Certificate Policy for the Government Public Key Infrastructure

Version 1.7

Administrative Organization: National Development Council

Executive Organization: ChungHwa Telecom Co., Ltd.

January 31, 2013

Contents

1. Introduction

In order to create an electronic government infrastructure environment, the Government Public Key Infrastructure (GPKI) was established to provide an administrative agency electronic certification and security system in conjunction with the electronic government program (2001 to 2004). The public key infrastructure hierarchy established for this infrastructure in accordance with ITU-T X.509 standards includes the public key infrastructure trust anchor - Government Root Certification Authority (GRCA) and subordinate CAs formed by government agencies. Addition of certificate authorities (CAs) to this infrastructure must be done by CAs established by the competent authorities based on electronic government certificate service assignments to issue certificate used for electronic government applications in order to provide faster and more convenient internet services, raise government administration efficiency and promote the development of e-government and e-commerce applications.

The National Development Council (NDC) is the administrative agency of the infrastructure. The NDC and Government Electronic Certification Steering Committee (GECSC) shall perform duties including those detailed in section 1.3.1 to assist in the administration of this infrastructure. This Certificate Policy for the Government Public Key Infrastructure (GPKI CP) was established specifically to provide common specifications for certificate administration of this infrastructure as well as promote internal and external infrastructure interoperability.

1.1 Overview

1.1.1 Certificate Policy

The certificate policy is technical policy document established based on Electronic Signature Act and related international standards (such as IETF RFC 2527) which serves as a basis for certification policy statements set up for this infrastructure. In order to ensure the interoperability of public key certificates, the government agency CAs added to this infrastructure shall follow this certificate policy and may not establish independent certificate policies.

There are five assurance levels defined under this certificate policy:

test level, level 1, level 2, level 3 and level 4. Of these, test level, the lowest assurance level, is used exclusively for test certificates. For levels 1, 2, 3 and 4, the level of assurance is higher as the number increases. This CP takes the following three aspects into general consideration when defining the different assurance levels:

(1) The ability of the relying party to ensure the recording of certificate subject and public key binding in the certificate.

(2) The ability of the relying party to ensure the certificate subject recorded in the certificate can control the use of private key which corresponds to public key recorded in the certificate.

(3) The ability of the relying party to ensure the security of the systems and procedures used to issue and administer certificates and deliver private keys.

Regarding the CP object identifiers (CP OID, see section 1.2) for the five assurance levels jointly registered for this infrastructure, an appropriate CP OID may be listed in the certificatePolicies Extension in the certificate when a CA issues a certificate which may be used by relying party to check the applicability of the certificate.

In addition, the CP OID for the five assurance levels registered for this infrastructure can be provided to CAs when issuing cross-certificates. When there is a policy mapping relationship for the policyMappings Extension field indicated in the cross-certificate CP, the relying party may use the CP OID to check certificate policy mapping relationship of the issuing CA to the subject CA.

1.1.2 Relationship between Certificate Policy and Certification Practice Statement

CAs must state how to achieve the assurance level used by this CP in the CPS.

1.1.3 Certificate Policy Object Identifiers Used by Certificate Authorities

This infrastructure’s CP object identifiers (OID) used by CAs must be approved by the NDC. If there are any problems caused by the use of this CP by other CAs outside this infrastructure, the CA shall bear full responsibility.

CAs shall select a suitable CP OID based on the respective scope of

use of the certificate and record it in the certificate's CP extension field. However, the GRCA's self-signed certificates only serve as a trust anchor information object in the infrastructure. The relying party directly trusts the public key information recorded in the self-signed certificate and therefore the CP OID does not have to be listed in the certificate.

The GRCA and non-infrastructure CAs only may use the infrastructure's CP OID in the policyMappings Extension after the GECSC approves the corresponding relationship to the CP.

1.2 Certificate Policy Identification

The name of this policy is the Certificate Policy for the Government Public Key Infrastructure. This is version 1.7. The announcement date was January 31, 2013.

The CP OID for the five assurance levels defined in the CP are registered in the id-tw-gpki arc as follows:

id-tw OBJECT IDENTIFIER ::= {2 16 886}
id-tw-gov OBJECT IDENTIFIER ::= {id-tw 101}
id-tw-gpki OBJECT IDENTIFIER ::= {id-tw-gov 0}
id-tw-gpki –certpolicy OBJECT IDENTIFIER ::= {id-tw-gkpi 3}

Table 1-1 CP OID

Assurance level	OID Name	OID Value
Test level	id-tw-gpki-certpolicy-testAssurance	{id-tw-gpki-certpolicy 0}
Level 1	id-tw-gpki-certpolicy-class1Assurance	{id-tw-gpki-certpolicy 1}
Level 2	id-tw-gpki-certpolicy-class2Assurance	{id-tw-gpki-certpolicy 2}
Level 3	id-tw-gpki-certpolicy-class3Assurance	{id-tw-gpki-certpolicy 3}
Level 4	id-tw-gpki-certpolicy- class4Assurance	{id-tw-gpki-certpolicy 4}

1.3 Communicability and Applicability

1.3.1 Government Electronic Certification Steering Committee

The NDC established the Government Electronic Certification Steering Committee in order to establish the electronic government certification system, promote the electronic government public key

infrastructure and speed up development of convenient internet public services by government agencies. The Government Electronic Certification Steering Committee has one convener concurrently served by vice chairman appointed by the committee and 9 to 17 committee members. Except for the convener who is an ex-officio member, scholars, experts, industry and agency representatives may serve as committee members. Their duties are as follows:

(1) Examination of Government Electronic Certification Policy and Certification Practice Statement.
(2) Examination of the Government Electronic Certification Policy related technical specifications.
(3) Review of the government electronic certification system framework
(4) Other matters related to government electronic certification administration.

1.3.2 Government Root Certification Authority

The GRCA is the highest level root CA in this infrastructure. Its main duties are:

(1) Subordinate CA certificate issuance and administration.
(2) Establishment of the cross-certification procedure for this infrastructure. Issuance and administration of this infrastructure's level 1 subordinate CA certificates and certificates of other CAs outside this infrastructure.
(3) Posting certificates and certification authority revocation list (CARL) in the repository and ensuring normal operation of the repository.

The GRCA is the trust anchor of this infrastructure. Considering that the trust anchor must have the highest level of credibility, the GRCA must operate at assurance level 4. With the permission of the GECSC, the GRCA may perform cross-certification with CAs outside this infrastructure. The GRCA shall specify the cross-certification procedure with CAs in the CPS.

1.3.3 Subordinate Certification Authorities

Subordinate certification authorities (subordinate CAs) are another type of certification authority in the infrastructure which are mainly responsible for the issuance and administration of end entity certificates.

When necessary, the hierarchy of the public key infrastructure structure may be followed with the level 1 subordinate CAs issuing certificates to level 2 subordinate CAs, level 2 subordinate CAs issuing certificates to level 3 subordinate CAs and so on. The subordinate CA structure may not directly perform cross-certification with CAs outside this infrastructure.

The subordinate CA structure shall be established in accordance with relevant regulations in the CP and include contact windows.

1.3.4 Registration Authorities

Registration Authorities (RAs) are mainly responsible for collection and authenticity verification of subscriber identity and related information to facilitate the entry of this information into certificates and storage of certificate application information by subsequent CAs.

GRCA shall serve the role of its own RA and perform RA work in accordance with the approved CPS. RAs may be set up independently by subordinate CAs. Their duties shall be stated in the CPS.

1.3.5 Repository

The repository provides inquiry and downloading services for CA certificates, CRLs and certificate status and also publishes information related to certificate work in the CP and CPS.

Each CA must at least have one repository for external service. Repositories may maintained by the CA itself or its operation commissioned to another organization. CAs shall state the repository website in the CPS and ensure the usability, access control and information integrity of the repository.

1.3.6 End Entities

End entities (EE) including the following two types of entities:

(1) Subscriber

(2) Relying parties

1.3.6.1 Subscriber

For certificates issued to organizations or individuals, subscribers refers to the entity identified by the certificate subject name on the certificate. That entity holds the private key which corresponds to the certificate’s public key. The subscriber must legally use the certificate and

its corresponding private key according to the CP OID recorded in the certificate. For the issuance of property type (such as application processes) and device certificates, the property has no capacity to act so the subscriber is the individual or organization applying for certificate.

CAs may issue CA certificates to other CAs but the CA identified by the certificate subject name in the CA certificate is not named as the subscriber but the subject CA.

1.3.6.2 Relying Parties

Relying parties refer to the certificate subject name of trusted certificates and entities that have binding relationships with public keys. Relying parties must check the validity of all certificates used based on the the CA certificate and certificate status information.

Relying parties may use certificates to verify the integrity of digitally signed information to confirm the identity of the information sender and establish secret communication channels between subscribers. In addition, the relying parties may use the information in certificates (such as CP OID) to determine if the certificate usage time is adequate.

1.3.7 Other Related Members

CAs may select other organizations to assist with the processing of certificate-related work. The related work procedures and identity of entrusted organizations shall be stated in the CPS.

1.3.8 Applicability

Five types of assurance levels are defined in the CP based on individual security requirements in response to various application requirements. When determining the certificate assurance level, the CA shall carefully assess the various risks including environmental, potential risks, vulnerabilities, certificate usage and importance based on their application.

