Taiwan-CA Inc. Public Key Infrastructure Certificate Policy (CP)

(Version 2.6.1)

Effective Date: 2024/07/01

Revision Record

Version	Effective	Released by	Description
1.0	1 Apr 2001	TaiCA PMA	CP first issue.
1.1	1 Jan 2002	TaiCA PMA	Revised by integrating TaiCA CA PKI system documentation (CPS, CP etc.) to combine with the TRAVAN EDI PAA CP.
1.2	1 Apr 2002	TaiCA PMA	Revised according to the items to be specified in the Certificate Practice Statement (CPS) and Certification Authority Management Regulations (CAMR) established by the Department of Commerce, MOEA.
1.3	13 Aug 2008	TWCA PMA	Approval of PMA change.
1.4	30 Mar 2009	TWCA PMA	• Supplementation made to the OID to indicates the different assurance level. • Changed the public key validity.
1.5	4 Aug 2009	TWCA PMA	Revised section 6.3.2 according to the resolution made at the PMA meeting on 29 July 2009.
1.6	22 Aug 2012	TWCA PMA	Revised section 1.2 according to the resolution made at the PMA meeting on 22 Aug 2012 to modify OID of EC Security Certificate.
2.0	23 Nov 2012	TWCA PMA	Modify OID of every CA.
2.1	26 Dec 2013	TWCA PMA	Add Device Certificates OID.

2.2	30 Apr 2019	TWCA PMA	• Modified to compliance with CABF Baseline Requirement V1.6.4. • Add CA / Browser Forum Policy OID. • Add AATL Certificate Policy. • Remove Internet NB certificate.
2.3	4 Aug 2021	TWCA PMA	Revised section 6.3.2: • Remove RSA 1024 bits key algorithm. • Add ECC P256 and ECC P384 key algorithms. • Add TSA Certificates OID.
2.4	30 May 2022	TWCA PMA	• Merge Device Certificates to TLS / SSL Certificates. • Remove unused OID in TLS / SSL Certificates and EV SSL Certificates. • Add description for certificate types that BR applies to. • Unified names of TLS / SSL Certificates and EV SSL Certificates

2.5	30 Dec 2022	TWCA PMA	• Revise section 1.2: object identifiers. • Revise section 1.4: certificate usage. • Revise section 3.2.2: authentication of organization. • Revise section 3.2.3: authentication of individual. • Revise section 3.2.3: retention period for archive. • Revise section 7.1.3: algorithm object identifiers. • Rename InfoSec UCA certificate to InfoSec certificate. • Rename TLS/SSL certificate to SSL certificate. • Unify the term of unified CA/Browser Forum specification. • Add sections 1.6, 1.7.
2.6	20 Jul 2023	TWCA PMA	Define the S/MIME certificates and add the related description of S/MIME BR specification.
2.6.1	1 Jul 2024	TWCA PMA	No change in the annual review, version number updated.

1. Introduction

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).

In order to build a secure and trusted network transaction environment; to ensure information transmitted over the network is not fabricated, interpolated or marauded; to authenticate the identity of both parties of transactions and to prevent the repudiation of transactions afterwards, TWCA has established a public key infrastructure (PKI) to be the root

certification authority (RCA) for the trust anchor. TWCA has also established various subordinate certification authorities (Sub-CA) to provide the subscriber network identity and transaction certification services in order to build up the user's faith in e-commerce transactions and to ensure the rights and benefits of both parties.

In order to provide subscribes the certification service required for transactions made over the Internet, TWCA has established the Internet certification service system equipped with the related certification security mechanism. The service system is equipped with the leading-edge public key cryptography with security standards complying with the Electronic Banking Security Control Standards for Financial Institutions announced by the Ministry of Finance. The feature includes the non-repudiation, subscriber identify authentication, verification of information integrity, information encryption, and other forms of security controls required in network transaction security. The system can be applied to e-banking, online ordering, as well as other e-commerce systems, such as insurance, bonds and notes, enterprise enquiries, purchasing, and payment.

1.1 Overview

The certificate policy (CP) of the PKI established by TWCA (collectively known as TWCA PKI CP, or CP), is a technical policy document established in accordance with the Electronic Signature Act and the relevant international standards (e.g. IETF RFC 3647) as a reference for the PKI CAs to establish the certification practice statement (CPS).

In order to cope with the e-commerce security requirements of various businesses, the PKI has included different kinds of CAs. CAs should follow this PKI CP to carry out the operating procedures, usage of certificates, responsibility and authority, and certificate administration specific to their CAs.

Special considerations have been made to the following items when establishing this CP:

1. whether or not relying party can identify the associations between the certificate holder (individual subscriber, corporate subscribers or subscriber of relevant hardware, software and application systems) and the public key specified in the certificate.
2. whether or not relying party can identify if the certificate holder has the corresponding private key;
3. whether or not subscribers and the relying party trust the security of PKI CAs, and their systems, keys, and operating procedures; and
4. the specifications of the Electronic Signature Act.

1.2 Document Name and Identification

1.2.1 Object Identifiers of this CP

Object Identifiers (OIDs) are defined according to the content of certificates, the type of certificates, and the usage of certificates.

The OIDs of this CP are:

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

  (2.16.158.3.1.5.5)

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

  (1.3.6.1.4.1.40869.1.1)

Based on the type of certificates, the OIDs of corresponding CPs are as follows:

Commercial XML Certificate:

- { joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) XML(8) id-CP-policy(5) }

  (2.16.158.3.1.8.5)

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA (40869) certificates(1) policies(1) XML(12) }

  (1.3.6.1.4.1.40869.1.1.12)

Commercial EC Certificate:

- { joint-iso-itu-t(2) country(16) Taiwan(886) TWCA(3) CA(1) EC+(3) id-CP-policy(1) }

  (2.16.886.3.1.3.1)

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) EC(11) }

  (1.3.6.1.4.1.40869.1.1.11)

EC Security Certificate: (No longer used, will be eliminated in the future)

- { joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) EC+(3) id-CP-policy(1) }

  (2.16.158.3.1.3.1)

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) ECSECURITY(24) }

  (1.3.6.1.4.1.40869.1.1.24)

FXML Certificate:

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

  (2.16.158.3.1.5.5)

SSL Certificate:

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) SSL(21) }

  (1.3.6.1.4.1.40869.1.1.21)

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) T WCA(40869) certificates(1) policies(1) DeviceCert(25) }

  (1.3.6.1.4.1.40896.1.1.25) (No longer used, will be eliminated in the future)

EVSSL Certificate:

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

  (1.3.6.1.4.1.40869.1.1.22)

InfoSec Certificate:

- { joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) InfoSec(8) id-CP-policy(5) }

  (2.16.158.3.1.8.5)

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) InfoSec(23) }

  (1.3.6.1.4.1.40869.1.1.23)

AATL Certificate:

- { ISO (1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) AATLCert(26) }

  (1.3.6.1.4.1.40869.1.1.26)

TSA Certificate:

- { ISO (1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) TSACert(27) }

  (1.3.6.1.4.1.40869.1.1.27)

S/MIME Certificate:

- { ISO (1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) SMIMECert(28) }

  (1.3.6.1.4.1.40869.1.1.28)

1.2.2 Object Identifiers of others

The OIDs of CA/Browser Forum are:

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1)}

  (2.23.140.1)

Based on the type of certificates, the OIDs of corresponding CPs are as follows:

TLS BR Organization-validated:

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2) }

  (2.23.140.1.2.2)

EVG:

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) extended-validation(1) }

  (2.23.140.1.1)

S/MIME BR Mailbox-validated:

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) legacy (1)}

  (2.23.140.1.5.1.1)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) multipurpose (2)}

  (2.23.140.1.5.1.2)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) strict(3)}

  (2.23.140.1.5.1.3)

S/MIME BR Organization-validated:

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) legacy (1)}

  (2.23.140.1.5.2.1)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) multipurpose (2)}

  (2.23.140.1.5.2.2)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) strict (3)}

  (2.23.140.1.5.2.3)

S/MIME BR Sponsor-validated:

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) legacy (1)}

  (2.23.140.1.5.3.1)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) multipurpose (2)}

  (2.23.140.1.5.3.2)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) strict (3)}

  (2.23.140.1.5.3.3)

S/MIME BR Individual-validated:

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) legacy (1)}

  (2.23.140.1.5.4.1)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) multipurpose (2)}

  (2.23.140.1.5.4.2)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) strict(3)}

  (2.23.140.1.5.4.3)

CAs under this PKI should specify and use in their CPS the OIDs specified in this CP. Where new OIDs are needed to identify with the new items in the certificate usage, CAs must expand these new OIDs according to the certificate OIDs defined in this CP.

