying party means an individual accepting the self-issued certificate of the RCA for verifying the validity of the Sub-CA certificate issued by the RCA and the validity of the digital signature message of Sub-CAs with the public key in the Sub-CA certificate.

A relying party shall determine the reliability the Sub-CA certificate or its availability for special usage with the information registered in the Sub-CA certificate issued by the RCA.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The RCA issues Sub-CA certificates for establishing the trust relationship between the RCA and Sub-CAs in order to establish the required certification trust path for constructing the PKI.

The certificates issued by the RCA are intended for use as security control for identity verification.

The Sub-CA certificates issued by the RCA according to this CPS are intended for Organizations playing the role as a SCA after approved by the RCA. With the Sub-CA certificate, these Organizations can verify the mutual trust relationship between the RCA and Sub-CA. When verifying the certificate of a Sub-CA with the RCA public key, it can validate the trust relationship between the Sub-CA and the RCA.

1.4.2 Prohibited Certificate Uses

In addition to applying the Sub-CA certificates issued by the RCA according to the certification applicability, Sub-CA certificates shall be prohibited for use in applications or businesses that may cause mental and physical injuries or death to persons, or hazards to social order and the social environment. The use of the SCA certificates shall also be prohibited for the exceptions of applications and businesses specified in the Electronic Signature Law, other relevant laws and regulations, and the regulations specified by the competent authorities of respective businesses.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The Policy Management Authority (PMA or TWCA PMA), of the TWCA shall be responsible for the establishment, update, and publication of this CPS.

1.5.2 Contact Person

If you have any suggestions for this CPS, please email or mail your suggestions, description of suggestions and contact information to the following contact window. Subscribers may make enquiries about certificate registration, application, update, status check, or report a lost key and worries about security to the following window:

Company	TAIWAN-CA INC. (TWCA)
Contact Window	Policy Management Authority (PMA)
Address	10th Floor, 85 Yen-Ping South Road, Taipei City , Taiwan, R.O.C
Phone	886-2-23708886
Fax	886-2-23700728

Email)	ca@twca.com.tw

1.5.3 Person Determining CPS Suitability for the Policy

This CPS established by the RCA shall be approved by the PMA.

1.5.4 CPS Approval Procedures

This CPS shall be established by the RCA and approved by the PMA.

Pursuant to the Electronic Signature Law, this CPS established by the RCA shall be approved by the Ministry of Economic Affairs (MOEA) prior to publication and offering certificate issue services.

2. Publication and Repository Responsibilities

2.1 Repositories

The repository of this RCA shall offer the enquiry and download of information relating to certification, such as certificates, CRLs, CP, and CPS.

The universal resources location (URL) of the repository is: http://www.twca.com.tw.

2.2 Publication of Certificate Information

The information published by this RCA shall include:

(1) CP and this CPS;

(2) RCA self-issued certificates and related information;

(3) issued certificates; and

(4) CRLs.

2.3 Time or Frequency of Publication

The latest version of the CP after revision and the PMA approval shall be published immediately on the TWCA website.

The latest version of the CPS revised according to actual needs shall be published on the TWCA website immediately after approval by the competent government department.

The self-issued certificates and certificates issued by the RCA shall be published on the repository immediately after their effectivity.

The CRL shall be published at least once every 24 hours.

2.4 Access Control on Repositories

When publishing issued certificates and CRLs, certificate management personnel of the RCA shall store manually in a portable storage device the certificates and CRLs to be published prior to copying them to the repository server for publication.

This CPS and the repository are open to the public without access control. However, access control shall be applied to repository updates to prevent malicious interpolation.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of names

The RCA shall issue the X.509 certificate using the X.500 distinguished name as subject name.

The self-issued certificates and certificates issued to Sub-CAs of the RCA also use this distinguished name.

3.1.2 Need for Names to be Meaningful

The subject identifier the Sub-CA certificate shall comply with the nominalization rules specified in the relevant laws and regulations and be able to identify the particular organization, unit or individual, and shall be readily identifiable by the relying parties.

3.1.3 Anonymity or Pseudonymity of Subscribers

Neither anonymity nor alias is allowed for Sub-CAs according to this CPS.

3.1.4 Rules for Interpreting Various Name Forms

The interpreting rules of the identifier registered in the SCA certificates shall be subject to the name attributes defined in the ITU-T X.520.

3.1.5 Uniqueness of Names

The RCA shall review the uniqueness of the Chinese and English names and distinguished name of Sub-CAs. When the same name or identifier is registered by more than one Sub-CAs, the name or identifier will be assigned to the first applicant.

The name formats of Sub-CAs shall include:

C=TW, O=(Sub-CA English name), OU=(English name of the CA business information of the Sub-CA), CN=(the English name of the CA of the Sub-CA)

The name of the RCA in the self-issued certificate:

C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Root Certification Authority

3.1.6 Name Claim Dispute Resolution Procedures

When more than one Sub-CAs use the same distinguished name, the RCA shall assign the identifier to the first applicant. When there are disputes over this decision, the name specified in the CPS approved by the competent authorities shall prevail.

When the legal documents issued by the competent authorities prove that the distinguished name claimed by the Sub-CA is possessed by another applicant, the RCA shall cancel this distinguished name that has been registered by this Sub-CA and revoked the certificate that has been issued to it. Also, this Sub-CA shall be responsible for the relevant liabilities.

3.1.7 Identification, Authentication and Role of Trademarks

The RCA respects the trademarks of the Chinese and English names of Sub-CAs and shall accept their use of such names. However, the RCA makes no guarantee for the approval, verification and uniqueness of the Sub-CA's trademarks. The arbitration of the relevant disputes shall not be covered in the scope of businesses of the RCA and the RA. Subscribers shall apply for arbitration to the relevant competent authorities.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Sub-CAs shall generate the public key and its corresponding private key that is used in the certificate on their own. They shall also submit to the RCA the PKCS#10 certificate service request(CSR) file signed by the private key as a proof of the private key possession. The RCA shall verify the signature message in the PCKS#10 CSR file submitted by the Sub-CA with the Sub-CA public key in order to validate the Sub-CA's possession of the private key, and the integrity of the private and public key pair and Sub-CA identity information.

3.2.2 Authentication of Organization Identity

When verifying the identity of a Organization Sub-CA, the RCA shall verify the documents issued by the competent authorities or other documents proving its existence. The statutory representative of the Organization shall perform in person the identity verification at the RCA. If the verification is made by the authorized agent the Organization, this agent shall submit his/her identify documents and perform in person the verification of the relevant identity identification data.

3.2.3 Authentication of Individual Identity

The RCA shall not accept a natural person to be an SCA.

3.2.4 Non-Verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

The documents of the statutory representative of a Organization, the agent to the statutory representative of a Organization, and the identity of a Organization shall be issued by a government agency. The RA shall validate the authenticity of the agent's assignment documents.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The longer the time of key use, the higher the risk of key loss or compromise. It is thus necessary for Sub-CAs to change over their keys regularly to ensure key security.

The changeover of certificate keys means to re-generate a pair of public key and private key when the certificate is about to expire and re-apply for a certificate to the RCA as shown in Initial Verification, section 3.2.

3.3.2 Identification and Authentication for Re-Key After Revocation

After the Sub-CA certificate is revoked, Sub-CAs shall repeat the initial verification specified in section 3.2 in order to apply for a new certificate.

3.4 Identification and Authentication for Revocation Request

When a Sub-CA request a certificate revocation, the RCA shall verify the request of certificate revocation. The identity verification shall be conducted according to the procedures specified in section 3.2. If the private key of the Sub-CA has been compromised or there is doubt, the RCA may verify the signature generated with the private key corresponding to the Sub-CA certificate, whether or not the private key is compromised. However, the procedures specified in section 3.2 shall be run again afterwards.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

If the TWCA is not the Sub-CA, the statutory representative or his/her agent of the Sub-CA shall be the certificate applicant.