1.3.8.1 Certificate Usage

The CP does not have mandatory provisions concerning certificate usage at various assurance levels and does not restrict the use counterparts of each assurance level. Recommended usage is described below:

Table 1-2 Certificate Usage

Assurance level	Usage
Test Level	Only provided for test use. No legal liability borne for the transmitted data.
Level 1	Rudimentary assurance level. Suitable for use in Internet environments with a low risk of malicious tampering or identification of subscriber entity names. Guarantees the integrity of a signed document when a higher assurance level cannot be provided. Not suitable for use with electronic transactions requiring certification.
Level 2	Basic assurance level. Suitable for use with data which may be tampered with. Malicious tampering is not present in the Internet environment (data interception is possible but the probability is not high). Not suitable for the signing of important documents.
Level 3	Medium assurance level. Suitable for applications where there is a higher risk of malicious interception or tampering of data by users in the Internet environment compared to level 2. Transmitted data includes electronic transactions.
Level 4	High assurance level. Suitable for use in high-risk Internet environments or restoration costs of tampered data are high. Transmitted information includes high value electronic transactions and highly confidential document.

1.3.8.2 Certificate Use Restrictions

Relying parties shall first determine which assurance level is required for the application. Then, a certificate with the suitable assurance level is selected and the instructions in section 6.1.9 are followed to determine whether that certificate is suitable for use as a private key for that application.

The relying parties shall use the validation method defined in accordance with related international standards (i.e. X.509 standard or IETF RFC 5280) to determine certificate validity when checking the certificate.

1.3.8.3 Certificates are not Permitted to be Used for the Following:

The certificates issued by CA with this infrastructure are not permitted to be used for the following purposes:

(1) Crime

(2) Control of military orders for nuclear, biological and chemical weapons.

(3) Operation of nuclear equipment.

(4) Aviation flight and control systems.

1.4 Contact Details

1.4.1 Certificate Policy establishment and administration organization

National Development Council

1.4.2 Contact Information

Submit any suggestions regarding this CP to the NDC. For contact information, refer to http://grca.nat.gov.tw/.

1.4.3 Certificate Practice Statement Review

The CA shall first check if the CPS conforms to related CP regulations and then send it to the Government Electronic Certification Steering Committee for review. Following review and approval, the CA may formally apply the CP to this infrastructure.

Certificate issuance services may be offered to external parties only after the CPS is approved by the MOEA in accordance with the bylaws of the Taiwan Electronic Signatures Act.

The NDC has the right to audit CAs to determine if the certificate

policy is being followed (follow section 2.7). CAs shall also conduct routine self-audits to verify that the CP assurance level is being maintained.

2. General Provisions

2.1 Obligations

2.1.1 CA Obligations

The CA has the following obligations:

(1) Issue and post certificates.

(2) Perform authentication procedures in accordance with Chapter 3.

(3) Issue and post CARLs and CRLs or provide on-line status checking services.

(4) Provide related controls in accordance with Chapter 4 and 6.

(5) Post CPS and explain the obligations of subscribers and relying parties.

(6) Protect private keys in accordance with Chapters 4, 5 and 6.

(7) Confirm private key usage of individual CAs. Private keys used for certificate and CRL issuance may not be used for other purposes such as regular digital signatures, identification, data encryption or key encryption.

(8) The CP shall be followed for the CA infrastructure specified in CPS.

2.1.2 RA Obligations

The RA have the following obligations:

(1) Provide related controls in accordance with Chapters 4, 5 and 6.

(2) Perform identification and authentication of certificate applications in accordance with Chapter 3.

(3) Notify subscribers and relying parties about CA and RA obligations and responsibilities.

(4) Notify subscribers and relying parties the relevant provisions of the CP which should be followed during use or receipt of CA issued certificates.

(5) Protect private keys in accordance with Chapters 4, 5 and 6.

(6) Confirm private key usage for individual RAs. RAs shall follow the private key use instructions in section 6.1.9. RA private keys may not be used for non-RA work without the permission of the CA.

2.1.3 Subscriber Obligation

Subscribers who receive certificates issued by the CA shall have the following obligations:

(1) Follow procedures in Chapters 3 and 4.

(2) Correctly use certificates.

(3) Properly keep and use private keys (not required for certificates having a test level assurance level).

(4) Immediately notify the CA in the event of private key compromise (not required for certificates having a test level assurance level).

2.1.4 Relying Party Obligation

Relying parties using certificates issued by the CA shall have the following obligations:

(1) Familiarity of certificate applicability and assurance level.

(2) Use certificate in accordance with certificate applicability.

(3) Check certificate validity for accuracy. Use the validation method defined in accordance with related international standards (i.e. X.509 standard or IETF RFC 5280) to verify the certificate validity when checking the certificate path.

(4) Check certificate revocation and suspension lists for accuracy.

2.1.5 Repository Service Obligations

The CA repository is obligated to provide the following services:

(1) Regularly post issued certificates.

(2) Regularly post information on revoked and suspended certificates.

(3) Post latest CP and CPS information.

(4) Repository access controls must be established in accordance with Section 2.6.3.

2.2 Liability

2.2.1 CA Obligations

2.2.1.1 Warranties and Limitations on Warranties

If the CP OID set up for any assurance level are used for CA issued certificates, it means the CA guarantees compliance of the information contained in the issued certificate with the CP. The CA must follow CP regulations. Otherwise, the CP OIDs listed in the CP for any assurance level may not be used for certificate issuance.

2.2.1.2 Disclaimer and Limitations of Warranties

CAs may place disclaimers and limitations in the CPS to exclude liability outside the above limitations. However, CAs may not include the consequences arising from their own negligence in the exclusions.

2.2.1.3 Other Exclusions

CAs may specify other exclusions regarding damages arising from a force majeure and other reasons not attributable to the CA including natural disasters, accidents, emergencies or specific events in the CPS.

However, CAs may not include the consequences arising from their own negligence in the exclusions.

2.2.2 RA Liabilities

CA shall bear all liabilities for work performed by RAs on behalf of the CA. RA liabilities shall be determined based on the rights and obligations with the CA. CAs shall state RA liabilities in the CPS or in RA contracts or agreements.

2.2.2.1 Warranties and Limitations on Warranties

Not specified.

2.2.2.2 Disclaimers and Limitations

Not specified.

2.2.2.3 Other Exclusions

Not specified.

2.3 Financial Responsibility

2.3.1 Indemnification by Subscribers and Relying Parties

The liability responsibility of subscribers and relying parties shall be included in the CA CPS.

2.3.2 Administrative Processes

The competent authorities of the CA shall determine the administrative procedures of the CA.

2.4 Interpretation and Enforcement

Where there are versions of this CP in languages other than the traditional Chinese version, the traditional Chinese version shall prevail if there are any discrepancies between the traditional Chinese version and versions in other languages.

2.4.1 Governing Law

This CP was established in accordance with the laws and regulations of the Republic of China (ROC). In the event of a dispute, the laws and regulations of the ROC shall govern the interpretation of this CP.

2.4.2 Severability, Survival, Merger and Notice

Should it be determined that any section in the CPS is incorrect or invalid, the other sections of the CPS shall remain in effect until the CPS is updated. The process of updating the CPS is described in Section 8.1.

2.4.3 Dispute Resolution Procedures

Disputes arising from the interpretation of the CP content shall be settled through negotiation by the parties involved if so possible. If the matter cannot be settled through negotiation, the NDC may establish another dispute resolution procedure or request an interpretation. The CA shall stipulate the dispute resolution procedure in the CPS.

2.5 Fees

2.5.1 Certificate Issuance and Renewal Fees

Not specified.

2.5.2 Certificate Inquiry Fees

Not specified.

2.5.3 Revocation and Status Inquiry Fees

Not specified.

2.5.4 Fees for Other Services

Not specified.

2.5.5 Refund Policy

Not specified.

2.6 Publication and Repository

2.6.1 Publication of CA Information

The CA shall regularly publish the following in the repository:

(1) This Certificate Practice Statement

(2) CRLs (or provide on-line certificate status inquiry)

(3) CA self-certificates at least until expiry of all certificates issued by the corresponding private key of that certificate).

(4) Issued certificates (including certificates issued to other CA)

(5) CARLs (if the CA issues certificate to other CA)

(1) Privacy protection policy

In addition to the above information, the CA shall publish information needed for the verification of digital signatures.

The CA CPS shall contain the maximum time limit for repository service suspension times.

2.6.2 Frequency of Publication

The CRL publication frequency is stipulated in section 4.4.

2.6.3 Access Controls

(1) Access controls are not needed for CP and CA CPS acquisition.

(2) The CA shall determine independently if access controls are needed for certificates.

The CA shall protect repository information to prevent malicious distribution or modification. Public key and certificate status information shall be made publicly available over the Internet.

2.6.4 Repositories

The repository shall be operated by CAs and other organizations in accordance with section 1.3.5. Related repository information shall be contained in the CA CPS.

2.7 Compliance Audit

CAs that issue assurance level 2, 3 and 4 certificates shall establish a fair and objective compliance audit system to verify that operations are in compliance with the procedures in the CPS and CP.

2.7.1 Compliance Audits

CAs shall undergo routine compliance audits. CAs operating under assurance levels 3 and 4 must receive at least one compliance audit each year and CAs operating under assurance level 2 must receive at least one compliance audit every two years. There is no specified compliance audit requirement for CAs operating under the test level and assurance level 1.

CAs may conduct routine and non-routine compliance audits of subordinate CAs and RA to verify that operations of subordinate entities are in compliance with the CPS.

The NDC must perform non-routine compliance audits of subordinate certificate authorities (subordinate CA) that are interoperable with the GRCA. The reason shall be stated when non-routine audits are performed by the NDC.

2.7.2 Identity and Qualifications of Compliance Auditors

Compliance auditors shall be independent from the audited CA and may be performed by the following entities:

(1) Impartial third party

(2) Independent entity outside of the organization boundaries and

the audited CA.

The compliance auditors shall perform a fair and independent evaluation. Qualification determination must be approved by the NDC. Compliance auditors shall be familiar with related CA certificate issuance and administration regulations. The identity of compliance auditors shall checked during CA compliance audits.

2.7.3 Compliance Auditors' Relationship to the Audited Party

Compliance auditors shall be independent from the audited CA as stipulated in section 2.7.2.