1.3 PKI Participants

All individuals applying this CP shall be the participants of this PKI.

When using on application transaction systems, the public key certificates for a natural person or juristic person specified in this CP provides the identification and authentication of the identify of both the activator and recipient of the transaction; authentication of information integrity; information privacy protection; the applicability and the rights and obligations of the non-repudiation mechanism; and the rules for certificate usage.

1.3.1 Certification Authority (CA)

A CA is mainly responsible for the issuance and administration of certificates. Based on the characteristics of operations, the CA falls into the RCA (root certification authority) and Sub-CA (subordinate certification authority).

All CAs established under this PKI must follow the rules specified in this CP and must establish a contact window. When a CA is also a Sub-CA of other PKIs, this CP shall not apply to its up level of CA.

As the trust anchor of this PKI, the RCA shall maintain the highest credibility and operate according to the highest assurance level of security specified in this CP.

The Sub-CA is a Level 2 or Level 3 CA under this PKI. The certificate of a Level 2 CA is issued by the RCA, and the certificate of the Level 3 CA is issued by the Level 2 CA.

As the highest certificate administration authority of TWCA, the RCA is responsible for:

1. the issuance and administration of the Sub-CA certificates;
2. the administration and publication of the certificates and certificate revocation lists (CRLs) of Sub-CA stored in the repository; and
3. maintaining the stability and operations of the repository.

The main duties of Sub-CAs are:

1. issue and administration of subscriber certificates;
2. issue and administration of registration authority (RA) certificates;
3. administering and publishing the certificates and CRLs stored in the repository; and
4. maintenance of the stability and operations of the repository.

Sub-CAs issuing certificates to its Sub-CAs shall also be responsible for:

5. the issuance and administration of Sub-CA certificates; and
6. the administration and publication of the certificates and CRLs of the Sub-CAs stored in the repository

1.3.2 Registration Authority (RA)

The responsibilities of RA are to authenticate the identity of subscribers and the required information of the certificate for CAs to issue the subscriber certificate.

CAs under this PKI shall specify the responsibilities of RAs in their CPS.

When issuing a Sub-CA certificate, CAs under this PKI must be the RA and carry out the RA responsibilities specified in their CPS.

1.3.3 Subscriber

The subscriber is the end entity specified in the CA certificate subject and the holder of the private key corresponding to the certificate public key. The usage of subscriber certificates shall be specified in the CPS. When issuing a certificate to an entity without the capacity specified by the law for the purpose of identification in the application system, such subscribers shall be the natural or juristic person applying for the certificate.

1.3.4 Relying Parties

A relying party means the acceptance the certificate of others (subscribers) for verifying the validity of the signature information or delivery of encryption information to the subscriber after encrypting the information of the subscriber certificate in order to maintain the privacy of the

information contents of both parties in communication.

Based on the information specified in the certificate, the relying party shall determine the reliability of certificate or if the certificate is intended for special usage.

1.3.5 Other Participant

New members wishing to join this PKI must be approved by the Policy Management Authority (PMA) center of TWCA. For example, when it is necessary for the CAs of this PKI to cross certified with the CAs of other PKIs.

1.4 Certificate Usage

The assurance level of certificate specified in this CP and their appropriate uses are as follows:

Testing Class: Testing assurance level is for the certificate testing of subscribers or relying party, and usage other than certificate testing is not allowed.
Class 1: Basic assurance level, a little confidence in the identity of the user, and it is suitable for use in network environments of very low threat of malicious interpolation.
Class 2: Preliminary assurance level, providing basic identity authentication, some level of confidence in the identity of the user, and it is suitable for use in network environments of lower risk of malicious interpolation but still with potential threat of information interpolation.
Class 3: Intermediate assurance level, providing advanced identity authentication, with high reliability for the identity of the user, and it is suitable for use in network environments of higher risk of malicious information interception or interpolation.
Class 4: High assurance level, providing the highest-level identity authentication, with high reliability for the identity of the user, and it is suitable for use in network environments of high risk of malicious information interpolation requiring a high recovery cost. It is only available for application by CAs.

The assurance levels applicable to different certificate types are as follows:

Assurance Level	**Types of Certificates**
Testing Class	Commercial XML Certificate, Commercial EC Certificate, EC Security Certificate, InfoSec Certificate

Assurance Level	Types of Certificates
Class 1	Commercial XML Certificate, Commercial EC Certificate, EC Security Certificate, InfoSec Certificate
Class 2	Commercial XML Certificate, Commercial EC Certificate, EC Security Certificate, InfoSec Certificate, AATL Certificate
Class 3	Commercial XML Certificate, Commercial EC Certificate, EC Security Certificate, InfoSec Certificate, AATL Certificate, TSA Certificate, SSL Certificate, EVSSL Certificate, S/MIME Certificate
Class 4	Only provide CAs to apply.

When applying the assurance level and their limitations on the scope of these guarantees specified in this CP to certificates, CAs shall specify them in their CPS. Subscribers and relying party must select the appropriate certificates according to the assurance level and their scopes of usage specified in the CPS.

1.4.1 Appropriate Certificate Uses

Subject to the CPS of respective CAs.

1.4.2 Prohibited Certificate Uses

Subject to the CPS of respective CAs.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The Policy Management Authority of TWCA (PMA or TWCA PMA) is responsible for the establishment, revise, and publication of this CP.

1.5.2 Contact Person

Subscribers may email or mail their suggestions, description of suggestions, and contact information to the following contact window if they have any opinions on the certificate policy:

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

Company	TAIWAN-CA INC. (TWCA)
Email	ca@twca.com.tw

1.5.3 Person Determining CPS Suitability for the Policy

The certification practice statement (CPS) established by CAs under this PKI must be approved by the PMA.

1.5.4 CPS Approval Procedures

CAs shall establish the CPS and ensure their consistency with this CP. Also, according to the Electronic Signature Act, CPS established by CAs must be approved by the Ministry of Economic Affairs (MOEA) before they are allowed to issue certificates.

1.6 Definitions and Acronyms

Defined in Appendix 2.

2. Publication and Repository Responsibilities

2.1 Repositories

The repositories shall offer the enquiry and download of information relating to certificate operations, such as certificates, CRLs, certificate status, CP, and CPS. Each CA under this PKI must provide at least one external repository, and its universal resources location (URL) shall be specified in the CA's CPS. The CA shall ensure the availability, accessibility, and information integrity of the repository.

2.2 Publication of Certificate Information

CAs shall publish the information required by subscribers and relying party, including but not limited to the CPS and CRL. The CA information to be published shall be subject to the CPS of respective CAs.

If CAs issued SSL certificates, EVSSL certificates or S/MIME certificates, CAs must comply with the requirements of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (TLS BR), "Guidelines for the Issuance and Management of Extended Validation Certificates" (EVG) or "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" (S/MIME BR) formulated by CA/Browser Forum.

2.3 Frequency of Publication

The frequency of publication of the CA information shall be subject to the CPS of respective CAs.

The frequency of publication of the CRL must be published in the CPS.

If the CAs issued Public Trusted certificates, CAs must develop, implement, enforce and revise CP/CPS to detail the latest status of these requirements.

If CAs issued SSL Certificates, EVSSL Certificates or S/MIME Certificates, CAs must annually review and revise its CP and/or CPS that describes in detail how the CA implements the requirements of TLS BR, EVG or S/MIME BR.