When the TWCA is the Sub-CA, the certification officer of the Sub-CA shall be the certificate applicant.

4.1.2 Enrollment Process and Responsibilities

Sub-CAs shall read through the terms of use (TOU) in advance to understand the rights and obligations of certificate use. After agreeing to the TOU, applicants shall complete the application form and prepare the original or photocopy of the relevant documents of identity to apply for registration at the RCA.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The Sub-CA shall follow the procedures below to apply for a certificate.

(1) The Sub-CA statutory representative or his/her agent shall be the applicant to apply for the certificate on behalf of the Sub-CA.

(2) The Sub-CA shall submit in correspondence the certificate application form, the self-generated PKCS#10 CSR file, CPS, CP and CPS cross reference table, and the report of an external audit conducted by an unimpaired third-party. The Sub-CA shall affix the seal of the Sub-CA statutory representative and the seal of the organization, and such seals shall be identical to the seals that are used in the registration of organizational establishment at the competent authorities.

(3) The applicant shall bring the above data/documents, his/her ROC Citizen Identity Card, and the power of assignment of the Sub-CA to the RCA to complete the application formalities. The RCA shall perform the identity identification and verification according to the procedures specified in section 3.2.

(4) The RCA shall examine if the Sub-CA’s CPS complies with the CP based on the CP and CPS cross-reference table submitted by the Sub-CA.

(5) The PMA shall review the documents and data submitted by the Sub-CA and the examination results of the RCA to determine if the application is accepted, or

additional data shall be submitted, or is rejected.

(6) After the application is accepted, the TWCA and the Sub-CA applying for the certificate will discuss about the contract terms before signing the contract.

(7) After the contract is signed by both parties, the certificate issue procedure will begin.

The procedure for certificate application when the TWCA is a Sub-CA:

i. The Sub-CA certification officer shall be the applicant.

ii. The applicant shall submit a personally signed certificate application form and the PKCS#10 CSR approved by the authorized personnel.

iii. The PMA shall review the content of the application form and CPS for compliance with the CP.

iv. The certificate issue procedure will begin after the PMA approval.

4.2.2 Approval or Rejection of Certificate Applications

After completing the identification and verification procedures in section 4.2.1, the application for certificates shall be deemed as accepted. When it is unable to complete the above identification and verification procedures, the application for certificates shall be rejected.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The certificate issuing procedures of the RCA are as follows:

(1) Sub-CAs shall mail the CSR file generated by themselves according to the PKCS#10 format and the certificate application form to the RCA.

(2) The RCA shall validate if the CSR file submitted by the Sub-CA is generated by the Sub-CA.

(3) The integrity of the CSR file in the PKCS#10 format is validated by verifying the digital signature. The subject identifier in the CSR file shall be inspected for consistency with the subject identifier in the certificate application form and application extension field.

(4) After all items are correct, the RCA shall immediately issue the certificate to the

Sub-CA. The issued certificate shall be delivered to the Sub-CA either offline or online.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

After issuing the certificates, the RCA shall notify the Sub-CA by either phone or email. After confirming with the Sub-CA, the certificate shall be delivered to the application either offline or online.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

After receiving the certificate, Sub-CAs shall perform the following procedures.

(1) Check if the certificate contents are consistent with the application contents and the CA information is correct.

(2) Check if the certificate public key is consistent with the public key information in the PKCS#10 certificate application file.

(3) Verify the certificate validity and legitimacy with the RCA self-issued certificate.

(4) Immediately report to the RCA to revoke the certificate if the above procedures cannot be performed and apply for the re-issue of certificate according to section 4.3.

(5) After receiving the certificate, applicants shall sign the acceptance confirmation document and notify the RCA in writing. Sub-CAs shall specify that they have fully understood the rights and obligations of certificate use in the confirmation document. If Sub-CAs fail to notify the RCA within 30 calendar days from receiving the certificate, this shall be considered as a rejection of the certificate and the RCA shall immediately revoke the certificate. However, Sub-CAs may apply for the re-issue of certificate according to procedures specified in section 4.3 within 30 calendar days.

4.4.2 Publication of the Certificate by the CA

After the Sub-CA completed the acceptance procedure, the RCA shall immediately publish on the repository the certificate issued to the Sub-CA.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The usage, scope and limitations of the Sub-CA certificate are specified in section 1.4

When there are doubts of private key fraud, exposure or loss, Sub-CAs shall report to the RCA.

4.5.2 Relying Parties Public Key and Certificate Usage

Prior to trusting a Sub-CA certificate issued by the RCA, the relying parties shall carry out at least the following required procedures in order to use it to verify the digital signature signed by the Sub-CA.

(1) To acquire the RCA self-issued certificate through the appropriate and secure channel.

(2) To check if the Sub-CA certificate has expired.

(3) To verify the digital signature signed by the RCA included in the Sub-CA certificate with the public key contained in the RCA self-issued certificate.

(4) To check if the Sub-CA certificate has been revoked by the RCA.

If the Sub-CA certificate fails to pass the above verification, this suggests that the Sub-CA certificate obtained by the relying parties is not issued by the RCA or invalid, and the relying parties shall not trust this Sub-CA certificate.

4.6 Certificate Renewal

A certificate renewal means the issue of a new certificate using the same subscriber information and containing the same key but a different serial number and an extended validity.

4.6.1 Circumstances for Certificate Renewal

The RCA shall not accept the renewal of Sub-CA certificates.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Procedures of Renewed Certificate Acceptance

Not applicable.

4.6.6 CA Publication of Renewed Certificates

Not applicable.

4.6.7 Issue of CA Notice of Extended Certificates to Other Authorities

Not applicable.

4.7 Certificate Re-Key

The changeover of a certificate key means the generation of a new public and private key pair and application for the issue of a certificate to the CA with the original registration information.

4.7.1 Circumstances for Certificate Re-Key

As specified in section 3.3.1.

4.7.2 Who May Request Certification of a New Public Key

Sub-CAs shall be eligible for changing over the certificate key.

4.7.3 Processing Certificate Re-Keying Requests

- Identify and verify the identity of subscribers according to section 3.3.
- Issue the certificate according to section 4.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

Subject to section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Subject to section 4.4.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Subject to section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Subject to section 4.4.3.

4.8 Certificate Modification

A certificate change means the issue of a new certificate after changing the identifier information of the subscriber name, without changing the public key of the certificate.

4.8.1 Circumstances for Certificate Modification

The RCA shall not accept the request of certificate change from Sub-CAs. Sub-CAs changing the identification information or information registered in the certificate shall apply for a new certificate according to sections 4.1-4.4.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Under any of the following circumstances that a Sub-CA may apply for certificate revocation:

(1) Sub-CAs wish to terminate the use of a certificate.

(2) It is necessary to correct the information errors in the valid Sub-CA certificate.

(3) The relevant private key of the Sub-CA certificate is proven or alleged to be compromised, damaged, lost, exposed and/or interpolated.

When a Sub-CA violated the laws and regulations of the competent authorities and/or breaches the CP, this CPS or the contract signed with the TWCA, the RCA shall revoke its SCA certificate without prior notice.

When the above situations occur, the relevant certificate shall be revoked and added to the CRL. All revoked certificates shall be included in the CRL published later than the revocation, until they are expired.

4.9.2 Who Can Request Revocation

(1) Sub-CAs;

(2) the RCA; and

(3) the competent authorities or a court of law.