2.7.4 Scope of Compliance Audits

The scope of compliance audits is as follows:

(1) CA compliance with the CPS.

(2) CA CPS compliance with CP regulations.

Compliance auditors may conduct audits of CA-related maintenance and operation units such as RAs.

If the CA signs a cross-certification agreement with a subordinate CA, the scope of the compliance audit should cover subordinate CA compliance with the provisions of the cross-certification agreement.

2.7.5 Actions Taken as a Result of Deficiencies

When a compliance auditor discovers that the establishment, operation or maintenance of the CA does not comply with the CP or cross-certification agreement, the following actions shall be taken:

(1) Discrepancies noted by audit personnel.

(2) Competent authorities of the CA shall be informed of the discrepancies. The NDC shall be informed immediately of severe deficiencies.

The CA where the deficiency occurred shall correct the deficiency as

stipulated in the audit report, CP and cross-certification agreement.

Depending on the type, severity and the time required to fully correct the deficiency, the NDC may decide to suspend GRCA operations, revoke GRCA certificates issued to subordinate CAs or other courses of actions. Related procedures are established separately by the NDC.

2.7.6 Communication of Results

Information concerning the certificates relied upon by relying parties shall be made public unless the information may be used for attacks on the system.

The results of the most previous compliance audit shall be published by the CA.

2.8 Confidentiality

2.8.1 Types of Information to be Kept Confidential

(1) All personal and organization information contained on certificate applications other than person or organization information listed on the certificate is considered confidential information which shall not be disclosed without the consent of the subscriber or as stipulated under the law.

(2) The private keys and access codes used for CA operation are considered confidential information and may not be disclosed.

(3) Audit logs shall not be made available as a whole except under the circumstances described in section 2.7.6.

The categories of confidential information shall be listed in the CA CPS.

2.8.2 Types of Non-Confidential Information

(1) Certificate, CRL and revocation / suspension information is not

considered confidential.

(2) Identification or other information appearing on the certificates is not considered confidential unless stipulated otherwise.

The categories of non-confidential information shall be listed in the CA CPS.

2.8.3 Disclosure of Certificate Revocation / Suspension

Revocation and suspension information is non-confidential information which shall be made public.

2.8.4 Release to Law Enforcement Officials

Regulations regarding the provision of confidential information outlined in section 2.8.1 to law enforcement officials shall be set down in the CA CPS.

2.8.5 Release as a Part of Civil Discovery

Regulations regarding the provision of confidential information outlined in section 2.8.1 for civil suits shall be set down in the CA CPS.

2.8.6 Disclosure upon Subscriber Request

Regulations regarding the provision of confidential information outlined in section 2.8.1 to subscribers shall be set down in the CA CPS.

2.8.7 Other Information Release Circumstances

Release is handled in accordance with relevant laws and regulations.

2.9 Intellectual Property Rights

The intellectual property rights of the CP are jointly held by the NDC and Chunghwa Telecom Co., Ltd. (CHT). The NDC and CHT retains all rights to the CP. Relevant information may be downloaded

from the GRCA repository or reproduced and distributed in accordance with related copyright laws but must be copied in its entirety and state ‘property of National Development Council and Chunghwa Telecom Co., Ltd.’. In addition, those who reproduce or distribute this CP may not collect fees from other parties or refuse others access to the CP. The NDC and CHT shall not be liable for any consequences arising from improper use or distribution of this CP.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

The subject name of this infrastructure conforms to the Distinguished Name (DN) of X.500.

The CA reserves the right to decide whether a subject alternative name should be accepted during the certificate application process. If the CA requests the addition of a subject alternative name to the certificate, it must be listed as a non-critical extension field in the extension field.

3.1.2 Need for Names to be Meaningful

The subject names for organization and individual certificates must comply with subject name regulations in related ROC law and use the names provided in the official registration.

Subject names in equipment and server software certificates must be the name of the administrator of that equipment or server software. In addition, the common name included should be easily understandable in principle. For example, the name of the module, serial number or the name of the application program.

3.1.3 Rules for Interpreting Various Name Forms

The NDC is responsible for interpretation of name forms including those in certificate format profiles.

3.1.4 Uniqueness of Names

Certificate subject names in this infrastructure must be unique. The NDC is responsible to establishing related regulations for X.500 name space use by CA to ensure the uniqueness of names. Instructions on how to use X.500 name space must be included in the CA CPS. There should also be instructions on how to ensure the uniqueness of certificate subject names when identical names appear during certificate subject naming (i.e. how does the CA ensure that two persons with the same name from the same city / county receive unique certificate subject names when applying for certificates from the CA).

3.1.5 Name Dispute Resolution Procedure

Name ownership shall be handled in accordance with the naming rules in related ROC laws and regulations (Company Act, Name Act and Civil Education Act). CAs shall establish name dispute resolution procedures in the CPS. This requirement does not apply to CA operating at a test level assurance level.

The NDC is the arbitrator for disputes regarding names established for this infrastructure.

3.1.6 Recognition, Authentication and Role of Trademarks

If the certificate subject name includes a trademark, its name must comply with related ROC trademark laws.

3.1.7 Method to Verify Possession of Private Key

The CA shall verify possession of the private key of the certificate applicant during the certificate application process and make a record in

the certificate's public key pair.

Different methods must be used by key generators to verify possession of the private key. The three verification methods contained in the CP are as follows:

(1) When key pairs are generated by the CA or RA for subscribers:

Subscribers do not need to prove possession of the private key but must undergo identification verification in accordance with sections 3.1.8, 3.1.9 and 3.1.10 to obtain private key and activation data. The private key shall be sent to the subscriber in accordance with section 6.1.2.

(2) When key pairs are generated by a trusted third party (such as card issuance center) for subscribers:

CAs or RAs must obtain the subscriber's public key from a trusted third party through secure channels in accordance with section 6.1.3. Subscribers do not need to prove possession of the corresponding private key but must undergo identification verification in accordance with sections 3.1.8, 3.1.9 and 3.1.10 to obtain private key and activation data. The private key shall be sent to the subscriber in accordance with section 6.1.2.

(3) When key pairs are self-generated by subscribers:

The private key can be used by the subscriber to generate one signature and the signature is provided to the CA and RA in accordance with section 6.1.3. The CA and RA uses the subscriber public key to verify the signature to prove subscriber possession of the private key. The CP allows the use of other methods with an equivalent security level (for example the various methods listed in RFC 2510 or RFC 2511) to prove possession of the private key.

3.1.8 Authentication of Organization Identity

The number of identification documents, authentication verification procedure and counter processing requirement needed for organization identity differ based on the assurance level as listed in the Table below:

Table 3-1 Organization Identity Authentication Procedure

Assurance Level	Organization Identity Authentication Procedure
Test level	Not specified
Level 1	(1) Written documentation does not need to checked (2) Applicant only needs to have an e-mail address to apply for a certificate. Identification authentication procedure does not need to be followed. (3) Does not need to be processed at counter.
Level 2	(1) Written documentation does not need to be checked. (2) Subscriber submits organization information such as organization identification code (such as business administration number), name of organization, etc… This information should be cross-checked with CA-approved information. (3) Does not need to be processed at counter.
Level 3	There are two types of organization identity authentication: (1) Government agency (organization) or department identity authentication a. Official documents must be used for certificate application the first time a government authority or department applies for a certificate. The CA or RA must verify the existence of the agency or department and verify the authenticity of the official documents.

Assurance Level	Organization Identity Authentication Procedure
	b. For government authority certificate usage periods, CA or RA may use the agency code announced by the government directory service system or the Directorate-General of Personal Administration, Executive Yuan to verify the authenticity of the organization existence and then approve the issue of new certificates. However it may not be used by subordinate departments and new documents still need to be applied for. (2) Identity Authentication of Civic Organizations Application information shall include the organization, location and name of representative which is sufficient to identify the organization. Besides verifying the authenticity of the application information and representative identity, the CA or RA shall verify that the representative has the right to apply for a certificate on behalf of the organization. The representative shall appear in person at the CA or RA to process the application. If the representative is unable to appear at the counter in person to process the application, an agent with power of attorney shall process the application on his behalf but the CA or RA verify the authenticity of the letter of attorney (such as comparison of the representative's seal on the letter of attorney) and authenticate the agent's identity in accordance with assurance level 3 regulations in section 3.1.9. If the civil organization has completed the registration procedure from the competent authority or the above

Assurance Level	Organization Identity Authentication Procedure
	counter identification and authentication procedure of a CA, RA or trusted organization or individual (such as a notary public) of the CA prior to submitting the application and leaves behind the registration or identity verification or authentication information (for example leaving behind the seal impression or notary public affixing a certification stamp to the application), the CA or RA may allow the organization to show other supporting evidence in place of the above identification and authentication method when applying for a certificate. The CA must perform a risk assessment of the supporting evidence and confirm that the risk is not greater than the risk of adopting the above identification and authentication procedures. The CA or RA also must have the ability to authenticate supporting evidence before accepting the supporting evidence in place of the identification and authentication procedure used for certificate application. The above civic organizations refers to private legal persons, non-corporate bodies or subsidiary organizations of the previous two.
Level 4	Identity authentication of organizations may be done is one of the following two ways: (1) Government authority or department identity authentication Government authority or department identity authentication must appoint a CA or RA authenticable

Assurance Level	Organization Identity Authentication Procedure
	individual by official document to represent that government authority or department for CA or RA certification application. The CA or RA shall verify the existence of the government authority or department, the authenticity of the official documents and authenticate the identity of the individual representing the government authority or department in accordance with the assurance level 4 regulations in section 3.1.9. (2) Identity authentication of private organizations Application information should include the organization name, location and representative name which is sufficient to identify the organization. The CA or RA must verify the authenticity of application information and the identity of the representative and also verify that the representative has the right to apply for the certificate on behalf of the organization. The representative shall appear in person at the CA or RA to process the application. The above private organizations refers to private legal persons, non-corporate bodies and subsidiary organizations of the previous two.