2.4 Access Control of Repository

CAs shall establish the specifications for repository access control in their CPS.

3. Identification and Authentication

CAs under this PKI must establish in their CPS and registration specifications the procedures for identifying and authenticating the subscriber identity.

3.1 Naming

3.1.1 Types of names

CAs must be able to issue the X.509 certificate using the X.500 unique identifier as subject name. CAs shall specify in the CPS the types of names.

CAs may use the expanded subject alternate name extension field where necessary, provided that the subject name field must not be null, and the subject alternate name must comply with the X.500 standard.

3.1.2 Need for Names to be Meaningful

The subject identity name specified in the certificate shall be able to identify the particular organization, unit or individual, and shall be readily identifiable by the relying party.

3.1.3 Anonymity and Pseudonymity of Subscribers

CAs shall not allow subscribers to use anonymity, pseudonyms, or aliases, etc..

3.1.4 Rules for Interpreting Various Name Forms

The interpretation rules for subscriber name shall be subject to the relevant rules and regulations specified by the competent authorities. For example, the identifier of an Internet account shall be processed according to the rules governing the bank code and the user account for banks assigned by the Financial Data Center, Ministry of Finance; the uniformed identifier for the citizen identity card of individuals shall be processed according to the rules specified by the Ministry of the Interiors; the identifier of the profit business tax code shall be processed according to the rules specified

by the MOEA; and the rules for interpreting other subscriber identifiers shall be subject to the CPS of respective CAs.

3.1.5 Uniqueness of Names

CAs shall ensure the uniqueness of the name in the certificates issued by them, and shall specify in their CPS the nominalization rules and rules for ensuring name uniqueness.

3.1.6 Recognition, Authentication, and Role of Trademarks

When identical identifiers are detected, CAs shall assign the identifier to the first applicant. However, when another applicant requests the same identifier with the documents issued by the relevant competent authorities, CAs shall settle the dispute over such identifier.

CAs shall specify in the CPS the procedures for settling disputes over identifier.

3.1.7 Identification, Authentication and Role of Trademarks

Subject to the CPS of respective CAs.

3.2 Initial Identity Verification

3.2.1 Method to Prove Possession of Private Key

If the private key corresponding to the certificate public key is generated by the subscriber, a CA must request the subscriber to submit the prove possession of the private key, such as verify the signature information signed by private key (e.g. using the methods specified in the RFC 2314, RFC 2510 and RFC 2511 standards).

It will be no need to verify private key possession when the private key is generated by the RA, CA or other authorized third-party, provided that the security measures for private key delivery shall be specified in the CPS.

3.2.2 Authentication of Organization Identity

When authenticating the status of organizations, the organization shall submit documents issued by the competent authorities or other certifications proving its existence. The identity and authorization of its statutory representative shall be verified. If the application is made by the authorized agent of an organization, this agent shall also submit his/her identify certifications, and all documents and/or certifications shall be submitted in writing or handled by an agent in a manner equivalent to the strength of face-to-face authentication

CAs must define the organization identity authentication procedures in its CPS, and RAs shall release the policy of the organization identity authentication in accordance with the standards of the CPS and conduct the authentication procedures with the published policy.

The following shows the requirements for the identity authentication of organization under various assurance level:

Testing Class:
If CAs issue testing certificates, it shall be subject to the CPS of respective CAs.

Class 1:

- Organizations register with self-claimed identity information.
- RA must verify the uniqueness of the information and conduct limited verification.

Class 2:

- Must satisfy the above-mentioned Class1 relevant inspection.
- Organizations must submit evidence to prove their identity information.
- RA must check the existence and validity of the evidence.

Class 3:

- Must satisfy the above-mentioned Class2 relevant inspection.
- The representative or the agent holding the authorization document must provide the supporting documents sufficient to organization identity.
- RA must conduct the authentication similar to the strength of face-to-face, and inquire information through trusted third-party (such as Commerce Industrial Inquiry Services), and check the identity information claimed by the organization or the information only known to the organization.

Class 4:

- Must satisfy the above-mentioned Class3 relevant inspection.
- RA must conduct face-to-face authentication.

When performing the initial verification of the information or communication hardware and software equipment of an organization (e.g. routers, firewalls, and servers), the equipment administrator shall submit the following registration information:

1. equipment identification (e.g. serial number) or service name (e.g. domain name);
2. equipment public key;
3. the licensing usage and attributes of equipment (e.g. the licensing usage or attributes shall only be specified when it is included in the certificate);
4. the contact information of administrators for contacts made by the RA or CA;
5. CAs shall verify registration data with methods corresponding to the assurance level of certificates being applied for. The verification methods shall include, but not limited to, the methods specified in this part for authenticating the identity or the digital signature of subscribers (signature certificates shall be issued according to this CP).

For all SSL Certificates and EVSSL Certificates, the Applicant’s ownership or control of all requested Domain Name(s) and IP address must be verified with methods specified in TLS BR, EVG and must be detailed within the CPS.

For S/MIME Certificates, CAs should follow the S/MIME BR specification to verify the ownership of the email domain and email address provided by the applicant, and the verification method must be specified in the CPS.

Further information may be requested from the Applicant, and other information and/or methods may be utilized to achieve an equivalent level of confidence.

3.2.3 Authentication of Individual Identity

CAs must define the individual identity authentication procedures in its CPS, and RAs shall release the policy of the individual identity authentication in accordance with the standards of the CPS and conduct the authentication procedures with the published policy.

The following show the requirements for the identity authentication of individual subscribers under various assurance level:

> **Testing Class:**
> If CAs issue testing certificate, it shall be subject to the CPS of respective CAs.

Class 1: • Individuals register with self-claimed identity information. • RA must verify the uniqueness of the information and conduct limited verification.
Class 2: • Must satisfy the above-mentioned Class1 relevant inspection. • Individuals must submit evidence to prove their identity information. • RA must check the existence and validity of the evidence.
Class 3: • Must satisfy the above-mentioned Class3 relevant inspection. • The individual or the agent holding the authorization document must provide the supporting documents sufficient to individual identity. • RA must conduct the authentication similar to the strength of face-to-face, and inquire information through trusted third-party (such as MOICA Individual Inquiry Services), and check the identity information claimed by the individual or the information only known to the individual.
Class 4: Not applicable.

For the information or communication hardware and software equipment held by individual subscribers, the individual subscribers shall be deemed as the administrator of such equipment and shall complete the verification according to section 3.2.2.

3.2.4 Non-Verified Subscriber Information

No applicable.

3.2.5 Validation of Authority

The certifications of identity of an individual, organization representative, organization agent or organization shall be issued by the relevant government agencies. The RA shall validate the authenticity of the letter of assignment submitted by an agent.

3.2.6 Criteria for Interoperation

No applicable.

3.3 Identification and Authentication for Re-Key Requests

Subscribers of CAs shall follow the identity authentication requirements below to perform the subscriber identity identification and authentication for re-key request.

Testing Class: No stipulation.
Class 1: No stipulation.
Class 2: The key identify authentication shall be performed with the password of the authorized account or the use of current signing key.
Class 3: The key identify authentication shall be performed the use of current signing key.
Class 4: The initial verification must be performed for every re-key request.

3.3.1 Identification and Authentication for Routine Re-Key

The longer the time of use of a key, the higher the risk of key discloser or compromise. For this reason, it is necessary to change over the key for certificate subscribers to ensure key security. The changeover of certificate keys means to re-generate a public key and private key pair and to apply new certificate from the CA with the old registration data. The features and assurance level of the new certificate issued after re-key shall remain the same as the old certificate.

CAs shall specify in the CPS the requirements of routine re-key for the subscriber identity identification and authentication.

3.3.2 Identification and Authentication for Re-Key After Revocation

After revoking a certificate, subscribers shall repeat the initial verification specified in section 3.2 in order to apply new certificate.