4.9.3 Procedure for Revocation Request

Sub-CAs shall apply for certificate revocation according to the following procedures:

(1) The Sub-CA statutory representative or his/her agent shall be the applicant to apply for the certificate revocation on behalf of the Sub-CA.

(2) Sub-CAs shall submit a certificate revocation application form in writing specifying the certificate(s) to be revoked and the reasons for revocation, and affix the seal of the Sub-CA statutory representative and the seal of the organization, and such seals shall be identical to the seals that used in the registration of organizational establishment at the competent authorities.

(3) The applicant shall bring the above data/documents, his/her ROC Citizen Identity Card, and the power of assignment of the Sub-CA to the RCA to complete the application formalities. The RCA shall perform the identity identification and verification according to the procedures specified in section 3.2.

(4) After reviewing the application for certificate revocation and obtaining the PMA approval, the RCA shall revoke the Sub-CA certificate within one workday.

(5) If it is necessary to immediately revoke an Sub-CA certificate when the key of the Sub-CA certificate is proven or alleged to be compromised or involved in security problems, Sub-CAs may notify the RCA to revoke the problematic Sub-CA certificate with an electronic message signed digitally or protected with other security mechanisms valid for verifying the identity of the Sub-CA; provided that the Sub-CA shall complete the procedures in (2)-(4) afterwards.

The procedures for applying for certificate revocation or immediate certificate revocation by the TWCA as a Sub-CA:

(1) The certification officer shall be the applicant.

(2) The applicant shall submit a personally signed certificate revocation application form. After obtaining the PMA approval, the revocation personnel shall revoke the certificate within 3 workdays.

4.9.4 Revocation Request Grace Period

Sub-CAs shall apply for certificate revocation within 10 workdays from the occurrence of the reasons for certificate revocation.

4.9.5 Time Within Which CA Must Process the Revocation Request

The RCA shall complete the revocation within one workday from receiving the request of certification revocation from the Sub-CA.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties shall determine the interval for enquiring (or downloading) the revocation data (CRL) according to their risk, responsibility and consequences.

When verifying the digital signature of a Sub-CA certificate with the Sub-CA certificate issued by the RCA, relying parties shall check if the certificate has been revoked.

4.9.7 CRL Issuance Frequency

The RCA shall update and issue the CRL at lease once every 24 hours.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-Line Revocation/Status Checking Availability

The RCA does not provide the online certificate status protocol (OCSP).

4.9.10 On-Line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related To Key Compromise

When the signature key is compromised, the RCA shall follow the instructions below:

(1) Generate the new signature key pair and the corresponding certificates.

(2) Revoke all issued certificates and issue CRL with the new signature key. The CRL shall include all issued but still valid certificates (including revoked certificates issued before the key is compromised).

(3) Notify Sub-CAs.

(4) Securely deliver the new certificates to Sub-CAs.

(5) Issue new certificates to Sub-CAs with the new signature key.

When the key of an Sub-CA is compromised, the Sub-CA shall report to the RCA within 24 hours.

4.9.13 Circumstances for Suspension

The RCA does not offer the certificate suspension service.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Service

4.10.1 Operational Characteristics

Please refer to sections 4.9.9 and 4.9.11.

4.10.2 Service Availability

Please refer to sections 4.9.9 and 4.9.11.

4.10.3 Operational Features

Please refer to sections 4.9.9 and 4.9.11.

4.11 End of Subscription

Certificates issued by the RCA shall be invalid when they are expired, revoked by the Sub-CA, or when the RCA shuts down its business.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No key escrow shall be allowed for the RCA and Sub-CA keys.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Managerial and Operational Control

5.1 Physical Controls

5.1.1 Site Location and Construction

The construction of the site location of RCA shall comply with the standards of computer rooms for storing highly important and sensitive information and be equipped with physical security controls, such as access control, security, intrusion detection, and the CCTV system, in order to prevent unauthorized access to certificate-related equipment of the RCA.

5.1.2 Physical Access

The physical controls of the RCA are as follows:

(1) Three levels of access control with identity clearance (IC card or fingerprint) of more than two persons at the same time; 24-hour dynamic CCTV monitoring and recording, and the IrDA intrusion detection alarm system are applied to record the entry status of the computer room and prevent unauthorized entry.

(2) The RCA private key and its backup are properly and securely stored in a vault protected by the CCTV system. Certificate management shall be implemented by at least two certificate system operators at the same time, and the entire process is monitored and recorded by the CCTV system.

(3) The hardware and software equipment and hardware cryptographic modules are sited in environments protected by the CCTV system, and key management shall be implemented by at least two persons at the same time.

5.1.3 Power and Air Conditioning

The RCA is equipped with a diesel generator and uninterrupted power supply (UPS). When the ordinary power supply system fails, the diesel generator will automatically take over the power supply of the RCA. The power supply during the takeover is maintained by the UPS.

The RCA is equipped with an independent air-conditioning system to ensure system operation stability and provide the optimal work environment. The air-conditioning system is maintained and tested at planned intervals.

5.1.4 Water Exposures

The RCA computer room is a sealed building built with reinforced concrete, except the interior accesses. Elevated flooring is installed to prevent flooding.

5.1.5 Fire Prevention and Protection

The RCA is built with fireproof materials and equipped with the central fire extinguishing system activated automatically when a fire is detected.

5.1.6 Media Storage

The media storage environment of the RCA can avoid accidental damage of media, including magnetic shielding, antistatic equipment and environment for magnetically sensitive media. The media storing the backup copies of important data are stored in the fireproof vault, and the storage media of one backup copy are stored in the disaster recovery site protected with security controls.

5.1.7 Waste Disposal

The hardware equipment, disks, and cryptographic equipment of the RCA storing commercially sensitive and private information are securely removed and destroyed and verified by the audit unit prior to disposal, and records are maintain.

Documents and storage media containing commercially sensitive and private information shall be securely removed and destroyed prior to disposal to ensure that such information shall not be recovered, accessed and re-used. These documents and storage media shall be verified by the audit unit, and records are maintained.

5.1.8 Off-Site Backup

The RCA is equipped with a disaster recovery computer room and the relevant backup equipment. When equipment for routine operations is unable to operate properly as a result of an external influence, the backup equipment can maintain the continual operations of the RCA.

Backup copies of the media information and documentation required for operating the RCA stored in the disaster recovery site equipped with temperature and humidity controls, magnetic shielding and antistatic facilities, CCTV system, and maximum access control.

All backup log files of the RCA are stored in the disaster recovery computer room with maximum security control.

5.2 Procedure Controls

5.2.1 Trusted Roles

Under the PKI framework, the RCA shall perform certificate management with well-laid and secure operating procedures. In order to ensure optimal duty assignment and that the disaster recovery assignment shall not affect system security and operation integrity, the trusted roles of the RCA and their duties are as follows:

(1) Administrator: To be responsible for system installation, management, and environment parameter setup.

(2) Officer: To be responsible for issuing and revoking certificates.

(3) Auditor: To be responsible for internal audits, and the review and maintenance of audit records.

(4) Operator: To be responsible for routine maintenance, such as data backup, data recovery, and website data maintenance.

5.2.2 Number of Persons Required per Task

The number of persons required per role is:

(1) Administrator: at least two.

(2) Officer: at least two.

(3) Auditor: at least one.

(4) Operator: at least two.

5.2.3 Identification and Authentication for Each Role

The access to system resources of RCA administrators, officers, auditors and operators is assigned by duty; and a distinguished name, IC card, and relevant passwords are applied to ensure the identification and verification of trusted roles.

A detailed record is maintained for every operation operated by the relevant operators for carrying out their duty to ensure the accountability of system resource availability and to assess the threats and risks of system security.

5.2.4 Roles Requiring Separation of Duties

(1) An officer and the administrator shall not be the same person.