The identification and authentication procedures of certificate issuing CA towards subject CA shall reference the above identification and authentication procedures for organizations and may not lower than the assurance level of the certificates that the subject CA intends to issue.

The GRCA shall at least follow the identity authentication

procedures for government authorities or departments with an assurance level of 3 or above for the subordinate CA identity authentication set up by government authorities or departments.

3.1.9 Authentication of Individual Identity

The number of identification documents, authentication procedures and counter processing requirements for individual identification authentication differ based on assurance level as shown in Table below:

Table 3-2 Individual Identity Authentication Procedure

Assurance Level	Individual Identity Authentication Procedure
Test level	Not specified
Level 1	(1) Written documentation does not need to checked (2) Applicant only needs to have an e-mail address to apply for a certificate. Identification authentication procedure does not need to be followed. (3) Does not need to be processed at counter.
Level 2	(1) Written documentation does not need to be checked. (2) Subscriber submits personal information such as personal identification code (such as personal ID number), name of person, etc… This information should be cross-checked with CA-approved information. (3) Does not need to be processed at counter.
Level 3	(1) Cross-checking written documentation: Subscribers must display at least one original copy of approved identification with photo (such as national ID card) to

Assurance Level	Individual Identity Authentication Procedure
	the CA or RA when applying for a certification to authenticate the identity of the subscriber. If the subscriber (such as a minor) is unable to submit the above photo identification, written identification documents (such as household registration) issued by the government which are sufficient to prove identity may be used instead and have one adult with capacity to act to guarantee the identity of the subscriber. The identity of the adult providing the written guarantee must pass through the above authentication. (2) Personal data submitted by subscribers such as personnel identification numbers (ID card numbers), names and addresses (such as household registration address) shall be cross-checked with the information (such as household registration information) registered with the competent authorities or other information registered with trusted third parties approved by the competent authorities. (3) Counter processing: Subscribers must appear in person at the CA or RA to prove their identity. If the subscriber is unable to go to the counter in person for application processing, an agent with power of attorney must process the application at the counter. The CA or RA must verify the authenticity of the power of attorney (for example, comparison of the subscriber's seal on the power of attorney) and authenticate the identity of the agent in accordance with the above regulations. For individuals who have completed the counter

Assurance Level	Individual Identity Authentication Procedure
	authentication and authentication procedures at the CA, RA or a trusted organization or individual (such as notary public) of the CA or RA before certification application and have left supporting evidence for identification and authentication (such as providing biometric data, seal impression or certification stamp affixed to the application by notary public), the CA or RA may permit the supporting evidence to take the place of the above identification and authentication method when applying for a certificate. The CA must perform a risk assessment of the supporting evidence and confirm that the risk is not greater than the risk of adopting the above identification and authentication procedures. The CA also must have the ability to authenticate supporting evidence before accepting the supporting evidence in place of the identification and authentication procedure used for certificate application.
Level 4	(1) Cross-check written identification documents: Subscribers must display at least one original copy of approved identification with photo (such as national ID card) to the CA or RA when applying for a certification to authenticate the identity of the subscriber. (2) Personal data submitted by subscribers such as personnel identification numbers (ID card numbers), names and addresses (such as household registration address) shall be cross-checked with the information (such as household registration information) registered with the competent authorities. (3) For counter application processing, subscribers must appear

Assurance Level	Individual Identity Authentication Procedure
	in person at the CA or RA to prove their identity.

3.1.10 Authentication of Hardware Devices or Server Software

For computer and telecommunications equipment (routers, firewalls, etc..) or server software (web server) which have no legal capacity, the identity of the organization or individual as the equipment administrator must be submitted for certification application, The regulations in sections 3.1.8 or 3.1.9 must be followed for organization or individual identity authentication.

The following information shall be submitted when applying for a certificate:

(1) Equipment or server software identification information.
(2) Equipment or server software public keys (submit as specified in 6.1.3).
(3) Equipment or server software authorization and attributes (such as submit authorization or attributes only if required to be included in the certificate).
(4) Submit contact information of the organization or individual applying for the certificate.

3.2 Routine Key Change and Certificate Renewal

3.2.1 Routine Key Change

Routine key change is the issuance of one new certificate that has the same features and assurance level as the old certificate. In addition to

owning another newly generated public key (paired with a separate new private key) and separate serial number, the certificate may be assigned a different validity period.

For CA certificates, the CA issuing the certificate shall follow the authentication procedures in section 3.1 to identify and authenticate the subject CA when the subject CA applies for a routine key change.

For end entity certificates, the CA shall follow the regulations in Table 3-3 to identify and authenticate the subscriber when the subscriber applies for a routine key change.

3.2.2 Certificate Renewal

Certificate renewal refers to the issue of one new certificate with the same certificate subject name, key and related information as the old certificate. The validity period of the certificate is extended and one new serial number is given. If certificate key pairs have not entered their usage period (follow regulations in section 6.3.2), the private keys are not under eminent threat of compromise and the subscriber name and attributes are not change, the certificate will be permitted to apply for renewal.

For CA certificates, the CA issuing the certificate shall follow the initial registration authentication procedure in section 3.1 to identify and authenticate the subject CA when the subject CA applies for certificate renewal.

For end entity certificates, the CA shall identify and authenticate subscriber according to the regulations in Table 3-3 when a subscriber applies for certificate renewal.

Table 3-3 Routine Key Change and Certificate Renewal Identification Authorization Regulations

Assurance Level	Subscriber Certificate Routine Key Change and Certificate Authorization Requirements
Test level	Not specified
Level 1	Signature keys may be used to authorize the identity of subscribers or initial registration authorization procedures in section 3.1 may be followed.
Level 2	Signature keys may be used to authorize the identity of subscribers or initial registration authorization procedures in section 3.1 may be followed but if over 15 years have passed since initial registration, the initial registration authorization procedures in section 3.1 must be followed.
Level 3	A valid signature key may be used to authorize the identity of subscribers or initial registration authorization procedures in section 3.1 may be followed but if over 9 years have passed since initial registration, the initial registration authorization procedures in section 3.1 must be followed.
Level 4	A valid signature key may be used to authorize the identity of subscribers or initial registration authorization procedures in section 3.1 may be followed but if over 3 years have passed since initial registration, the initial registration authorization procedures in section 3.1 must be followed.

3.3 Rekey after Revocation

The regulations in section 3.1 shall be followed for the issuance of new certificates after certificate revocation. The subscriber must repeat the initial registration procedure.

3.4 Revocation Request

The CA or RA must authenticate the certificate revocation application. The CA shall follow the regulations in section 4.4 and specify the applicant and identity authentication method in the CPS to verify the applicant has the right to submit the certification revocation application.

Regardless of whether the private key is compromised, the private key signature and certificate to be revoked may be used to authenticate the identity of the certificate revocation application.

4 Operations Requirements

4.1 Certificate Application Procedure

The CA must specify the initial registration, certificate renewal and certificate key renewal application procedures, application locations and websites in the CPS.

In order to ensure the interoperability and reliability of the e-government related time stamp services, the operations of the Time Stamp Authority (TSA) established by the government authorities must conform to regulations in the Certificate Policy for the Government Public Key Infrastructure when applying for a time stamp server application software certificate with the infrastructure CA. The Practice Statement for the Time Stamp Authority must first pass Government Public Key Infrastructure Time Stamp Policy review when the infrastructure CA accepts the time stamp server application software certificate application.

The GRCA must accept certificate applications from CAs established by relevant competent authorities in accordance with electronic government certification service assignments to become level 1 CAs in the infrastructure. The application procedure shall be determined separately and published in the GRCA CPS.

The procedures for cross-certificate applications by CAs outside the infrastructure to the GRCA are set up separately by the NDC.

Subordinate CAs at all levels of the infrastructure may not accept applications from another CA to become its subordinate CA without the approval of the CA above it.

4.2 Certificate Issuance

Certificate issuance by CAs shall follow the regulations in section 5.2 and CPS. Suitable personnel shall perform related certificate issuance tasks. After certificate issuance, the CA or RA shall notify the application in a suitable manner. CAs operating at assurance levels 1, 2, 3 and 4 shall specify the applicant notification method after certificate issuance in the CPS.

If the CA or RA refuses to issue the certificate, the certificate applicant shall be notified in a appplicated manner and the reasons for the refusal shall be clearly explained to the applicant. Moreover, the CA may refuse to issue the certificate for reasons other than applicant identification and authentication issues. CAs operating at assurance levels 1, 2, 3 and 4 shall specify the applicant notification method after certificate issuance refusal in the CPS.

The GRCA shall issue one self-signed certificate during each key lifespan to establish a trust anchor for certificates and may issue a number of self-issued certificates in response to its own key and CP renewal. After the content of these certificates has been found to be error-free by the NDC, follow the regulations in section 6.1.4 to send the certificate to the trusted party.

4.3 Certificate Acceptance

After CAs which issues assurance level 2, 3 and 4 certificates issues a certificate, the applicant shall review the certificate content and accept the issued certificate before the issued certificate is posted on the repository. If the certificate applicant refuses to accept the issued certificate after reviewing its contents, the CA shall revoke the certificate.

CAs operating at assurance levels 2, 3 and 4 shall specify the following in the CPS:

(1) The certificate applicant confirms the certificate acceptance or refusal method.

(2) The certificate applicant shall review the certificate fields before deciding whether to accept the certificate.

(3) The certificate applicant refuses to accept the certificate processing method.

The above certificate applicant shall first review the certificate field including but not limited to the subject name before deciding to accept the certificate. Refusal of the certificate processing method by the certificate applicant due to fee collection and return issues shall be determined in accordance with Consumer Protection Act and fair trade principles.