3.4 Request of Certificate Revocation

CAs shall authenticate the request of certificate revocation. In authenticating a request of certificate revocation, CAs may verify the signature generated with the private key of the corresponding certificate, whether or not the private key has been compromised.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a of Certificate Application

When the certificate user is a natural person, he/she is the certificate applicant. When the certificate user is an organization, the statutory representative or his/her agent is the certificate applicant.

4.1.2 Enrollment Process and Responsibilities

Certificate applicants shall read through the terms of use (TOU) in advance. After agreeing to the TOU, applicants shall complete the application form together with the signed TOU to the RA.

CAs must specify in the CPS the methods for delivering the public key to the certificate issuer.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The RA shall follow the procedures below to handle the certificate application.

1. To acquire the relevant data of certificate application of applicants is described in section 3.2.
2. To verify and record the identification data of applicants is described in section 3.2.
3. To acquire the public key of applicants and check its associations with the private key of applications is described in section 3.2.
4. To validate the authenticity of information specified in the certificate.

CAs shall establish and specified the steps for completing the above procedures in the CPS. These procedures shall be completed prior to the issuance of certificates.

4.2.2 Approval or Rejection of Certificate Application

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

If CAs issued SSL Certificates, EVSSL Certificates or S/MIME Certificates, CAs and RAs shall follow industry standards (e.g. TLS BR, EVG or S/MIME BR) when approving and issuing Certificates, and state the practice statement in the CPS.

4.2.3 Time to process Certificate Applications

No stipulation.

4.3 Certificates Issuance

4.3.1 CA Actions During Certificate Issuance

The identity authentication shall be performed in communication of any forms between the RA and the CA. The communication shall be made either online or offline. The integrity and privacy of information shall be maintained during the communication.

When delivering the public key of certificate applicants to the CA, the CA shall ensure that the application data are correctly linked with public key. The CA may ensure the linkage with cryptographic methods or the non-cryptographic physical or procedural methods. These shall include, but not be limited to, the use of diskette (or other storage devices) delivered by with registered mail or courier service.

After receiving the request of certificate issuance, the CA shall

1. verify the identity of sender;
2. examine the integrity of delivered data;
3. after confirming the content of the certificate issuance complies with the regulations on the content of certificate issuance , the certificate will be issued.

4.3.2 Notifications to Subscriber of Certificate Issuance

After issuing certificates, CAs shall notify the issuance of certificates with appropriate methods and deliver the certificate to the corresponding subscribers. When the issuance of certificates is rejected, CAs shall notify subscribers with appropriate methods and inform subscribers of the reasons of rejection. The notification and delivery also can be made through the RA.

Apart from the applicant’s failure to pass the verification, CAs may disapprove the issuance of certificates for other reasons.

4.4 Certificate Acceptance

CAs shall specify the following in the CPS:

1. procedures of subscriber certificate acceptance;
2. certificate applicants have accepted and understood the responsibilities and obligations for using the certificate;
3. how to inform certificate applicants of the contents of certificates; and
4. when a certificate applicant rejects the certificate issued after reviewing the certificate contents, the RA shall notify the CA to revoke the certificate.

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers shall validate if the contents registered in the certificate are correct and understand the TOU before start to use the certificate.

4.4.2 Publication of the Certificate by the CA

CAs may publish the issued certificates to the repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Apart from delivery the certificate to the subscriber, CAs may deliver the certificate to the RA after the issuance.

4.5 Key Pair and Certificates Usage

4.5.1 Subscriber Private Key and Certificate Usage

The subscriber is the holder of the private key corresponding to the certificate public key. Restrictions in the intended scope of usage for a private key are specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate. CAs shall specify in the CPS the scope of certificates usage they issue.

When there are doubts of private key fraud, disclosure, compromise or loss, subscribers shall report to the RA or CA according to the procedures specified in the CPS of respective CAs.

The usage and constraint of subscriber’s certificate and private key shall follow the rule specified in this CP and the CA’s CPS.

4.5.2 Relying Party Public Keys and Certificates Usage

The examination steps for relying party to determine a trustee certificate are not specified in this CP. When examining a certificate, relying party shall follow the rules in the CPS of respective CAs to create a trust path and to verify the certificate status as a reference for determining to trust

or not a certificate. The relying party shall only apply a certificate to examine the correctness of a digital signature in the electronic documents and the identity of the signature holder after trusting a certificate.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

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

CAs under this PKI shall determine independently whether to accept certificate renewal or not.

4.6.2 Who May Request Renewal

All certificate subscribers are eligible for renewing a certificate.

4.6.3 Processing Certificate Renewal Request

1. Prior to the expiration of a certificate, subscribers shall apply for the issuance of a new certificate to the RA or CA with the original registration information and public key.
2. After receiving an application for certificate renewal, the CA shall validate the correctness of the registration information and public key of the applicant.
3. The CA shall issue a new certificate as described in section 4.3.

4.6.4 Notification of New Certificate to Subscribers

See section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See section 4.4.

4.6.6 Publication of Renewal Certificate by the CA

See section 4.4.2.

4.6.7 Notification of Certificate issuance by the CA to Other Entities

See section 4.4.3.

4.7 Certificate Re-Keys

4.7.1 Circumstances for Certificate Re-Keys

The certificate re-key means the generation of a new public and private key pair and apply a new certificate to the CA with the origin registration information.

CAs under this PKI shall specify independently the certificate re-key procedures.

4.7.2 Who May Request Certification of a New Public Key

All certificate subscribers are eligible for request the certification of a new public key.

4.7.3 Processing Certificate Re-Keying Requests

1. CAs shall perform the identification and authentication of subscriber identity as described in section 3.3.
2. CAs shall issue the certificate as described in section 4.3.

4.7.4 Notification of New Certificate Issuance to Subscribers

See section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See section 4.4.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA Other Entities

See section 4.4.3.

4.8 Certificate Modification

A certificate modification means the issuance of a new certificate after changing the identification information of the subscriber’s name, without changing the public key of the certificate.

4.8.1 Circumstances for Certificate Modification

Subject to the rules specified in the CPS of respective CAs.

4.8.2 Who May Request Certificate Modification

Subject to the rules specified in the CPS of respective CAs.

4.8.3 Processing Certificate Modification Requests

Subject to the rules specified in the CPS of respective CAs.

4.8.4 Notification of New Certificate Issuance to Subscriber

Subject to the rules specified in the CPS of respective CAs.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Subject to the rules specified in the CPS of respective CAs.

4.8.6 Publication of the Modified Certificate by the CA

Subject to the rules specified in the CPS of respective CAs.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Subject to the rules specified in the CPS of respective CAs.

4.9 Certificate Revocation and Suspension

If the CAs issued SSL Certificates, EVSSL Certificates or S/MIME Certificates, the CAs must comply with the provisions of TLS BR, EVG or S/MIME BR and describe the practice statement in the CPS.

4.9.1 Circumstances for Certificate Revocations

A certificate is revoked when

1. subscribers wish to terminate the use of a certificate or the certificate contract is terminated.
2. the subscriber information in the certificate has been changed during the certificate is valid.
3. the relevant private key of the certificate is proven or suspected to be compromised, damaged, lost, discloser and/or interpolated.
4. the subscriber breaches the CP, CPS or subscriber agreement.
5. the CA signing key is proven or suspected to be cracked.

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 Revocations

CAs shall specify in the CPS the eligibility for requesting a certificate revocation.

4.9.3 Procedure for Revocation Request

Applicants applying for a certificate revocation shall specify the certificate(s) to be revoked and the reason(s) for revocation. CAs shall specify in the CPS the procedures of certificate revocation.

4.9.4 Revocation Request Grace Period

CAs shall specify in the CPS the revocation request grace period.

4.9.5 Time Within Which CA Must Process the Revocation Request

CAs shall specify in the CPS the handling time of requests of certificate revocation.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying party shall determine the interval for enquiring (or downloading) the revocation data (CRLs) according to their risk, responsibility and consequences. When authenticating the digital signature of a subscriber certificate, relying party shall check if the certificate has been revoked.

CAs shall specify in the CPS the requirements of relying party to verify the CRL.