(2) An officer and the auditor shall not be the same person.

(3) An administrator and the auditor shall not be the same person.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

(1) RCA operators shall be loyal and enthusiastic to their work and reliable; and shall not engage in sideline jobs that may affect their certification work or have a criminal and/or bad credit record.

(2) An officer shall have at least practical certification experience or complete the relevant training and tests.

(3) An administrator shall have at least practical experience in certification, and the planning, operations and management of computer systems.

5.3.2 Background Check Procedures

The personnel management department shall conduct the background clearance of RCA personnel. The relevant departments shall review the practice and experience of personnel. Only personnel that pass the review are allowed to work at the RCA. The practice and experience of personnel of various levels and functions shall be reviewed once a year as a reference to determine if they are qualified for their work or to adjust their duty.

5.3.3 Training Requirements

RCA operators are educated and trained with the required skills and knowledge concerning the RCA operations according to their duties. These include hardware and software functions, operating procedures, security procedures, disaster recovery procedures, key management procedures, certificate policy, this CPS, and other related information security requirements. Education and training appropriate to the system modification or updates and upgrades are also provided.

Complete education and training procedures are established for the hardware, software, application, and security management systems of the certification management system. The relevant skill education and training is provided for new employees or after system changes. Records of on the effects of training are maintained as a reference for work assignment.

5.3.4 Retraining Frequency and Requirements

The RCA shall review the skills and knowledge related to the operation of certificate management systems for operators at least every year and give them appropriate education and training. Relevant education and training will be provided for operators after the update or upgrade of system functions and PKI or addition of new systems.

5.3.5 Job Rotation Frequency and Sequence

(1) An administrator shall be transferred to an officer or auditor after leaving the administrator post for one full year.

(2) An officer shall be transferred to an administrator or auditor after leaving the administrator post for one full year.

(3) An auditor shall be transferred to an administrator or officer after leaving the administrator post for one full year.

(4) Operators shall be transferred to an administrator, officer or auditor after working as an operator for 2 full years, receiving relevant education and training, and passing the evaluation.

5.3.6 Sanctions for Unauthorized Actions

Operators of the RCA certification management system carrying out operations outside of their duties, either intentionally or out of negligence and regardless of causing or not causing harm to the security of the certification management system, shall be immediately reported to the supervisor to take actions according to the relevant rules and regulations.

5.3.7 Independent Contractor Requirements

When it is necessary for the RCA to outsource work to a third-party due to staffing shortage, the background clearance of personnel from the third part shall be conducted according to section 5.3.2, and relevant education and training shall be provided. These third-party personnel shall be requested to sign the non-disclosure (confidentiality) agreement with the RCA and shall follow the rules and regulations and regulatory requirements concerning the work in which they engage. The rights and obligations of these third-party personnel shall be the same as that of the RCA personnel.

5.3.8 Documentation Supplied to Personnel

The RCA shall provide the operating documentations for personnel to carry out their work in order to ensure the normal operation of the certification management system. Such documentations shall at least include:

(1) the operating manuals of system hardware and software, network system, website, and cryptographic system;

(2) the operating documentations of the RCA certification management systems;

(3) this CPS, CP and relevant SOPs; and

(4) the RCA internal operating documentations, such as the system redundancy and recovery SOPs, disaster recovery SOPs, and routine work SOPs.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Either manually or automatically recorded, RCA audit records shall include at least the following items:

- Type of event
- Event date and time
- Event results (success or failure)
- Entity or individual evoking the event

The types of audit events recorded by the RCA include:

(1) Security audits

- Any changes of important audit parameters, e.g. the contents of the types of audit events and new and old parameters.
- Any attempt to delete or modify the audit logs.

(2) Management, identification and authentication of personnel and trusted roles

- New role setup, either a success or a failure
- The maximum counts of attempts of identity authentication
- The maximum counts of failures of identity authentication for user login
- Administrator’s unlocking of a locked account.
- Administrator’s change of the system identity authentication mechanism, e.g. changing password into biometrics.

(3) Key operating procedures

- Key generation
- Key destruction

(4) Loading and storage of private keys

- Loading private keys to system components

(5) Addition, deletion and storage of trustee public keys

- Changes of trustee public key, including addition, deletion and storage

(6) Output of private keys

- Output of private keys (not including one-time keys)

(7) Registration of certificates

- The registration application procedures of certificates

(8) Revocation of certificates

- The revocation application procedures of certificates

(9) Approval of certificate status change

- Approval or rejection of applications for certificate status change

(10) Configuration

- Changes of the security configurations

(11) Account management

- Addition or removal of roles and users
- Modifications of user account or role access authority

(12) Management of certificate format profiles

- Changes of certificate format profiles

(13) Management of CRL formation profiles

- Changes of CRL formation profiles

(14) Important events of system installation and operations

- Installation of operating systems
- Installation of certification management systems
- Installation of hardware cryptographic modules
- Removal of hardware cryptographic modules
- Destruction of hardware cryptographic modules
- Activation system
- Attempts to log in the certification management system
- Acceptance of hardware and software
- Attempts to set passwords
- Attempts to modify passwords
- Backup of RCA internal data
- Recovery of RCA internal data
- File operations (e.g. creation, rename and move)
- Sending information to the repository
- Access to the RCA internal database
- Key compromise
- Key changeover of the RCA or Sub-CAs

(15) Changes of RCA server settings

- Hardware
- Software
- OS
- Patches
- Security format profiles

(16) Physical access and site security

- Personnel access to the RCA computer room

- Access to the RCA servers
- Acknowledged or alleged violation of physical security regulations

(17) Abnormal events

- Software errors
- Failure in software integrity check
- Receiving of messages of incorrect formats
- Messages from abnormal routing
- Network attacks (probable or confirmed)
- Equipment failure
- Improper power supply
- UPS failures
- Distinct and critical network service or access failures
- Breaches of the CPS
- System clock reset

5.4.2 Frequency of Processing Log

The RCA shall review the audit records at least once a month to trace and investigate events that have occurred. The review shall include the non-interpolation of audit records, all record items, and any warning or anomaly. The causes of such events shall be investigated and the preventive actions for their recurrence proposed. Records of the record review results shall be maintained.

5.4.3 Retention Period for Audit Log

The relevant audit records and reports and media data shall be retained for at least two months.

5.4.4 Protection of Audit Log

(1) Audit records shall only be accessed by authorized personnel; and only authorized personnel shall make backup copies of audit records.

(2) Electronically archived audit records shall be protected with signature or encryption technology and stored in write-only DVDs or other write-only media.

(3) The key for protecting event records shall not be used for other purposes.

(4) Paper or physical audit records shall be stored in a secure place.

5.4.5 Audit Log Backup Procedures

Back up copies of electronic audit records shall be made at least once a month, and a copy shall be stored in a disaster recovery location with maximum security control outside of the RCA.

5.4.6 Audit Collection System (Internal vs. External)

The audit system is built in the RCA certification management system. The auditing procedure shall be activated when the system is started up and stop when the certification management shuts down.

Where the automatic audit system is unable to work properly, and the security mechanisms protecting system data integrity and confidentiality are at high risk, the RCA shall suspend all certificate issue services until the problem has been removed.

5.4.7 Notification to Event-Causing Subject

When an event is recorded by the audit system, it is no need for the audit system to notify the related entity generating that the event has been recorded by the system.