The content of the GRCA self-signed and self-issued certifications must be checked by the NDC before distribution to trusted parties in accordance with the regulations of section 6.1.4.

4.4 Certificate Suspension and Revocation

All CAs except for those CAs operating at a test assurance level should provide certificate revocation services. The CA may decide whether or not to provide certificate suspension services depending on certificate usage and service quality.

CAs shall follow to the following regulations during certificate suspension and revocation:

1. CAs operating at assurance levels 1 or 2 shall provide certificate suspension services at least within the working hours established by government authorities.

2. The certificate suspension and revocation services provided by CAs operating at assurance levels 3 and 4 shall conform the following regulations:

   (1) Provide round-the-clock certificate revocation services.

   (2) Provide round-the-clock certificate suspension services.

CAs providing certificate revocation services shall specify the service provision method, certificate revocation application procedures, application locations and websites in the CPS.

CAs providing certificate suspension services shall also provide certificate resumption services and specify the service provision methods for certificate suspension and resumption, certificate suspension application procedures, certificate resumption application procedures, processing locations and websites in the CPS.

After certificate revocation or suspension, the CA shall list the revoked or suspended certificates in the CARL and CRL and post them in the repository at the next scheduled publication time of the CARL or CRL at the latest. The published certificate status information shall include the revoked and suspended certificates until the certificates expire or use is resumed.

4.4.1 Circumstances under which a Certificate may be Revoked:

(1) The subscriber private key is suspect or known to the

compromised (such as the private key IC card kept by the subscriber is lost).

(2) If the CA private key is proven to be compromised, the certificates issued by private key shall be revoked.

(3) If certificate subscriber information or attributes are changed (such as subscriber name change, subscriber registration number or code change, subscriber identity loss due to dissolution or death) and the certificate subject information recorded on the CA certificate must be changed, the NDC must evaluate whether or not to approve the revocation of the CA certificate.

In addition to certificate revocation under the above circumstances, the subscriber may submit certificate revocation applications based on other reasons within the subscriber certificate validity period.

If the CA or RA has verified that a subscriber has violated the subscriber obligations in the CP or CPS, the CA may revoke the certificates of that subscriber.

If the CA suspects or verifies its own private key has been compromised, all certificates issued with that private key are revoked.

If next higher level CA verifies that the lower level CA has violated the CP and CPS, the certificates of the lower level CA are revoked.

If the CA verifies the cross-certificate CA has violated the CP or its CPS, the cross-certificates of that CA are revoked.

If the NDC decides to revoke the self-signed certificate of the GRCA (such as in the event of GRCA private key compromise), the GRCA self-signed certificate are revoked.

4.4.2 Who Can Request Revocation

If a certificate is revoked due to the circumstances stated in section 4.4.1 or other circumstances, the subscriber or entity in possession of the private key may submit the certificate revocation application to the CA or RA within the certificate validity period.

CAs may revoke subscriber, subordinate CA or cross-certificate CA certificates in accordance with the regulations in section 4.4.1.

4.4.3 Procedure for Revocation

After receiving the certificate revocation application, the CA and RA shall conduct identity verification and authentication on the applicant as stipulated in section 3.4 and CPS regulations. If no errors are found during identity verification and authentication, the CA or RA should, in principle, approve the application unless the CA key has been compromised.

If the certificate revocation application is approved or a decision is made to revoke a certificate, the CA or RA shall follow section 5.2 and CPS regulations. Suitable personnel shall perform the tasks related to certificate revocation. A suitable method shall be used by the CA or RA to notify the subscriber. CAs operating at assurance level 1, 2, 3 or 4 shall specify the method used to notify subscribers after certificate revocation in the CPS.

If the certificate revocation is not approved, the CA or RA shall use a suitable method to notify the subscriber and clearly state the reasons why the revocation was not approved. CAs operating at assurance levels 1, 2, 3 ad 4 shall specify the methods used to notify of the certificate revocation refusal in the CPS.

4.4.4 Certificate Revocation Application Processing Time

CAs shall specify the certificate revocation application processing time in the CPS.

4.4.5 Circumstances under which a Certificate may be Suspended

The related regulations for provision of certificate suspension and resumption services set up by CAs based on requirements shall be specified in the CPS.

4.4.6 Who Can Request Suspension of a Certificate

CAs that provide certificate suspension and resumption services shall specify the criteria of certificate suspension and resumption service applicants in the CPS.

4.4.7 Procedure for Suspension Request

CAs that provide certificate suspension and resumption services shall specify the procedures for certificate suspension and resumption requests in the CPS.

4.4.8 Certificate Suspension Process and Suspension Period

CAs that provide certificate suspension and resumption services shall specify certify suspension and resumption application periods and suspension periods in the CPS.

4.4.9 CARL and CRL Issuance Frequency

The GRCA issues CARLs and subordinate CAs and cross-certificate CAs issue CARLs or CRLs. Before a CARL or CRL is issued, the content

should be checked to verify the accuracy of the information. For example, using software to scan the CARL or CRL to check the accuracy of the information. CARLs and CRLs should be posted regularly. Issuance is necessary even if there is no change in certificate status to ensure that the certificate status information is updated.

The posting of certificate status information shall be completed the next time certificate status informative is updated. The certificate status information of application systems that assist off-line or remote operation is stored in local cache. CA shall strengthen coordination with the repository to reduce the time required between certificate status information generation to repository posting. The CPS should state the primary repository so subscribers can have access to the updated certificate status information in that repository.

When the certificate status information is posted, out-of-date certificate status information shall be removed from the repository it is stored in. CARL and CRL issuance frequency regulations are provided in the Table below.

Table 4-1 CARL and CRL Issuance Frequency

Assurance Level	**CARL Issuance Frequency**	**CRL Issuance Frequency**
Test level	N/A	Not specified
Level 1	N/A	Not specified
Level 2	N/A	At least once every 3 days
Level 3	At least once a day	At least once a day
Level 4	At least once a day	At least once a day

4.4.10 CARL and CRL Checking Requirements

Trusted parties using assurance levels 2, 3 and 4 must check the current CARL and CRL before certificate use to determine the current status of the certificate. The authenticity and integrity of the CARL and CRL must also be checked at this time. The trusted party must consider the risk, responsibilities and effect when individually deciding the certificate revocation information retrieval interval. With regard to related obligations, follow the regulations in section 2.1.4.

4.4.11 On-Line Status Inquiry Service

In addition to providing CARL or CRL services, CAs may choose to provide on-line certificate status inquiry functions to relying parties. Subscribers who use on-line certificate status inquiry do not need to obtain or process CARL or CRL. CAs shall specify whether and how on-line certificate status inquiry services are provided in the CPS.

4.4.12 On-Line Status Inquiry Requirements

Relying parties using assurance level 2, 3 and 4 certificates must use the on-line certificate status inquiry methods to check certificate status if the CARL or CRL is not checked.

4.4.13 Other Forms of Revocation Announcement

Not specified.

4.4.14 Checking Requirements for Other Forms of Revocation Announcements

Not specified

4.4.15 Other Special Requirements in the Event of Key Compromise

Follow the related regulations in sections 4.4.1, 4.4.2 and 4.4.3 in the event of key compromise.

4.5 Security Audit Procedures

CAs operating at test assurance level do not have to possess security audit functions. CAs that issue other assurance level certificates shall possess suitable audit log functions for related security events. Security audit logs shall be automatically generated by system whenever possible. If not possible, records may be made in work logbooks, paper form or other physical form. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs shall be maintained in accordance with the retention period for the archive in section 4.6.2.

4.5.1 Types of Events Recorded

Security audit functions of CA shall include security audits of the certificate administration system and the operation system upon which the certificate administration system depends. The following items should be included in each audit entry (for either automatically or manually

recorded audit events)

(1) Type of event.

(2) Entity that caused the event and operator identity.

(3) Location or site of the event

(4) Time and date of event occurrence.

(5) Result log of CA performing the certificate issuance or revocation procedure (regardless of successful or unsuccessful).

When an event occurs, the CA may decide independently whether to keep the audit log in electronic or physical form. The audit events recorded by CA operating at different assurance levels are stated in the Table below. Since these audit events need to be recorded and responded to, they are called auditable events:

Table 4-2 Regulations for Recording Audit Events

Auditable Events / Assurance Level	**Level 1**	**Level 2**	**Level 3**	**Level 4**
A.1 Security Audit				
A.1.1 Any changes to major audit parameters such as audit frequency, type of audit event and content of new / old parameters.		✓	✓	✓
A.1.2 Any attempt to delete or modify the audit logs.		✓	✓	✓
A.2 Identification and Authorization				
A.2.1 Successful and unsuccessful attempts to assume		✓	✓	✓

Auditable Events / Assurance Level	Level 1	Level 2	Level 3	Level 4
a role				
A.2.2 Change in the number of maximum identification or authorization attempts		✓	✓	✓
A.2.3 Maximum number of unsuccessful identification or authorization attempts during subscriber login		✓	✓	✓
A.2.4 Administrator unlocks an account that has been locked as a result of unsuccessful identification or authorization attempts		✓	✓	✓
A.2.5 Administrator changes the type of authenticator ranging from passwords to biometrics		✓	✓	✓
A.3 Key Generation				
A.3.1 Times when a key is generated by a CA (not including keys that have only been used once or limited to single use)	✓	✓	✓	✓
A.4 Private Key Loading and Storage				
A.4.1 Loading of private keys to system components	✓	✓	✓	✓
A.4.2 Any access to private keys kept by the CA for key restoration work	✓	✓	✓	✓
A.5. Additions, Deletions and Storage to the Relying Party's Public Key				
A.5.1 Any changes to the	✓	✓	✓	✓