4.9.7 CRL Issuance Frequency

CAs shall generate the CRL at planned intervals. Information of revoked certificates shall be updated within the time specified in the "Next Update" field in the CRL and include the information of revoked certificate in the CRL in the next update for relying party to enquire. CAs shall publish the CRL at planned intervals; even no subscribers have revoked any certificate during the interval.

Basically, CAs shall generate a CRL once every 24 hours, though the frequency of CRL generation may vary according to practical needs of respective CAs.

CAs shall specify in the CPS the CRL issuance frequency.

4.9.8 Maximum Latency for CRLs

The maximum latency for CRL means the time difference between the CRL generation and publication to the repository.

This is not defined in this CP.

4.9.9 On-Line Revocation/Status Checking Availability

CAs may provide the Online Certificate Status Protocol (OCSP) according to the actual needs. As on-line enquiries of certificate status may not be required by all relying party, CAs shall provide at least the CRL download service and specify in the CPS the availability of OCSP.

4.9.10 On-Line Revocation Checking Requirements

CAs shall specify in the CPS the OCSP inspection rules.

4.9.11 Other Forms of Revocation Advertisements Available

CAs shall specify in the CPS the operating methods of other forms of certificate status query functions, and shall apply protection for in information equivalent to the CRL protection.

4.9.12 Special Requirements Related to Key Compromise

When the signing key is compromised, CAs shall follow the instructions below:

1. Revoke all issued certificates.
2. Update the CRL or the certificate status information of the OCSP.
3. Generate the new signing key pair and corresponding new certificate.
4. Notify Sub-CAs that the superior CA key has been compromised.
5. When the key of a Sub-CA is compromised, the Sub-CA shall report to the superior CA within 24 hours.
6. Using new signing key, issue the new certificates to subscribers according to Parts 4.2 and 4.3.
7. The new certificates shall be delivered as described in 6.1.4.

CAs shall specify in the CPS the handling procedures for key compromise.

4.9.13 Circumstances for Suspension

Subject to the CPS of respective CAs.

4.9.14 Who Can Request Suspension

Subject to the CPS of respective CAs.

4.9.15 Procedures for Suspension

No certificate suspension is available, except for CAs issuing subscriber certificates.

When provide certificate suspension service, CA shall specify in the CPS the procedures of certificate suspension.

4.9.16 Limits on Suspension Period

Subject to the CPS of respective CAs.

4.10 Certificate Status Service

4.10.1 Operational Characteristics

See section 4.9.9, 4.9.11, and 4.9.13.

The CAs must not removes the revocation entries until the Expiry Date of the revoked Certificate.

4.10.2 Service Availability

See section 4.9.9, 4.9.11, and 4.9.13.

If the CAs issued SSL Certificates, EVSSL Certificates or S/MIME Certificates, the CAs must comply with the provisions of TLS BR, EVG or S/MIME BR and describe the practice statement in the CPS.

4.10.3 Operational Features

See section 4.9.9, 4.9.11, and 4.9.13.

4.11 End of Subscription

Certificates issued by CAs shall be invalid when they are terminated or expired, or when the CA shuts down its business.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

See section 6.2.3.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

5.1 Physical Control

5.1.1 Site Location and Construction

The construction of the site location of CAs 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 CCTV system, in order to prevent unauthorized access to certificate-related equipment.

5.1.2 Physical Access

The physical controls of CAs shall comply with at least the following requirements:

1. to prevent unauthorized access to hardware storage devices;
2. to ensure that all mobile storage media or paper documents containing sensitive information are stored in a secure place;
3. to apply manned or automatic monitoring and recording of unauthorized access at all times; and
4. to review the access records and ensure their availability.

CA computer rooms where certificate issuing equipment is located shall be equipped with access controls, and access is only made possible by two or more persons.

5.1.3 Power and Air Conditioning

CAs shall be equipped with adequate power supply and air-conditioning equipment that can be operable or shut down regardless of external influences. Also, a backup power supply system shall be equipped to supply electricity of no less than 6 hours for the repository to perform data backup.

5.1.4 Water Exposures

CA equipment shall be installed in locations containing physical protection against floods.

5.1.5 Fire Prevention and Protection

CA computer rooms shall be equipped with automatic fire extinguishing equipment to automatically extinguish any fire detected. A manual control shall be equipped at all major entrances for onsite personnel to operate such equipment in an emergency.

5.1.6 Media Storage

The media storage environment of CAs shall be sited or protected to prevent damage as a result of accidents. The backup copy of important data shall be stored in a location other than the CA’s location.

5.1.7 Waste Disposal

CAs shall establish and maintain and specify in the CPS procedures for the secure removal and destruction of sensitive information

5.1.8 Off-Site Backup

CAs shall be equipped with off-site backup facilities and specify in the CPS the off-site backup mechanism.

5.2 Procedural Controls

5.2.1 Trusted Roles

CAs 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, CAs shall define in the CPS the trusted roles and their duties. The four roles and their duties under this CP are defined as follows:

1. Administrator: To be responsible for system installation, management, and environment parameter setup.
2. Officer: To be responsible for generating the Certificate Service Request (CSR) files and the revocation and issuance of certificates.
3. Auditor: To be responsible for internal audits, and the review and maintenance of audit reports.
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

CAs shall specify in the CPS the number of persons required per task as described in 5.2.1.

If the CAs issued EVSSL certificates, the systems used to process and approve EVSSL Certificate Requests MUST require actions by at least two trusted persons before creating an EVSSL Certificate.

5.2.3 Identification and Authentication for Each Role

Each role shall be identified and authenticated prior to carrying out the designated duties.

5.2.4 Roles Requiring Separation of Duties

CAs shall perform duty separation according to the following rules:

1. equip with the four roles as described in section 5.2.1;
2. the officer and the administrator shall not be the same person;
3. the officer and the auditor shall not be the same person;
4. the administrator and auditor shall not be the same person.
5. the operator and the administrator shall not be the same person;
6. the operator and auditor shall not be the same person.

5.3 Personnel Control

5.3.1 Qualifications, Experience, and Clearance Requirements

CAs shall establish the competence requirements for operators implementing certificate management. These requirements shall at least include loyalty and reliability, and no criminal or credit records. The competence requirements shall be specified in the CPS, including the requirements for third-party personnel, if applicable.

5.3.2 Background Check Procedures

CAs shall establish the procedures for reviewing the background and duties of operators operating the certificate management system, and such procedures shall meet the requirements as described in section 5.3.1.

5.3.3 Training Requirements

Based on the duty of operators, CAs shall provide education and training concerning the operation of hardware and software functions, operating procedures, security control procedures, CP, CPS, and other related techniques and policies.

5.3.4 Retraining Frequency and Requirements

After a modification of the operating environment or security management, CAs shall provide operators appropriate training and shall specify in the CPS the education and training plan and frequency.

5.3.5 Job Rotation Frequency and Sequence

CAs shall establish the operating procedures for job rotation and specify these procedures in the CPS.

5.3.6 Sanctions for Unauthorized Actions

CAs shall specify in the CPS the procedures for punishing unauthorized actions.

5.3.7 Independent Contractor Requirements

CAs shall specify in the CPS the control procedures of contractor personnel.

5.3.8 Documentation Supplied to Personnel

The operating documentation of CAs shall at least meet the requirements for personnel of different roles to carry out their duties. CAs shall specify in the CPS the requirements of operating documentation.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

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

1. Type of event.
2. Event date and time.
3. Event place or location.
4. Results (success or failure) of certificate issuance or revocation.
5. Entity or individual evoking the event.

When an event occurs, the audit record shall be recorded either electronically or physically at the choice of the CA. The types of audit events recorded by CAs are as follows:

1. Security audit management.
2. Management, identification and authentication of personnel and trusted roles.
3. Creation, modification and deletion of subscriber information.
4. Generation of CA key.
5. Changes of private keys and trustee public keys.
6. Certificate applications, issue, revocation and status change.
7. Certificate management system configuration and change.
8. Activation and deactivation of systems and applications.
9. Personnel login and logout systems and applications.
10. Cryptographic Module installation, removal and destruction.
11. Access control management and access to physical environment.