5.4.8 Vulnerability Assessments

The following vulnerabilities shall be assessed once a year:

(1) operating system vulnerability

(2) physical facility vulnerability

(3) certification management system vulnerability

(4) network vulnerability

5.5 Record Archival

5.5.1 Types of Records Archived

The archival records of RCA shall include:

(1) The audited accreditation data

(2) CPS

(3) Sub-CA contracts

(4) System and equipment configurations

(5) Contents of modifications and updates of system or configurations

(6) Certificate application data

(7) Revocation application data

(8) Validation documents of certificate acceptance

(9) Issued or published certificates

(10) RCA key changeover records

(11) Issued or published CRLs

(12) Audit records

(13) Other descriptive data or applications for verifying and authenticating archive contents

(14) Documented requirements of public auditors

(15) Data for verifying SCA identity

5.5.2 Retention Period for Archive

The RCA archive data shall be retained for at least 15 years.

5.5.3 Protection of Archive

No writing, modification or deletion of archival data shall be allowed. Archival individual data of SCAs are allowed for retrieval by the respective SCAs and legally approved agencies.

A copy of archival data shall be retained in another site equipped with security controls and harmless to the storage media.

5.5.4 Archive Backup Procedures

Keys, certificates and transaction data shall be archived and backed up on a daily, weekly and monthly bases according to the backup and disaster recovery operating procedures. A copy shall be retained at the TWCA in an environment with security controls, and another copy in the DR site equipped with security controls. When the certification system cannot be started up properly, personnel shall recover the system according to the system backup and recovery manual with the backup data.

5.5.5 Requirements for Time-Stamping of Records

Archived electronic records (e.g. certificates, CRLs and audit records) shall include the date and time information. These records shall be protected with the digital signature or encryption to detect if the date and time information contained in the records has been interpolated. However, instead of the electronic time stamp data from the unimpaired third-party, the date and time information contained in these electronic records shall be the system date and time.

The date and time of all RCA computer systems shall be calibrated at planned intervals to ensure the accuracy and reliability of the date and time in the electronic records.

Archived paper records shall also contained a date, and time shall also be recorded where necessary. The date and time in paper records shall not be changed without prior permission, and all date and time corrections shall be validated by the auditor.

5.5.6 Archive Collection System (Internal or External)

The archive records of the RCA shall be generated by TWCA personnel in an environment with independent resources and security controls. Information collected in the audit records are also generated by the internal control system. The archival records of documents related to certification system operations are collected and managed by the responsible personnel.

5.5.7 Procedures to Obtain and Verify Archive Information

The retention records related to the operations of the certification system shall be verified according to the internal management regulations of the TWCA at least once a year.

5.6 Key Changeover

In order to minimize the risk of others cracking the RCA signature key, the RCA shall change over its signature key at plant intervals.

The validity of the RCA signature key shall be identical to the lifecycle of its corresponding certificate, and the lifecycle of certificates shall not exceed 30 years.

When changing over a key, the RCA shall generate a new key pair and the self-issued certificate, and then provide them for relying parties to download according to section 6.1.4.

When selecting the key validity, Sub-CAs shall consider the key length, protection, controls and other factors of the key, and shall not violate section 6.1.5.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

When the key is compromised or lost (though not yet determined as compromised), RCA shall handle the situation according to the following procedures:

- Notify all Sub-CAs as soon as possible with secure emails or in writing.
- Generate a new key pair and the self-issued certificate according to section 6.1.
- Revoke all issued certificates and issue the CRL with the new signature key. The CRL shall include the information of all issued but still valid certificates (including certificates revoked prior to the cracking of the key).

- Issue new certificate to all Sub-CAs according to the procedures specified in section 4.3.

The RCA shall investigate and report to the PMA the causes of a cracked or lost key and actions taken to prevent their recurrence.

As a trust anchor, the RCA uses a self-issued certificate that it is not necessary to verify the new public key with the original public key.

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

The RCA shall establish and maintain the procedures for recovering damage on its computer resources, software and data, and shall carry out an exercise every year.

When the computer equipment is damaged or unable to work but the signature remains intact, the RCA shall recover the repository operation in the first priority and restore the issue, revocation and management of certificates.

5.7.3 Entity Private Key Compromise Procedures

When a Sub-CA has doubts about the key is compromised, it shall handle the situation according to the procedures specified in section 4.9.3.

5.7.4 Business Continuity Capabilities After a Disaster

When the RCA is unable to restore certification services within 24 hours after a natural disaster or other disasters, it shall activate the facilities in the DR site to restore the certification services within 24 hours.

5.8 CA or RA Termination

When the RCA terminates its services, it shall follow the procedures specified in the Electronic Signature Law.

When the RCA shuts down its businesses, it shall minimize the impacts on system operations by transferring the certification services to other CAs.

The RCA shall notify the competent authorities 30 days prior to the termination of services.

(1) The RCA shall notify the Sub-CAs and publish on the repository the services to be terminated and the services to be taken over by other CAs three months prior to the termination of services.

(2) When the RCA shuts down its business, the relevant private keys and certificates shall be transferred to the CA taking over the business when the operating environment has no security doubts.

(3) The CP, CPS, CA-related operating manuals and documentations, subscriber contracts and registration data, audit records, archived data, certificate status data, and other documents required for taking over the business shall be transferred to the CA taking

over the business.

(4) The RCA shall expunge all relevant private keys and officially announce to the Sub-CAs that the business has been transferred to the CA taking over the business.

When shutting down the business, the relevant rights and obligations of the RCA shall also be arranged according to the terms and conditions specified in the contract signed with the Sub-CAs.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Based on the procedures specified in section 6.2.1, the RCA shall produce the RSA key pair with the hardware cryptographic module complying with CNS 15135, ISO19790 or FIPS 140-2/Level 3. After generation, the private key will be stored in the hardware cryptographic module without leakage.

The key shall be generated in the presence of a third-party witness who shall sign the key generation certificate after the generation as a sign of trust.

6.1.2 Private Key Delivery to Subscriber

The RCA does not generate the key pair for Sub-CAs.

6.1.3 Public Key Delivery to Certificate Issuer

The Sub-CA public key is delivered to the RCA with the PKCS #10 application file. The key shall be delivered in a diskette or disc together with the letter of application. The possession of private key shall be verified according to the procedures specified in section 3.2.1.

6.1.4 CA Public Key Delivery to Relying Parties

The RCA shall publish its self-issued certificate and the Sub-CA certificates it issues to the repository for relying parties to enquire and download.

6.1.5 Key Sizes

The size of RCA RSA key shall at least be 2048 bits.

The size of the Sub-CA RSA key shall at least be 1024 bits.

6.1.6 Public Key Parameters Generation and Quality Checking

The RCA uses the RSA (Rivest, Shamir and Adleman) encryption algorithm, and there is no key parameter. The prime generator generates the RSA-required primes with the ANSI X9.31 algorithm to ensure the prime is a strong prime.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The key usage extension field in X.509v3 certificate issued to the Sub-CAs is for the keyCertSign and cRLSign.

6.1.8 Generation Equipment of Subscriber Keys

Sub-CAs shall use the hardware cryptographic module comply with CNS15135, ISO19790, or FIPS140-2 (or FIPS140-1)/Level 3.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The RCA shall protect private keys with the cryptographic module complying with the FIPS140-2/Level 3 and with multiple control.

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

The m-out-of-n multiple person control is applied to the RCA private key. It is a perfectly secret way of secret sharing for secure private key backup and recovery in order to maximize the security control for the RCA private key.

The IC card and PIN protecting the private key information are controlled by different administrators of different duties and stored in an environment with security control.

6.2.3 Private Key Escrow

Not applicable.

6.2.4 Private Keys Backup

(1) The RCA private key is stored inside the hardware cryptographic module after encryption and back up copies of the key are made after it is encrypted according to the multiple control specified in section 6.2.2, and the multiple control information of the encrypted key is stored in the highly secured IC card.