Auditable Events / Assurance Level	Level 1	Level 2	Level 3	Level 4
relying party's public key including additions and deletions				
A.6. Private Key Export				
A.6.1 Private key export (not including keys that have only been used once or limited to single use)	✓	✓	✓	✓
A.7. Certificate Registration				
A.7.1 Any certificate registration request processes	✓	✓	✓	✓
A.8. Certificate Revocation				
A.8.1 Any certificate revocation request processes		✓	✓	✓
A.9. Certificate Status Change Approval				
A.9.1 Approval or denial of a certificate status change request		✓	✓	✓
A.10. GRCA or Subordinate CA Configuration Setting				
A.10.1 Any configuration setting changes related to CA security		✓	✓	✓
A.11. Account Administration				
A.11.1 Addition or deletion of roles and subscribers	✓	✓	✓	✓
A.11.2 The access authorization of a subscriber account or role is modified	✓	✓	✓	✓
A.12. Certificate formal profile management				

Auditable Events / Assurance Level	Level 1	Level 2	Level 3	Level 4
A.12.1 Any certificate profile changes	✓	✓	✓	✓
A.13. CARL / CRL format profile management				
A.13.1 Any CARL / CRL format profile modifications		✓	✓	✓
A.14. Miscellaneous				
A.14.1 Installation of operating system		✓	✓	✓
A.14.2 Installation of CA system		✓	✓	✓
A.14.3 Installation of hardware cryptographic modules			✓	✓
A.14.4 Removal of hardware cryptographic modules			✓	✓
A.14.5 Destruction of hardware cryptographic modules		✓	✓	✓
A.14.6 System activation		✓	✓	✓
A.14.7 Login attempts to CA apps		✓	✓	✓
A.14.8 Receipt of hardware / software			✓	✓
A.14.9 Attempts to create passwords		✓	✓	✓
A.14.10 Attempts to modify passwords		✓	✓	✓
A.14.11 Backing up the CA internal database		✓	✓	✓

Auditable Events / Assurance Level	Level 1	Level 2	Level 3	Level 4
A.14.12 Restoration of the CA internal database		✓	✓	✓
A.14.13 File manipulation (e.g. creation, naming and transfer)			✓	✓
A.14.14 Posting of any information to a repository			✓	✓
A.14.15 Access to the CA internal database			✓	✓
A.14.16 All certificate compromise complaints		✓	✓	✓
A.14.17 Certificate loading symbols			✓	✓
A.14.18 Token delivery			✓	✓
A.14.19 Token zeroing		✓	✓	✓
A.14.20 CA rekey	✓	✓	✓	✓
A.15 Configuration Changes to the CA Server				
A.15.1 Hardware		✓	✓	✓
A.15.2 Software		✓	✓	✓
A.15.3 Operating system		✓	✓	✓
A.15.4 Patches		✓	✓	✓
A.15.5 Security profiles			✓	✓
A.16 Physical Access and Site Security				
A.16.1 Physical access to the CA server room			✓	✓
A.16.2 Access to CA servers			✓	✓

Auditable Events / Assurance Level	Level 1	Level 2	Level 3	Level 4
A.16.3 Known or suspected violations of physical security regulations		✓	✓	✓
A.17 Abnormalities				
A.17.1 Software error		✓	✓	✓
A.17.2 Software integrity check failure		✓	✓	✓
A.17.3 Receipt of improper messages			✓	✓
A.17.4 Misrouted messages			✓	✓
A.17.5 Network attack (suspected or actual))		✓	✓	✓
A.17.6 Equipment failure	✓	✓	✓	✓
A.17.7 Improper power supply			✓	✓
A.17.8 UPS failure			✓	✓
A.17.9 Clear or significant network service or access failures			✓	✓
A.17.10 Violations of Certificate Policy	✓	✓	✓	✓
A.17.11Violations of the Certification Practice Statement	✓	✓	✓	✓
A.17.12 Resetting of the operating system clock		✓	✓	✓

4.5.2 Frequency of Record File Processing

Audit logs shall be reviewed as specified in the Table below and explanations added to the major events in the audit reports. Review work

shall include verifying tampering of records, examination of all log items and investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

Table 4-3 Frequency of Record File Processing

Assurance Level	Frequency of Record File Processing
Test level	Not specified
Level 1	Not specified
Level 2	Not specified
Level 3	At least once every two months Major security audit logs are reviewed by the CA after the previous audit review and further investigations shall be made of any possible malicious activities.
Level 4	At least once a month Major security audit logs are reviewed by the CA after the previous audit review and further investigations shall be made of any possible malicious activities.

4.5.3 Retention Period for Security Audit Logs

The retention periods for security audit logs of CAs operating under the assurance level 1 or test level are not specified.

The retention period for security audit logs for CAs operating under assurance level 2, 3 or 4 is at least two months. The log retention administration system regulations in sections 4.5.4, 4.5.5, 4.5.6 and 4.6 shall also be followed.

When the retention period for audit logs ends, the information requiring removal is removed by audit personnel. Other personnel may not perform this task.

4.5.4 Protection of Security Audit Logs

Protection for security audit files of CAs operating under the assurance level 1 or test level are not specified.

The electronic audit log system for CAs operating under assurance level 2, 3 or 4 must include protection systems. Manually recorded audit information shall also be protected to prevent unauthorized reading, modification or deletion.

4.5.5 Audit Log Backup Procedures

Table 4-4 Audit Log Backup Procedure

Assurance Level	Audit Log Backup Procedure
Test level	Not specified
Level 1	
Level 2	Backup of audit log files must be done at least once a month.
Level 3	
Level 4	Backup of audit log files must be done at least once a month. Off-site backup must be done at least once a month. Related off-site backup procedures shall be specified in the CPS.

4.5.6 Security Audit System

The security audit system can be inside or outside the certificate administration system. Audit procedures shall be activated upon

certificate administration system startup and end only when the certificate administration system is shut down.

If the automatic audit system is not operating normally and the integrity of the system and the information protected by the system is at high risk, it shall be determined whether the certificate administration system should stop operation until the problem is remedied and service may resume.

4.5.7 Notification of an Event-Causing Subject

When an event is recorded, the audit system does not need to notify the entity which caused the recorded event.

4.5.8 Vulnerability Assessments

CAs operating under assurance levels 3 and 4 shall conduct routine security control vulnerability assessments. There is no vulnerability assessment requirement for CAs operating under test level or assurance levels 1 and 2.

4.6 Record Archival

4.6.1 Types of Events Archived

The following records shall be archived (not required for CAs operating under the test assurance level) based upon the security requirements of various assurance levels.

Table 4-5 Record Archival

Archived Information / Assurance Level	Level 1	Level 2	Level 3	Level 4

Archived Information / Assurance Level	Level 1	Level 2	Level 3	Level 4
CA accreditation process and result information (presumed use)	✓	✓	✓	✓
Certification Practice Statement	✓	✓	✓	✓
Major contracts	✓	✓	✓	✓
System and equipment configuration	✓	✓	✓	✓
Modifications and updates to systems or configurations	✓	✓	✓	✓
Certificate request data	✓	✓	✓	✓
Revocation request data		✓	✓	✓
Subscriber identity data specified in section 3.1.9		✓	✓	✓
Document receipt and certificate acceptance		✓	✓	✓
Token activation log		✓	✓	✓
Issued or published certificates	✓	✓	✓	✓
CA rekey records	✓	✓	✓	✓
Issued and/or published CARLs / CRLs		✓	✓	✓
Audit logs	✓	✓	✓	✓
Other information or applications used to verify or substantiate archive contents		✓	✓	✓
Document requests of audit personnel		✓	✓	✓

4.6.2 Retention Period for Archives

The minimum retention period for archive information is as follows:

Table 4-6 Retention Periods for Archives

Assurance Level	Minimum Retention Period
Test level	Not specified
Level 1	3 years
Level 2	5 years
Level 3	10 years
Level 4	20 years

If the above retention period cannot be reached with the storage media used, a system to regularly transfer archive information to new storage media systems must be established. The applications used to archive information must also be checked at regularly scheduled intervals (the length of interval shall be determined by the CA competent authority).

The handling method for archived files upon expiry of the retention period shall be specified in the CPS.

4.6.3 Protection of Archive

There is no archive protection requirement for CAs operating under test level or assurance level 1.

For CAs operating under assurance levels 2, 3 and 4, the archive information must be stored at a location outside the CA and suitable

protection provided. The protection level may not be lower than the protection level of the CA premises.

4.6.4 Archive Backup Procedures

Not specified.

4.6.5 Requirements for Time-Stamping of Records

Not specified.

4.6.6 Archive Collection System

Not specified.

4.6.7 Procedures to Obtain and Verify Archive Information

Procedures for CA establishing, checking, formatting, packeting, transfer and storage of archive information shall be specified in the CPS.

4.7 Key Changeover

4.7.1 CA Key Changeover

CA private keys must be routine changed in accordance with section 6.3.2. The new private keys are used in place of the old private key to issue certificates and all entities relying on the certificates shall be notified at an appropriate time. The old private key still must respond to CRL and on-line certificate status requests to maintain and protect all subscriber certificates issued with the old private key until expiry.

If use of a private key stops due to the revocation of the CA's own certificate, then the key pair must be replaced.

The key pairs used to issue certificates to subordinate CAs must be replaced by the GRCA three months before certificate expiry at the latest

and one new self-signed certificate and one self-signed certificate cross-issued each with the new and old private keys are issued. The procedure for issuance of these three new certificates is specified in section 4.2.

The key pairs used to issue certificates must be replaced by subordinate CAs two months before certificate expiry at the latest. The subordinate CA shall apply for a new certificate from the upper level CA after the key pair is replaced in accordance with section 4.1.

4.7.2 Subscriber Key Changeover

Subscribers must follow the regulations in section 6.3.2 for routine private key changeovers.