12. Hardware and software system updates.
13. Data backup and recovery.
14. Unauthorized access to file systems.
15. Abnormal network system access.
16. Key compromise, system anomalies and hazards.
17. Violations of the CP and CPS.

5.4.2 Frequency of Processing Log

CAs shall inspect the audit records at least once a month. The inspection shall include the integrity of audit records, the non-interpolation of audit records, and review of all record items. Anomalies or warnings shall be carefully investigated. Solutions for the inspection results shall be documented.

5.4.3 Retention Period of Audit Log

The relevant audit records and reports and media data shall be retained at the CA for at least two months. The relevant audit records shall be archived prior to removal, except to video recordings.

5.4.4 Protection of Audit Log

CAs shall prevent the retrieval of audit records by unauthorized personnel and make a backup copy of audit records, and shall prevent audit records from interpolation.

5.4.5 Audit Log Backup Procedures

CAs shall specify in the CPS the procedures of making backup copies of audit records. Backup copies of audit records shall be made at least once a month, and a copy shall be stored in an off-site location outside of the CA.

5.4.6 Audit Collection System (Internal vs. External)

Audit records may be collected outside of or inside the CA certificate management system. The automatic audit procedure shall be activated by the certificate management system until the system shuts down. Audit records may be collected automatically by the computer or manually by the operating system, certificate management system or certificate management operators.

5.4.7 Notification to Event-Causing Subject

When an event is recorded by the audit system, there is no need to notify the related personnel generated the event. The reporting procedures of abnormal events shall be specified in the CPS of respective CAs.

5.4.8 Vulnerability Assessments

CAs shall assess the vulnerabilities of the security control at planned intervals.

5.5 Record Archival

5.5.1 Types of Records Archived

The archival records of CAs shall include at least the following five types:

1. Data concerning the external accreditation of CAs
2. CPS
3. Contracts related to CA operations
4. System environment implementation and setup files
5. System change records
6. Certificate application files
7. All issued and published certificates
8. Key Changeover records
9. Audit data files
10. Revocation request record
11. Subscriber registration data
12. Subscriber contracts
13. Revoked certificate data files
14. Data and tools for verifying archival records
15. Documents requested by auditors

CAs offering subscriber key escrow service shall also archive such keys.

5.5.2 Retention Period for Archive

CAs shall retain archival data for at least 7 years and must not less than 2 years after the relevant key is destroyed, and shall specify in the CPS the retention period of archival data.

5.5.3 Protection of Archive

No writing, modification or deletion of archival data shall be allowed. Archival personal data of subscribers are allowed for retrieval by the subscriber, his/her agent, and legally approved agencies. A cope 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

CAs shall specify in the CPS.

5.5.5 Requirements for Time-Stamping of Records

CAs shall specify in the CPS.

5.5.6 Archive Collection System (Internal or External)

CAs shall specify in the CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

CAs shall specify in the CPS.

5.6 Key Changeover

In order to minimize the risk of compromise of the CA signing key, CAs shall change over the CA signing key at plant intervals, and shall not use the previous key to issue certificates after the changeover.

When selecting key validity, CAs shall consider the length, protection, controls and other factors related to the key. The key validity shall not exceed the term described in section 6.1.5.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The CA organizations shall have an Incident Response Plan and a Disaster Recovery Plan.

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

If the CAs issued SSL Certificates, EVSSL Certificates or S/MIME Certificates, the procedures of key compromised and emergency response must comply with the provisions of TLS BR, EVG or S/MIME BR and shall be specified in the CPS.

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

CAs shall re-implement as soon as possible any abnormal or damaged equipment and shall put the recovery of certificate status information generation on the top priority. CAs shall specify in the CPS the recovery procedures and conduct an exercise on the recovery of computer resource, software and data damage at least once a year.

5.7.3 Entity Private Key Compromise Procedures

CAs shall specify in the CPS or related documents the procedures for handling the compromised private key of members within this PKI.

5.7.4 Business Continuity Capabilities After a Disaster

CPS shall specify in the CPS the procedures for rescuing CA equipment and maintaining business operations prior to the reconstruction of a secure environment after a natural disaster or other accidents.

5.8 CA or RA Termination

CAs shall specify in the CPS the procedures to be followed after the termination of service, and such procedures shall comply with the Electronic Signature Act.

6. Technical Security Control

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The process of key pair generation shall be specified in the CPS. The key generation equipment of CAs shall at least be equipped with the hardware cryptographic module complying with the FIPS 140-2 level 3, or FIPS 140-3 level 3 or higher levels.

The CAs should described the subscriber key pair generation requirement in the CPS.

6.1.2 Private Key Delivery to Subscriber

CAs offering subscriber key pair generation service shall specify in the CPS the security controls for private key delivery.

6.1.3 Public Key Delivery to Certificate Issuer

When delivering the subscriber public key to the CA, the authenticity of data shall be validated. The public key shall be delivered by means of electronic signature-protected message, physical media (e.g. diskette) by courier service or the applicant in person, or other means.

CAs shall establish in the CPS the methods of public key delivery to CAs.

6.1.4 CA Public Keys Delivery to Relying Parties

When it is necessary for CAs to deliver a public key, the protection for the information integrity of the public key shall at least be provided.

6.1.5 Key Sizes

The RSA key size of CA certificates shall at least be 2048 bits, and the ECC curve shall at least be P-256.

The RSA key size of subscriber certificates shall at least be 2048 bits, and the ECC curve shall at least be P-256.

6.1.6 Public Key Parameters Generation and Quality Checking

The generation and selection of CA public key parameters shall be the prime number parameters generated by the random number generator complying with FIPS 186-4 or similar specifications; or the generation of random numbered public key parameters shall comply with FIPS 140-2 or FIPS 140-3.

When subscribers use hardware cryptographic modules (e.g. IC card), such modules shall at least comply with FIPS 140-2 Level 2 or FIPS 140-3 Level 2 or other specifications of the same security level.

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

The constraints of key usage purposes shall be specified in the extension field of key usage purposes of the X.509 certificate.

Only the *keyCertSign* and *cRLSign* bits shall be set in CA certificates for issuing certificates and CRLs.

The *digitalSignature* and/or *nonRepudiation* bit shall be set in the subscriber signature certificate, and the *keyEncipherment* and/or *dataEncipherment* bit shall be set for encrypted certificates.

CAs issuing certificates for other usage shall specify the key usage purposes in the CPS, except for signature and encrypted certificates.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CA cryptographic modules shall at least pass the certification of FIPS 140-2 level 3 or FIPS 140-3 level 3, or other specifications of the same security level.

RA software and hardware cryptographic modules shall at least comply with FIPS 140-2 level 2 or FIPS 140-3 level 2, or other specifications of the same security level.

When subscribers use hardware cryptographic modules (e.g. IC card), such modules shall at least comply with FIPS 140-2 Level 2 or FIPS 140-3 Level 2, or other specifications of the same security level.

All CA cryptographic modules shall be equipped with multiparty security controls.

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

The signature private key of CAs shall comply with the multiparty security control procedure described in section 5.

6.2.3 Private Key Escrow

No CA signing private keys shall be escrowed.

CAs offering subscriber private key escrow, recovery and retention services shall specify in the CPS the relevant operating procedures.

6.2.4 Private Key Backup

The backup of CA private keys stored in an encrypted hardware cryptographic module after encryption shall be performed by means of multi-person control, and the backup copy shall be retained in the off-site. CAs shall specify in the CPS the produces for making private key backup copies.

The procedures for making and retaining backup copies of RA and subscriber private keys are not specified in this CP.

6.2.5 Private Keys Archive

No CA signing private keys shall be archived.

CA encryption private keys can be archived, and CAs shall specify in the CPS the procedures for CA encryption private key encryption.

The procedures for RA and subscriber private key achieve are not specified in this CP.