(2) The IC card where the multiple control information of the encrypted key is stored is sited in a secure environment with dual security control and kept by the security control personnel after sealing.

(3) At least two copies of the multiple control information of the encrypted key are kept. One copy is stored in a secure place within the RCA and another one in the DR site with security controls.

6.2.5 Private Key Archival

The RCA does not archive the RCA private key.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The RCA private key is generated by and stored in the hardware cryptographic module. It shall only be input to another hardware cryptographic module for making backup copies and recovery. The RCA private key shall be retrieved from the hardware cryptographic module according to the procedures specified in section 6.2.4.

6.2.7 Private Key Storage on Cryptographic Module

The RCA private key is stored in the hardware cryptographic module after encryption.

6.2.8 Method of Activating Private Key

Private keys stored in the cryptographic module shall be activated by at least two authorized officers after identity authentication. The identification of officers shall be authenticated with the IC card, and the activation control procedures shall comply with the section 5.2.

6.2.9 Method of Deactivating Private Key

The RCA operates in the offline mode. Therefore, the RCA private key is in the deactivated mode in general to prevent illegal use of the private key.

After the private key is activated, it is deactivated either manually by turning off the hardware cryptographic module or automatically by the system after the idling timeout to prevent illegal use of the private key.

6.2.10 Method of Destroying Private Key

The RCA shall destroy the private key when it is expired. Therefore, after the private key is expired, the RCA shall expunge the old private key in the cryptographic module by means of zeroization.

6.2.11 Cryptographic Module Rating

The hardware cryptographic module that used by RCA shall comply with the CNS15135, ISO19790 or FIPS 140-2/Level 3.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The RCA shall archive the certificates it issues when they are expired, including the public keys.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity of the RCA public and private keys shall be the same.

The validity of the public and private keys of this RCA and its Sub-CAs varies according to the key length described as follows:

(1) RSA 2048-bit key pair: maximum 30 years.

(2) RSA 1024-bit key pair: maximum 10 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data of signature private key shall be generated with various IC cards and controlled by multiple parties by means of duty separation. The activation data in the IC card shall be retrieved by the card reader authenticated by the personal identification number (PIN).

6.4.2 Activation Data Protection

The activation data shall be protected by means of IC card. The IC card PIN shall be kept by the responsible personnel and shall not be recorded in any media. The IC card shall be locked after three login failures. When handing out the IC card, the new keeper shall change the PIN.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Control

6.5.1 Specific Computer Security Technical Requirements

Te RCA shall provide the following security controls from the operating system or by integrating the operating system, software and hardware protection technologies.

(1) System login mechanism with identity identification and authentication

(2) User-defined access control

(3) Security audit capability

(4) Access control constraints of certification services and trusted roles

(5) Identity identification and authentication of trusted roles

(6) Communication and database security

(7) Secure and trusted channels for the identity authentication of trusted roles

(8) Procedural integrity and security control protection

6.5.2 Computer Security Rating

The RCA computer systems shall comply with at the TCSEC C2 or equivalent international information security standards.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The RCA certification management system shall be developed according to the ISO/CNS 27001 International Standard.

The RCA hardware and software is intended for dedicated use only the components comply with the safety policy. No irrelevant hardware devices, network connection or component software shall be installed and operated in the RCA system. The system shall be scanned for malware prior to use.

6.6.2 Security Management Controls

When installing software installed for the first time, the RCA shall validate that the software shall be the legally licensed and unmodified version provided by the developer. The RCA shall also verify the software integrity prior to activation every time.

The RCA shall record and control changes in the system configurations and functions.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The certification management system of the RCA shall be an offline and independent system and operated by authorized personnel of relevant business manually. The firewall, IDS, and antivirus systems shall be installed and implemented to prevent network intrusions and damage in order to ensure network security.

The RCA server and internal database shall not be connected to external networks. The repository shall be connected to the Internet to deliver uninterrupted certificate and CRL query services (except for necessary maintenance or recovery).

The RCA repository data (e.g. CRL) shall be updated and published manually in offline mode.

The RCA repository shall be protected with patch update, system vulnerability scan, IDS and firewalls in order to prevent attacks, such as denial of service (DoS) and intrusions.

6.8 Time Stamps

No stipulation.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profiles

7.1.1 Version Number(s)

Both the self-issued certificate and certificates issued to Sub-CAs shall be in the X.509 v3 version.

7.1.2 Certificate Extensions

The use of certificate extensions shall comply with the IETF RFC 3280. Please see the RCA certificate and CRL format profiles for details of certificate fields.

7.1.3 Algorithm Object Identifiers

The algorithm OIDs for certificate issued by the RCA are as follows:

Algorithm Type	Algorithm	OID
Key	rsaEncryption	{iso(1)member-body(2)us{840}rsadsi(113549)pkcs(1)pkcs-1(1)1}
Signature	sha1WithRSAEncryption	{iso(1)member-body(2)us{840}rsadsi(113549)pkcs(1)pkcs-1(1)5}
Signature	sha256WithRSAEncryption	{iso(1)member-body(2)us{840}rsadsi(113549)pkcs(1)pkcs-1(1)11}

7.1.4 Name Forms

The format of the subject and issuer name of certificates issued by RCA and Sub-CAs shall comply with the X.500 Distinguished Name (DN) format. The attributes of the DN shall comply with the RFC 3280.

7.1.5 Name Constraints

When issuing certificates, the RCA may use the nameConstraints extension if necessary.

7.1.6 Certificate Policy Object Identifier

The CP OID defined in the CP shall be applied to the certificatePolicies extension in the certificates issued by the RCA.

7.1.7 Usage of Policy Constraints Extension

The RCA may use the policyConstraints extension in the certificates it issues if necessary.

7.1.8 Policy Qualifiers Syntax and Semantics

The RCA may use syntax containing the policy qualifier (policyQualifier) in the certificates it issues if necessary.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profiles

7.2.1 Version Number(s)

The CRL issued by RCA shall conform to the X.509 v2 format.

7.2.2 CRL and CRL Entry Extension

Please see the RCA certificate and CRL format profiles for details of certificate fields.

7.3 OCSP Profile

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

8. Compliance Audits and Other Assessments

8.1 Frequency and Circumstances of Assessment

The RCA shall conduct an internal audit and an external audit at least once a year.

8.2 Identity/Qualifications of Assessor

CA auditors shall at least be familiar with the CP and this CPS, as well as the audit criteria conforming to the audit. Auditors carrying out the internal and external RCA audits shall at least be equipped with CA and information security audit knowledge, two years of related audit experience, familiar with the CPS, and knowledge and experience of IT system operations and computer hardware and software systems. Where the competent authorities have specified the requirements for auditors, such requirements shall prevail.

An external audit shall be performed by auditors with professional capacity. External auditors shall possess the national auditor license or international audit qualifications and practical experience in RCA audits in order to provide unimpaired and objective audit service. The RCA shall verify the identity of auditors prior to carrying out the audit.

8.3 Assessor's Relationship to Assessed Entity

RCA auditors carrying out the internal audit shall be independent from the work of the audited units and have no conflict of interest that will affect the objectivity of audit. Auditors shall carry out the audit independently in an unimpaired and objective attitude.

The RCA shall assign the external audit to an audit service provider to audit the operations of the RCA.

8.4 Topics Covered by Assessment

The audit items shall include:

(1) whether or not the CPS and relevant operating procedures are established and published, including operating procedures established according to the CPS;

(2) whether or not certification management is carried out according to the CPS and the relevant operating procedures in order to ensure the integrity of certification service and the security controls of RCA environment; and

(3) the conformance of the CPS to the CP.

8.5 Actions Taken as a Result of Deficiency

When detecting nonconformities to the CPS, auditors shall itemize the defects by severity detected in the CA audit and notify the RCA.