After the subscriber certificate is revoked, use of its private key is stopped. After key pair replacement, the subscriber may apply for a new certificate with a CA or RA as specified in section 4.1.

For subscribers with assurance levels 2, 3 and 4, the key pair must be replaced if the certificate has not been revoked within one month prior to certificate expiry at the latest. A new certificate may be applied for with a CA or RA as specified in section 4.1.

4.8 Compromise and Disaster Recovery

For disaster recovery work, the CA shall assign priority to repository restoration so certificate status information can be provided normally.

4.8.1 Restoration Procedure for Damaged or Corrupted Computer Resources, Software or Data

To achieve the goal of sustainable operations, CAs shall make sure

to implement various backup measures in accordance with CP and CPS to reduce damage to computer resources, software and information to a minimum and quickly restore certificate issuance and administration work.

CAs operating under assurance levels 3 and 4 shall hold computer resource, software and information damage recovery drills at least once each year.

4.8.2 Restoration of Revoked CA Signature Keys

CAs operating under assurance levels 2, 3 and 4 shall specify the restoration procedure for revoked CA signature keys in CPS or related documents to quickly restore certificate issuance and administration functions.

CAs operating under assurance levels 3 and 4 shall hold restoration drills for revoked CA signature key certificates at least once per year.

4.8.3 Restoration of Compromised CA Signature Keys

CAs operating under assurance levels 2, 3 and 4 shall specify the restoration procedures in the event of CA signature key compromise in the CPS or related documents to quickly restore certificate issuance and administration functions.

CAs operating under assurance levels 3 and 4 shall hold CA signature key compromise drills at least once per year.

4.8.4 Recovery of CA Security Facilities Following a Disaster

CAs operating under assurance levels 2, 3 and 4 shall specify the

recovery steps for CA security facilities following a natural or other type of disaster in the CPS or related documents.

CAs operating under assurance levels 3 and 4 shall hold post-disaster recovery plan drills at least once a year.

4.9 Termination of CA Services

In the event of termination of CA services, the related provisions of the Electronic Signatures Act shall apply.

5. Non-Technical Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

There are no requirements for CAs operating under test level or assurance level 1. The site location and construction requirements for CAs operating under assurance level 2 or above must comply with facility standards for the housing of highly important and sensitive information and other physical security protection system including access control, security, intrusion detection and video monitoring to prevent unauthorized access to related CA equipment.

5.1.2 Physical Access

There are no requirements for CAs operating under test level or assurance level 1. Physical access control must be implemented for CA equipment after cryptographic module installation and activation for CAs operating under assurance level 2 or above to prevent unauthorized access. Even if an cryptographic modules is not installed or activated, physical access control shall be implemented for related CA equipment to reduce the risk of unauthorized activation or damage to the equipment.

The physical access control requirements for each assurance level is as follows:

The physical access control requirements for CAs operating at assurance levels 1 and 2 are:

(1) Protect against unauthorized intrusion.

(2) Ensure that portable storage media containing sensitive information and documents are kept in a safe location.

The physical access control requirements for CAs operating at assurance levels 3 and 4 are:

(1) Set up a round-the-clock manual or electronic monitoring equipment to prevent unauthorized intrusion.

(2) Routine maintenance and examination access log files.

(3) At least two people must jointly conduct physical access control of computer systems and password modules.

Since the GRCA must issue certificates at all assurance levels, the security system for the equipment environment must be in compliance with assurance level 4 physical access control regulations. There are no requirements for physical access control of CAs operating at test level or assurance level 1 but they must be specified in the CPS.

The following checks must be done when personnel leave the CA facility to prevent unauthorized personnel from accessing the facility.

(1) Appropriate security is provided for security cabinets.

(2) Physical security systems (such as door locks and entry and exit access) are working properly.

5.1.3 Electrical Power and Air Conditioning

There are no requirements for CAs operating under test level or assurance level 1. There must be sufficient electrical power and air conditioning backup equipment to support CA related systems which can

operate or shut down normally when affected by external factors for CAs operating under assurance level 2 or above. UPS must also be provided which can provide at least 6 hours of backup power for repository backup data (including issued certificates and CRL).

5.1.4 Flood Prevention and Protection

The CA site must be in location that is safe from flood damage.

5.1.5 Fire Prevention and Protection

There are no requirements for CAs operating under test level or assurance level 1. The CA facilities for CAs operating under assurance level 2 or above must have automatic fire detection and alarm functions and systems which include automatic fire extinguishing equipment. Manual switches should be placed on major entrances and exits to allow manual operation by on-site personnel during emergencies.

5.1.6 Media Storage

There are no requirements for CAs operating under test level or assurance level 1. Protective system-related storage media for CAs operating under assurance level 2 or above must be safe from accidental damage (water, fire and electromagnetic fields).

5.1.7 Waste Disposal

Not specified.

5.1.8 Off-Site Backup

There are no requirements for CAs operating under test level or

assurance level 1. Related CA systems for CAs operating under assurance level 2 or above must be regularly backed up offsite. A full backup of data must be done at least once per week. Other schedule cycles must be specified in the CPS.

Off-site backup locations must be at least 30 kilometers away from the CA host. The backup content must at least include data and system programs. When a malfunction occurs, normal operation capability must be restored. Off-site backup systems shall have an equivalent security level of the CA system.

5.2 Procedural Controls

5.2.1 Trusted Roles

CAs must assign trusted roles responsible for performance of related tasks to serve as a trust anchor for the CA. Failure of achieve security goals due to accidents or human oversight may compromise CA objectivity. The following two methods may be used by CAs to enhance security:

(1) Ensure that the personnel serving as trusted roles receive adequate training and are completely trustworthy.

(2) Properly distinguish each type of task. Assign the same task to more than one person to prevent individuals from engaging in malicious activities.

The tasks performed by trusted roles are as follows:

(1) Administrator: Installation, configuration and maintenance of related CA systems. Creation and maintenance of system

subscriber accounts. Setting or audit parameters and generation of component keys.

(2) Officer: Issuing and revoking certificates.

(3) Auditor: Checking and maintenance of audit logs.

(4) Operator: System backup and troubleshooting.

5.2.1.1 Administrator

The administrator is primarily responsible for:

(1) Installation, configuration and maintenance of related CA systems.

(2) Creation and maintenance of system subscriber accounts.

(3) Setting of audit parameters.

(4) Generation and backup of CA keys.

5.2.1.2 Officer

The officer is primarily responsible for:

(1) Logging in new subscribers and receipt of certificate issuance applications.

(2) Check subscriber identity and accuracy of certificate information.

(3) Review and perform certificate issuance.

(4) Certificate revocation application receipt, review and processing.

5.2.1.3 Auditor

The auditor is primarily responsible for:

(1) Checking, maintenance and archiving of audit records.

(2) Perform or supervise internal audits to ensure the CA is operating in compliance with CPS regulations.

5.2.1.4 Operator

The operator is primarily responsible for:

(1) System physical security controls (such as facility access controls, fire prevention, water protection and air conditioning systems).

(2) Daily operation and maintenance of system equipment.

(3) System backup and recovery.

(4) Update of storage media.

(5) System hardware and software updates.

(6) Network and website maintenance: Set up system for security, virus protection system and network security event detection and reporting.

5.2.2 Roles Assignment

CA role assignment is performed as follows:

Table 5-1 Role Assignment

Assurance Level	Role Assignment
Test level	Not specified
Level 1	Not specified
Level 2	For the four trusted roles defined in section 5.2.1, one person is allowed to assume more than one role but may not concurrently assume the operator and administrator role.
Level 3	For the four trusted roles defined in section 5.2.1, one person is allowed to assume more than one role but may not concurrently assume the operator and administrator role.
Level 4	For the four trusted roles defined in section 5.2.1, personnel and role assignment must follow the following regulations: (1) The administrator, officer and auditor roles may not be held concurrently by one person but the controlled role may be concurrently held. (2) The self-auditing function may not be performed by any one role

5.2.3 Number of Persons Required Per Task

In order to achieve optimal security for CA equipment and maintenance, role assignment for personnel must be done in accordance with section 5.2.2. The number of persons required for each task must be specified in the CPS.

5.2.4 Identification and Authentication of Each Role

There is no requirement for CAs operating under test level or assurance level 1. For CAs operating under assurance level 2 or above, Identification and authentication of personnel must be done before role performance and task assignment of related personnel.

5.3 Personnel Controls

CAs must maintain control over all personnel engaged in CA or RA operation. Security controls for work assignment of personnel must comply with the following regulations:

(1) Work assignments must be in written form.

(2) Work qualifications are based on legal or contractual requirements.

(3) Acceptance of related work training.

(4) Sensitive CA security information and subscriber information as defined under the law or in contractual requirements shall not be disclosed.

(5) Work assignments shall conform to conflict of interest avoidance principles.

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

CAs must perform identification checks on personnel. Necessary qualifications are loyalty, reliability, integrity and ROC citizenship. Personnel qualifications, selection, supervision and auditing regulations must be specified in the CPS.

5.3.2 Background Check Procedures

Background check procedures must be specified in the CPS.

5.3.3 Training Requirements

Relevant CA personnel shall receive the following instruction and training:

(1) CA and RA security certification system.

(2) PKI software used by the CA system.

(3) Work responsibilities for PKI establishment.

(4) Disaster recovery and sustainable operation procedures.

5.3.4 Retraining Requirements and Frequency

For hardware or software upgrades, work procedure changes or equipment replacement, CAs will schedule retraining for relevant personnel and record the training status to ensure that related work procedure and regulatory changes are understood.

New personnel must also receive relevant training. CAs must review the training status of relevant personnel each year.

5.3.5 Job Rotation Frequency and Sequence

Not specified

5.3.6 Sanctions for Unauthorized Actions

CAs shall take appropriate administrative actions to protect against authorized access of information by personnel and publish related regulations in the CPS. The CA must take appropriate administrative and disciplinary action for personnel who violate the CP or CPS.