6.2.6 Private Key Transfer into or From a Cryptographic Module

Private keys shall be generated in the cryptographic module. When it is necessary to transfer a private key from one cryptographic module to another cryptographic module, the transfer shall be performed by authorized personnel. Also, private keys must not exist in plaintext outside of the cryptographic module. The encryption key for encrypting private keys must be protected against leakage.

6.2.7 Private Key Storage on Cryptographic Module

Private keys shall be stored in the cryptographic module in either plaintext or cipher text.

6.2.8 Method of Activating Private Key

Private keys stored in the cryptographic module shall be activated by authorized personnel after identity authentication. The authentication shall include, but not be limited to, password, PIN, or biometric identification. Activation data shall be protected against leakage during data entry.

6.2.9 Method of Deactivating Private Key

Private keys shall be deactivated by authorized personnel.

CAs shall specify in the CPS the procedures for private key deactivation.

6.2.10 Method of Destroying Private Key

When the CA signing private key is no more in use, or the corresponding public key has expired or is revoked, the private key in the cryptographic module shall be expunged by means of zeroization.

6.2.11 Cryptographic Module Rating

The cryptographic modules used by CAs shall at least pass the certification of FIPS 140-2 level 3 or FIPS 140-3 level 3, or other specifications of the same security level.

CAs shall specify in the CPS the specification of subscriber cryptographic modules.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key has been archived when the certificate is archived. Therefore, it is not need to archive the public key again.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity of the public key and private key of participants of this PKI may be the same. The validity by strength (key sizes) is as follows:

1. RSA 4096-bit key pair: maximum 40 years.
2. RSA 2048-bit key pair: maximum 30 years.
3. ECC P-384 key pair: maximum 40 years.
4. ECC P-256 key pair: maximum 30 years.

CAs shall specify in the CPS or relevant operating procedures the validity of the Sub-CA and subscriber keys.

6.4 Activation Data

CAs shall specify in the CPS the protection of activation data, including the protection of the entire lifecycle of data from generation, archive to destruction.

6.4.1 Activation Data Generation and Installation

Activation data for deciphering CA’s or subscriber’s private keys or the relevant access control mechanisms shall be protected appropriately.

CA activation data may be selected by the user by means of multi-person control. Activation data shall be protected with biometric or cryptographic-module-enhanced security mechanisms.

Subscribers may select their own activation data. Data that must be generated prior to delivery shall be delivered through channels with appropriate protection.

6.4.2 Activation Data Protection

CA activation data shall be protected with cryptographic or physical access control.

6.4.3 Other Aspects of Activation Data

CAs may specify in the CPS the operating procedures of activation data according to the security requirements of the scope of certificate usage.

6.5 Computer Security Control

6.5.1 Specific Computer Security Technical Requirements

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

1. User login identification and authentication.
2. User-defined access control.
3. Security audit capability.
4. Access control constraints of CA services and PKI trusted roles.
5. Identification and authentication of PKI trusted roles.
6. Communication and database security.
7. Secure and trusted channels for the identity authentication of PKI trusted roles.
8. Procedural integrity and security control protection.

If the CAs issued Public Trusted certificates, CAs should implement the security control which are complied with NETWORK AND CERTIFCATE SYSTEM SECURITY REQUIREMENTS published by CA/Browser Forum.

6.5.2 Computer Security Rating

CA computer platforms shall comply with at least the EAL3 [ISO/IEC 15408 Common Criteria], C2 [TCSEC] or E2 [ITSEC] security standards.

CAs shall specify in the CPS the standards of the security level of their computer platforms.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The development of the CA certificate management system shall comply with the following requirements:

1. Detailed documentation shall be furnished.
2. The purchase of certificate management system software and hardware shall minimize the procedure of component interpolation.
3. CA-specific software and hardware shall be developed in a controllable environment, and the development process shall be defined and documented.

6.6.2 Security Management Controls

CAs shall ensure complete control and maintain records of the settings, modifications and upgrades of the certificate management system; and mechanisms for detecting unauthorized software modification or setting changes shall be equipped.

CAs shall establish and maintain controls to ensure the software integrity of the certificate management system.

CAs shall establish and maintain the operating procedures for the security control over the lifecycle of the hardware and software equipment of the certificate management system. A security clearance policy shall be established for accepting hardware and software equipment.

CAs shall only install certification-related software in and run related operations on the hardware and software equipment of the certificate management system. Software unrelated to CA business or certification shall not be installed in the system. The installation and update of software and hardware equipment shall be subject to the relevant operating procedures in an environment with security control.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The CA certificate management system shall be equipped with an independent operating system to be operated by authorized personnel.

CAs shall install and implement firewalls, IDS and antivirus management system to protect the network against intrusions and damage in order to improve the security controls of the NMS (Network Management System).

The RCA certificate management system must be installed in an environment with security control and must be set to off-line status when not in use. The system shall only be used with an authorization.

6.8 Time-Stamping

No stipulation.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profiles

CAs shall specify in the CPS or the relevant operating procedures the format of certificates they issue.

7.1.1 Version Number

CAs shall issue certificates in the X.509 V3 (ITU-T X.509 06/1997, ISO 9594-8) version.

7.1.2 Certificate Extensions

The use of certificate extension fields shall comply with the ITUT X.509 or IETF RFC 5280 standards.

7.1.3 Algorithm Object Identifier

The algorithm OIDs for certificate issuance are as follows:

Algorithm Type	Algorithm	OID
Key	rsaEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
Key	ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) ecPublicKey(1)}
Signature	sha1WithRSAEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) sha1-with-rsa-signature(5)}
Signature	sha256WithRSAEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

Algorithm Type	Algorithm	OID
Signature	sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}
Signature	ECDSAWithSHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}
Signature	ECDSAWithSHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}

CAs shall specify in the CPS the specification of the algorithm OIDs used.

7.1.4 Name Forms

The format of the subject name of certificates issued by CAs must comply with the X.500 Distinguished Name (DN) format.

7.1.5 Name Constraints

CAs may use the Name Constraint extension field in the certificates issued if necessary.

7.1.6 Certificate Policy Object Identifier

CAs may include the CP OID in the certificates issued if necessary.

7.1.7 Usage of Certificate Policies Extension

CAs may use the Certificate Policy Constraints Extension Field if necessary.

7.1.8 Policy Qualifiers Syntax and Semantics

CAs may use the Policy qualifiers if necessary.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profiles

CAs shall specify in the CPS or the relevant operating procedures the detailed contents of the CRL they issue.

7.2.1 Version Number(s)

The CRL issued by CAs shall conform to the X.509 V2 format.

7.2.2 CRL and CRL Entry Extensions

CAs shall specify in the CPS or the relevant operating procedures the format of the CRL extension field, if applicable.

7.3 OCSP Profiles

CAs shall digitally sign the response message when provide OCSP service.

7.3.1 Version Number(s)

No stipulation.

7.3.3 Online Certificate Status Protocol Expansion Field

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. Other CAs shall specify the audit frequency in the CPS.

8.2 Identity/Qualifications of Assessor

CA auditors shall at least be familiar with the CPS and this CP, as well as the audit criteria conforming to the audit.

8.3 Assessor's Relationship to Assessed Entity

CA auditors shall audit the audited in independent, unimpaired and objective attitude.

8.4 Topics Covered by Assessment

A CA audit shall include at least the following items:

1. the conformance of the CPS to this CP
2. the conformance to the CPS of the CA’s certificate management.

If the CAs issued SSL Certificates or EVSSL Certificates, the audit schemes must be disclosed in the CPS.

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 auditing and audited units of the audit results. The audited unit 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 audit results of all CAs shall be submitted to the PMA.

8.7 Self-Audits

If the CAs issued SSL Certificates, EVSSL Certificates or S/MIME Certificates, the CAs SHALL monitor adherence to the requirements of TLS BR, EVG or S/MIME BR, and strictly control its service quality by performing self-audits at planned interval basis against a randomly selected sample of certificates issued during the auditing period.

9. Other Businesses and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

CAs shall specify them in the CPS.

9.1.2 Certificate Access Fees

CAs shall specify them in the CPS.