The RCA shall propose and implement the corrective and preventive actions for the detected defects. The results of improvements shall be followed up.

8.6 Communications of Results

The RCA shall publish on the repository the results of the latest audit, including, but not limited to, information that may cause security threats to the RCA.

9. Other Businesses and and Legal Matters

9.1 Fees

The fees for the RCA certification services to the Sub-CAs shall be specified in the contract signed between the RCA and Sub-CAs after negotiations between both parties.

9.1.1 Certificate Issuance or Renewal Fees

As specified in section 9.1.

9.1.2 Certificate Access Fees

As specified in section 9.1.

9.1.3 Revocation or Status Information Access Fees

As specified in section 9.1.

9.1.4 Fees for Other Services

As specified in section 9.1.

9.1.5 Refund Policy

Sub-CAs shall not request a refund after accepting the certificate.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

(1) The RCA shall assume no liability for processing the registration data and certification for Sub-CAs, except for the negligence attributable to the RCA.

(2) The RCA shall assume no liability for the damage that caused Sub-CAs due to the certificates issued to the Sub-CAs as a result of an act of God, e.g. wars and earthquakes, or any event that is beyond the reasonable control of the RCA.

(3) The RCA shall compensate the direct damage that caused to a Sub-CA as a result of the RCA personnel's intention or negligence; failure to follow the CPS, CP and the relevant operating procedures when processing the registration, certificate issue and certificate revocation; or violation of the relevant laws and regulations. The amount of maximum damages shall be specified in the contract signed between the RCA and Sub-CA.

(4) After the RCA, or any individual or entity entitled with such right, requests the revocation of a Sub-CA certificate and prior to the RCA's publication of the revocation of such Sub-CA certificate (specified in the CRL), the RCA shall

assume no liability for the legal disputes arising out of or in connection with the use of that Sub-CA certificate by the Sub-CA when the RCA handles such request according to this CPS and the relevant operating procedures.

(5) The RCA shall assume no liability for the damage that caused by the use of a fabricated certificate or incorrect certificate by a Sub-CA.

(6) The validity of the request of damages by the certificate shall be subject to the relevant laws and regulations.

(7) The RCA shall hire an unimpaired and objective third-party auditor to audit the RCA's financial operations every year.

(8) In risk management, in addition to purchasing earthquake and fire insurance for the building and hardware facilities, the RCA is negotiating with domestic and overseas insurance companies for the certification liability insurance.

9.2.2 Other Assets

The RCA is part of the certification business of the TWCA. Prior to purchasing the certification liability insurance, the TWCA will appropriate a sum of NT$30 million as the financial fund for the liabilities of the certification business.

9.2.3 Insurance or Warranty Coverage for End-Entities

The liability for subscribers is specified in section 9.2.1.

Relying parties shall carry out their obligations specified in section 9.6.4. The RCA shall assume no liability for relying parties as a result of violating this CPS or negligence not attributed to the RCA.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Confidential information shall include:

(1) the private key and password for operating the RCA;

(2) the multiple control data for controlling the RCA private key;

(3) Sub-CA application data;

(4) auditable and traceable records generated or retained by the RCA;

(5) the audit records and documentations produced by auditors in the audit; and

(6) operation-related classified documents.

9.3.2 Information Not Within the Scope of Confidential Information

CP, CPS, RCA-issued certificates, RCA-issued CRLs, external audit results (not including information that may cause security threats to the RCA) are information that can be disclosed.

9.3.3 Responsibility to Protect Confidential Information

Under no circumstance shall the RCA disclose the registration basic data and identity verification data of the Sub-CA to the responsible management unit or any individual; except for any of the following:

(1) a request by the law with the authorization of the responsible unit made according to the legal procedure; or

(2) a request or application made according to the legal procedure for a dispute or arbitration arising from or in connection with the certificate referred to a court of law or an arbitration organization with such jurisdiction.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The RCA shall operate according to the Computer-Processed Personal Data Protection Act of the Republic of China.

9.4.2 Types of Personal Privacy Information

Subject to section 9.4.1.

Sub-CAs shall specify in their CPS or Privacy Protection Policy the types of information to be kept confidential.

9.4.3 Information Not Deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

Subject to the relevant laws and regulations.

9.4.5 Notice and Consent to Use Private Information

Subject to the relevant laws and regulations.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Subject to section 9.3.3.

9.4.7 Other Information Disclosure Circumstances

The RCA shall provide the information of Sub-CAs only with the written application made by the Sub-CA. Other parties requesting the provision of Sub-CA information shall obtain the written approval of the respective Sub-CA.

9.5 Intellectual Property Right

(1) The key pair and key multiple control information generated by the RCA shall be the intellectual property of the TWCA.

(2) The certificates and CRLs issued by the RCA shall be the intellectual property of the TWCA.

(3) The Sub-CA key pair shall be the intellectual proper of the corresponding Sub-CA. However, the Sub-CA public key issued in the form of a certificate by the RCA shall be the intellectual proper of the TWCA.

(4) The RCA shall ensure the correctness of the Sub-CA name. This shall not include the ownership of the intellectual property right of such names.

(5) Documentation established by the RCA for carrying out certification management shall be the intellectual proper of the TWCA.

(6) This CPS shall be the intellectual proper of the TWCA.

(7) This CPS is available for free download from the RCA repository or distributed according to the Copyright Act.

(8) No charge shall be collected for the distribution of this CPS.

(9) The RCA assumes no liability for the consequences of the misuse or improper distribution of this CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

(1) The RCA shall keep the registration data, certificate data, and relevant information of Sub-CAs in good faith to prevent the leakage, fraud, interpolation or unauthorized use of such data and information.

(2) The RCA shall accept the information concerning certificate application, certificate changeover, and certificate revocation requested by Sub-CAs; validate the correctness and integrity of relevant information delivered to the RCA by Sub-CAs; carry out certificate issue and revocation; and correctly and securely reply such information to Sub-CAs according to the CP and CPS.

(3) When issuing Sub-CA certificates, the RCA shall verify the authenticity and legitimacy of the application documents and identity of Sub-CAs.

(4) When there are security threats of the RCA private key, the RCA shall immediately notify its Sub-CAs.

(5) When issuing certificates, the RCA shall securely deliver such certificates to the repository according to this CPS.

(6) When revoking a Sub-CA certificate, the RCA shall generate the CRL and securely deliver it to the repository according to this CPS.

(7) Prior to signing a contract with a Sub-CA, the RCA shall explain to the Sub-CA the operating procedures for certificate application, changeover, revocation and use, and the relevant rights and obligations.

(8) The RCA shall use the certificate issuing key and the certificate revocation key independently, and shall not use these keys for other purposes. When it is necessary to sign or encrypt other information, a different key shall be used.

9.6.2 RA Representations and Warranties

As the RCA is also a RA, the responsibility of RA is subject to section 9.6.1.

9.6.3 Subscriber Representations and Warranties

Sub-CAs are the subscribers of the RCA, and their obligations shall include:

(1) When applying for a certificate to the RCA, Sub-CAs shall understand and agree to the rights and obligations specified in the application form and the contract and the relevant regulations in this CPS.

(2) When a Sub-CA has doubts about the Ssub-CA private key is lost or being cracked, or when the Sub-CA has changed its information, it shall report to the RCA according to the relevant operating procedures.

(3) When applying for a certificate, Sub-CAs shall provide detailed and correct information. When accepting the certificate issued by the RCA, Sub-CAs shall validate the correctness of information contained in the certificate and that the

public and private keys are in a pair.

(4) Sub-CAs shall properly generate, retain and use the private key, and shall follow the restrictions on the use of key pairs and certificates.