9.1.3 Revocation or Status Information Access Fees

CAs shall specify them in the CPS.

9.1.4 Fees for Other Services

CAs shall specify them in the CPS.

9.1.5 Refund Policy

CAs shall specify this in the CPS.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

CAs shall specify this in the CPS.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

CAs shall specify this in the CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope Types of Confidential Information

CAs shall specify this in the CPS and implement according to the relevant laws and regulations.

9.3.2 Information Not Within the Scope of Confidential Information

CAs shall specify this in the CPS and implement according to the relevant laws and regulations.

9.3.3 Responsibility to Protect Confidential Information

CAs shall specify this in the CPS and implement according to the relevant laws and regulations.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

CAs shall operate according to the Computer-Processed Personal Data Protection Act or the relevant regulations of other government agencies. CAs shall also follow the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data announced by the Organization for Economic Co-operation and Development (OECD) in transnational cooperation.

9.4.2 Information Treated as Private

CAs shall specify in the CPS or the Privacy Protection Policy the types of personal privacy information to be kept confidential.

9.4.3 Information Not Deemed Private

CAs shall specify in the CPS the types of information that can be disclosed, such as subscriber certificate, certificate revocation and suspension information, and CPS.

Information that will be disclosed in other business shall also be specified in the CPS.

9.4.4 Responsibility to Protect Private Information

CAs shall specify this in the CPS and implement according to the relevant laws and regulations.

9.4.5 Notice and Consent to Use Private Information

CAs shall specify this in the CPS and implement according to the relevant laws and regulations.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

CAs shall specify in the CPS the types of protected information to be disclosed as a result of an executive order or judicial request.

9.4.7 Other Information Disclosure Circumstances

CAs shall specify in the CPS the types of protected information to be disclosed at the subscriber’s request in accordance with the relevant laws and regulations.

9.5 Intellectual Property Right

The intellectual property right of this CP is owned by TWCA Inc.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

1. To establish the CPS according to this CP.
2. To publish the CPS and ensure that all operations and services conform to the CPS.
3. To issue and publish certificates and keep appropriate certification information.
4. To make sure that Subscriber Agreement satisfies Baseline Requirements.
5. To revoke the certificate of subscribers breaching their obligations or for any of the reasons specified in the Baseline Requirements.
6. To issue and publish the CRL.

7. To provide the repository services as described in section 2.

If CAs issued SSL Certificates or EVSSL Certificates, CA shall ensure the following compliant to requirements of TLS BR:

- Right to Use Domain Name or IP Address
- Authorization for Certificate
- Accuracy of Information
- No Misleading Information
- Identity of Applicant

If CAs issued S/MIME Certificates, CA shall ensure the following compliant to requirements of S/MIME BR:

- Right to Use the Email Address
- Authorization for Certificate
- Accuracy of Information
- No Misleading Information
- Identity of the applicant

9.6.2 RA Representations and Warranties

1. To carry out subscriber registration according to this CP and the CPS of CAs.
2. To carry out subscriber registration according to the security requirements specified in this CP and the CPS of CAs.
3. To accept certificate application request information and keep certification information valid for verifying the correctness of certificate application request information.
4. To ensure that subscribers understand and agree to the subscriber obligations during the subscriber registration.

9.6.3 Subscriber Representations and Warranties

1. To provide detailed and correct identity certifications and data when registering at the RA.
2. To reliably, properly and securely protect the private key according to this CP and the CPS of CAs.
3. To understand and agree to the terms governing the acceptance and use of certificates specified in this CP and the CPS of CAs and to use the certificate after accepting and agree to such terms.
4. To report to the RA according to the CPS of CAs when there are doubts about the fraud, exposure and loss of the private key corresponding to the certificate.
5. To follow the scope and restrictions specified in this CP and the CPS of CAs for the certificate and its corresponding private key.

9.6.4 Relying Party Representations and Warranties

Relying party shall examine the certificate according to the relevant rules specified in the CPS of respective CAs by creating the certificate trusted path and authenticating the certificate as a reference to determine if it is to trust the certificate.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

CAs shall specify them in the CPS.

9.8 Limitations of Liability

CAs shall specify them in the CPS.

9.9 Indemnities

CAs shall specify in the CPS the liability of CAs, RAs, subscribers and trustees according to the relevant terms in the Electronic Signature Act.

9.10 Term and Termination

9.10.1 Term

This CP shall be effective immediately after it is approved by the PMA.

9.10.2 Termination

The termination of this CP shall be determined by the PMA.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

The PMA shall establish contact channels with CAs under this PKI, including, but not limited to, phone, fax and/or email.

9.12 Amendments

9.12.1 Procedures for Amendment

The PMA of TWCA shall be the supervisor of this CP. This CP shall be reviewed at least once a year. CAs using this CP shall review their CPS at least once a year.

When this CP must be amended as a result of changes in the regulatory requirements and/or updates of international standards, CAs using this CP shall also update their CPS correspondingly.

Amendments made to this CP shall be approved by the PMA of TWCA.

9.12.2 Notification Mechanism and Period

When there are suggestions for updating this policy, please send or email such suggestions to the contact window described in section 1.5.2 for the PMA to review.

9.12.3 Circumstances Under Which OID Must Be Changed

The changes of OIDs in this CPS shall be approved by the PMA of TWCA.

9.13 Dispute Resolution Provisions

Disputes arising from or in connection with the use of this CP shall be settled in due faith by both parties through negotiations for a reasonable resolution.

CAs shall specify in the CPS the procedures for settling disputes arising from or in connection with the use of certificates.

9.14 Governing Law

The contents of this CP and the relevant CA 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

CAs shall specify in the CPS the applicable laws and regulations.

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 CP 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 amendment of CP is described in section 9.12.

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

No stipulation.

9.16.5 Force Majeure

Where the certificates are damaged as a result of Force Majeure or events beyond the reasonable control of CAs (e.g. wars or earthquakes), the CA issuing the certificate shall be free from any liability.

9.17 Other Provisions

No stipulation.

Appendix 1: Glossary

1. Internet

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

2. (Electronic) Message

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

3. Electronic Signature

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

4. Encrypt/Encipher

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

5. Decrypt/Decipher

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

6. Digital Signature

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

7. Private Key

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

8. Public Key

   In the digital signature using asymmetric cryptosystem, it refers to a set of matching public digital data for generating and verifying a digital signature. It can be used to verify the correctness of data in messages signed by the signed person, and can encrypt delivery messages when running the message privacy function.

9. <Public Key>Certification or Certificate

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

10. Certification Authority or Certificates Authority (CA)

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

11. Certification Practice Statement (CPS)

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

12. Asymmetric Cryptosystem

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

13. Hash Function

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

14. Issue a Certificate (Electronic Certification)

    It refers to the public key certificate or other certificates issued by the certification center (CA) after reviewing the 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.

15. CABF (CA/Browser Forum)

    It is a non-profit organization composed of CAs and browser developers. The organization's primary goal is to develop and drive industry standards for certificates, ensuring certificates are trusted and widely accepted. At present, the organization has defined relevant specifications for TLS certificates, CodeSign certificates, and S/MIME certificates. CAs should abide by relevant regulations when issuing such certificates, so that the certificates they issue can be trusted by the public (https://cabforum .org/).

Appendix 2: Acronyms and Abbreviations

TLS BR Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

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

EAL Evaluation Assurance Level

EVG Guidelines for the Issuance and Management of Extended Validation Certificates

EVSSL Extended Validation SSL

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

NB Network Banking

OCSP Online Certificate Status Protocol

OID Object Identifier

OECD Organization for Economic Co-operation and Development

PAA Pan-Asian e-Commence Alliance

PMA Policy Management Authority

PKCS Public Key Cryptography Standard

PKI Public Key Infrastructure

RA Registration Authority

RCA Root Certification Authority

RSA Rivest, Shamir, Adleman (encryption algorithm)

S/MIME BR Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates

SSL Secure Socket Layer

TCSEC Trusted Computer System Evaluation Criteria

URL Universal Resources Location