(5) When a cause of certificate revocation occurs, e.g. private key information leakage or loss, a Sub-CA shall immediately notify the RCA and apply for certificate revocation; provided that the Sub-CA shall be responsible for the risk and liability arising from or in connection with the use of such certificate prior to the publication of certificate revocation.

(6) When the RCA is unable to operate properly, Sub-CAs shall seek other solutions to accomplish the legal behavior for others as soon as possible. Sub-CAs shall not use the improper operation of the RCA as an excuse to avoid their legal responsibility.

(7) Sub-CAs shall store their certificate and CRL in a secure repository and ensure the availability of such repository for relying parties to query at any time.

9.6.4 Relying parties Representations and Warranties

(1) Relying parties shall follow this CPS to acquire the RCA self-issued certificate and the Sub-CA certificate.

(2) Relying parties shall establish and verify the certification chain with the RCA self-issued certificate in order to determine whether or not to trust a Sub-CA certificate.

(3) Relying parties shall verify if the digital signature in the Sub-CA certificate is signed with the RCA private key with the RCA self-issued certificate, and if the Sub-CA certificate has been revoked with the CRL.

(4) Relying parties shall verify the digital signature in the CRL issued by the RCA prior to use in order to validate if the CRL is still valid.

(5) Relying parties shall carefully select a secure computer environment and a reliable AP system. Relying parties shall be in full responsibility for the damage that caused to the rights and benefits of users as a result of their computer environment and/or AP system.

(6) When the RCA is unable to operate properly, relying parties shall seek other solutions to accomplish the legal behavior for others as soon as possible. Relying parties shall not use the improper operation of the RCA as an excuse to avoid their legal responsibility.

(7) When accepting the certificate issued by the RCA, relying parties have expressed that they have understood and agreed to the legal terms and conditions of the RCA, and they shall trust certificates within the scope specified in this CPS.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

(1) The RCA shall assume no liability for processing the registration data and certification for Sub-CAs, except for the negligence attributable to the RCA.

(2) The RCA shall assume no liability for the damage that caused Sub-CAs due to the certificates issued to the Sub-CAs as a result of an act of God, e.g. wars and earthquakes, or any event that is beyond the reasonable control of the RCA.

(3) The RCA shall be responsible for the damage that caused to a third party as a result of the leakage, fraud, interpolation or unauthorized use of the relevant information due to its negligence in retaining the registration and certification data of Sub-CAs.

(4) After receiving an application for certificate revocation, the RCA shall complete the revocation within one workday and issue the certificate revocation list (CRL) and publish it to the repository within one day. A Sub-CA shall take proper action to minimize the effect on relying parties and shall be in full responsibility for the use of such certificate prior to the publication of the CRL.

9.8 Limitations of Liability

When damages arises between the RCA and a Sub-CA as a result of the issue or use of the certificate, the liability of both parties shall be limited to the scope specified in the relevant laws and regulations and the contract.

9.9 Indemnities

Subject to section 9.2.1.

9.10 Term and Termination

9.10.1 Term

After being approved by the competent authorities according to the Electronic Signature Law, this CPS shall be effective immediately after being published on the RCA repository.

9.10.2 Termination

When the new version of the CPS is approved by the competent authorities and published on the RCA repository, the previous version shall be terminated.

9.10.3 Effect of Termination and Survival

After the termination of this CPS, its effect shall continue until the expiration or revocation of the last certificate issued under this CPS.

9.11 Individual Notices and Communications with Participants

The RCA shall establish contact channels with Sub-CAs with proper methods, including, but not limited to, phone, fax and/or email.

9.12 Amendments

9.12.1 Procedure for Amendment

(1) The RCA shall be the responsible unit of this CPS and shall review this CPS as least once a year. The revision method shall include annexing supplementary documents to the CPS or direct corrections of the CPS contents.

(2) This CPS shall be modified when there is an update of the CP or OID.

(3) This CPS shall also be updated when there is a change in the regulatory requirements and/or updates of international standards.

(4) After being approved by the competent authorities, revisions made to this CPS shall be publish on the repository according to section 3.

9.12.2 Notification Mechanism and Period

(1) When there are suggestions for updating this CPS, please send or email such suggestions in detail to the contact window specified in section 1.5.2 for the PMA to review.

(2) After being approved by the competent authorities, revisions made to this CPS shall be publish on the RCA repository for download.

(3) Unless otherwise specified, the RCA shall change the communication mechanisms with Sub-CAs according to section 9.11.

9.12.3 Circumstances Under Which OID Must be Changed

The OIDs quoted in this CPS shall remain unchanged when the contents of this CPS are changed, except the addition of the version identifier of this CPS.

9.13 Dispute Resolution Provisions

When there are disputes arising from or connection with the RCA services and/or the

certificates it issued, Sub-CAs shall settle the disputes according to the following methods:

(1) Both parties shall seek a reasonable resolution in due faith through negotiations.

(2) When both parties are unable settle the dispute within 30 calendar days, a competent and unimpaired third party shall be appointed as the mediator to settle the disputes through consultations. Both parties shall agree to the consultations and decisions made by the mediator.

(3) When both parties are unable concur the consultations and decisions made by the mediator within 60 calendar days, both parties shall agree that the Taipei District Court of Taiwan shall be the jurisdiction court for the first instance of the dispute.

(4) The fees incurred from the negotiations and litigations of the dispute shall be shared according to the negotiation or relevant laws and regulations.

(5) Transnational or trans-regional disputes that cannot be settled through the above methods shall be settled according to the relevant transnational or trans-regional dispute arbitration regulations.

9.14 Governing Law

The contents of this CPS and the relevant RCA businesses shall be implemented and interpreted in accordance with the relevant laws and regulations of the competent authorities and the law of the Republic of China.

9.15 Compliance with Applicable Law

This CPS and the RCA shall comply with the Electronic Signature Law and its bylaws.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Where terms and conditions in this CPS shall be modified as a result of inapplicability, the rest of the terms and conditions shall remain effective and unaffected by the inapplicable terms and conditions until the updated version of the CP is completed and published.

The update of CPS shall be subject to section 9.12.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

The RCA shall assume no liability for an act of God or events beyond the reasonable control of the RCA (e.g. wars or earthquakes).

9.17 Other Provisions

Not specified

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 the human senses but for electronic processing.

(3) Electronic Signature

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

(4) Encrypt/Encipher

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

(5) Decrypt/Decipher

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

(6) Digital Signature

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

(7) Private Key

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

(8) Public Key

In the digital signature using asymmetric cryptosystem, it refers to a set of matching public

digital data for generating and verifying a digital signature. It can be used to verify the correctness of data in messages signed by the signed person, and can encrypt delivery messages when running the message privacy function.

(9) <Public Key>Certification or Certificate

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

(10) Certification Authority or Certificates Authority (CA)

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

(11) Certification Practice Statement (CPS)

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

(12) Asymmetric Cryptosystem

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

(13) Hash Function

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

(14) Issue a Certificate (Electronic Certification)

It refers to the public key certificate or other certificates issued by the certification center (CA) after reviewing the 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
CA	Certification Authority
CC	Common Criteria
CCITSE	Common Criteria for Information Technology Security Evaluation
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
FIPS	Federal Information Processing Standard
ISO/IEC	the International Organization for Standardization, The International Electrotechnical Commission
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificates Status Protocol
OID	Object Identifier
OECD	Organization for Economic Co-operation and Development
PMA	Policy Management Authority
PIN	Personal Identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RCA	Root Certification Authority

RSA	Rivest, Shamir, Adleman (encryption algorithm)
TCSEC	Trusted Computer System Evaluation Criteria
URL	Universal Resources Location