Appropriate administrative and disciplinary action shall be taken for

personnel in charge of the GRCA and repository server who violate the CP, CPS and other procedures published by the GRCA.

5.3.7 Requirements for Contracted Personnel

Contracted personnel performing related CA jobs must follow related regulations in the CA CPS.

5.3.8 Documentation Supplied to Personnel

CAs must provide the CP, the CPS and other related documents concerning rules, policies and contracts to related CA and RA personnel.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The cryptographic modules used by CAs to issue certificates must have a NDC assurance level equivalent to the key pairs generated by the cryptographic modules.

It should be computationally infeasible to compute a random number sequence with an equivalent length and randomness of the random numbers used in the key generation process even if sufficient information and equipment are provided.

The protection used for private keys stored in the cryptographic module except for key changeovers stated in section 4.7.1 or key backup recover and cryptographic module changeover reasons shall not allow disclosure of the content stored in the hardware cryptographic module. For private keys generated inside the cryptographic module, the key shall always be kept in the cryptographic module or encrypted and stored in the host. If the private key is generated outside the cryptographic module, the key shall be entered into the cryptographic module while not outside the key generation environment. It shall be guaranteed that personnel may not use any method to undetectably obtain generated private keys in the environment. After the private key is stored in the cryptographic module, the key shall immediately deleted from the key generation environment.

CAs shall adopt appropriate measures to ensure that the subscriber public key is the only PKI field under the administration of the CA.

6.1.2 Secure Delivery of Private Keys to Subscribers

Delivery of the private key is not required if the private key is generated and stored in the cryptographic module.

If a token held by an entity (such as a subscriber or IC card issuance center) is used to directly generate keys or keys are generated by another key generator and then sent to the entity's token, the entity is deemed to be in possession the private key when a private key is generated and accepted by the entity. If the above entity is not certificate subject on the subject application, the private keys shall be delivered to the certificate subject in a secure and auditable manner to complete the private key transfer.

If a key stored in hardware is delivered to the subscriber at any assurance level, delivery of the correct token and its activation data to the subscriber should be verified. CAs must keep one copy of the subscriber token receipt record. When using any systems including secret sharing (i.e. password or PIN number), the system must ensure that only the applicant and GRCA or subordinate CA are only ones that have a secret entity.

If the private key is generated by CA, RA or trusted third party, the cryptographic module must be securely transmitted to the subscriber. The subscriber receipt of the private key must be verified. Cryptographic module storage location and status tracking records must kept properly at least until it is verified that the subscriber has received the cryptographic module.

Under any circumstances, persons other than the subscriber may not access or control the signature private key. Any entity who generates signature private keys on behalf of the subscriber may not keep the backup of that key.

6.1.3 Secure Delivery of Public Keys to the CA

The methods that are used by the subscriber to send the public key to CA when the CA does identity authentication for the subscriber include:

(1) The RA sends out an electronic message for the certificate application.

(2) The CA or RA must pass through auditable security channels to obtain the subscriber's public key when the key is generated by a third party.

(3) Completed through other secure electronic systems.

(4) Completed through secure non-electronic means. These methods include (but are not limited to) floppy disk (or other storage media) sent through registered mail or express mail.

6.1.4 Secure Delivery of CA Public Keys to Relying Parties

The GRCA public key must be accessible at all times. The subordinate CA must use a reliable method to deliver the GRCA self-signed certificate or public key to the subscriber. Reliable certificate transmission methods including the following:

(1) The CA uses a token to store the GRCA self-signed certificate or public key for securely transmission to the relying party.

(2) Use of out-of-band channels to transmit the GRCA self-signed certificate or public key.

(3) Use of out-of-band channels to transmit the hash value or fingerprint for the GRCA self-signed certificate or public key to the subscriber for comparison (in-band hash tag or fingerprint together with the certificate are not considered to be authorized secure channels).

(4) Download the GRCA certificate or public key from a website with the equivalent or higher assurance level.

(5) Other methods approved by the NDC.

The above out-of-band channels shall be specified in the GRCA CPS.

The self-signed certificates issued by the GRCA must be posted in the repository. The new and old certificates of subordinate CAs issued by the GRCA must be posted in the CA repository.

6.1.5 Key Sizes

For certificates which expire prior to January 1, 2031, 2048-bit RSA keys or other types of keys with an equivalent security strength (such as 224-bit ECC) shall be used. For certificates which expire after December 31, 2030, 3072-bit RSA keys or other types with an equivalent security strength (such as 256-bit ECC) shall be used.

CAs shall completely change over to SHA-2 algorithm to issue certificates and respond to certificate, CRL and on-line status requests by December 31, 2016 at the latest.

Table 6-1 Key Sizes

Assurance Level	**Symmetric Key**	**Public Key**
Test level	Must at least have 3-DES (3 keys) or another type of key with an equivalent security strength (such as 128-bit AES	Must at least use a 1024-bit RSA key or another type of key with an equivalent security strength (such as a 161-bit ECC)
Level 1		
Level 2		
Level 3		

Assurance Level	Symmetric Key	Public Key
Level 4	128)	Must at least use a 2048-bit RSA key or another type of key with an equivalent security strength (such as a 224-bit ECC).

6.1.6 Public Key Parameters Generation

For RSA algorithms, the public key parameter is null. For other algorithms, the public key parameter is based on related international standards.

6.1.7 Key Parameter Quality Checking

For RSA algorithms, key parameter quality checking does not need to be done but primality testing is necessary. CAs shall specify the related testing that needs to be done in the CPS.

For other algorithms, testing shall be based on related international standards which should include primality testing.

6.1.8 Key Generation by Software / Hardware

Any keys used to generate random numbers must be approved by the NDC. The related regulations for the hardware and software used to generate subscriber random numbers, key pairs and symmetric keys are listed in the Table below:

Table 6-2 Key Generation System

Assurance	Key Generation

Level	System
Test level	Software or hardware
Level 1	Software or hardware
Level 2	Software or hardware
Level 3	Software or hardware
Level 4	Only limited to hardware

6.1.9 Key Usage Purposes

Public keys certified by CAs must state the key usage (signature or encryption) in the keyUsage extension field of the X.509 certificate. For certificates used for digital signatures (including authentication), the digitalSignature field must have a setting. For certificates used for encryption, the keyEncipherment or dataEncipherment fields must have a setting. The CA own certificates must have two key usage field settings: cRLSign and keyCertSign.

Test level and assurance level 1, 2 and 3 certificates can use a single key concurrently for encryption and signatures to support some old versions of secure multipurpose internet mail extensions (S/MIME) application software. Unless specified otherwise in the CP, this type of dual-use certificate must be generated and administered in accordance with signature usage certificate regulations and non-repudiation key usage settings are not allowed. Also, it may not be used for signature verification of important information. For subordinate CAs at any assurance level, two types of key pair certificates should be issued to subscribers: one for information encryption use and one for digital signature and identity verification use.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

The NDC determines the related standards for cryptographic module certification. The security requirements for cryptographic modules are determined in reference with FIPS 140 series or other standards with an equivalent security strength. Related standards are announced by the NDC. Cryptographic modules must undergo equivalent security level certification in accordance with related certification standards. The NDC shall examine the related technical documentation for the cryptographic modules used by the GRCA.

The minimum requirements for cryptographic modules are provided in the Table below. A higher security level may be used. The levels provided in the Table below follow FIPS 140 series definitions.

Table 6-3 Cryptographic Module Standard

Assurance Level	GRCA	**Subordinate CA**	**RA**	**Subscriber**
Test level	N/A	Not specified	Not specified	Not specified
Level 1	N/A	Level 1 (hardware or software)	Level 1 (hardware or software)	Not specified
Level 2	N/A	Level 2 (hardware or software)	Level 1 (hardware or software)	Level 1 (hardware or software)
Level 3	N/A	Level 2 (hardware)	Level 2 (hardware)	Level 1 (hardware or software)
Level 4	Level 3 (hardware)	Level 3 (hardware)	Level 2 (hardware)	Level 2 (hardware)

6.2.2 Key Splitting Multi-Person Control

The multi-person control procedure in Chapter 5 must be followed for the signature-use private keys of CAs that issue assurance level 3 or 4

certificates.

6.2.3 Private Key Escrow

Signature-use private keys shall not be escrowed.

6.2.4 Private Key Backup

6.2.4.1 CA Signature Private Key Backup

For CAs operating under assurance levels 3 and 4, the backup of their signature-use private keys shall be performed using multi-person control procedures and stored at the backup site. The key backup procedure must be specified in the CPS.

6.2.4.2 Subscriber Signature Private Key Backup

Backup or copying of subscriber signature private keys is allowed for assurance level 1, 2 and 3 certificates but the subscriber must have control.

For assurance level 4 certificates, backup and copying of subscriber signature is not allowed.

6.2.5 Private Key Archiving

Signature private keys may not be archived.

6.2.6 Private Key Importation into Cryptographic Module

Follow the regulations in section 6.1.1.

6.2.7 Methods for Activating Private Keys

Identity authentication of activator must be done when the private key stored in the cryptographic module is activated. Acceptable authentication methods include (but not limited to) pass-phrase, personal tokens, PIN or biometrics but the input activation data must be protected

from disclosure (may not be displayed).

Activated private keys should not be left unattended and unauthorized access should not be allowed.

6.2.8 Methods for Deactivating Private Keys

Cryptographic modules must stop operation when not required for use. After the manual logout procedure or a period of non-operation (length of time specified in the CPS), operation is automatically stopped. The hardware cryptographic module that are no longer being used must be separated from the host and stored in a secure place.

6.2.9 Methods for Destroying Private Keys

When the signature private key or its backup is no longer needed or the certificate has expired or has been revoked, the signature private key must be destroyed. For software cryptographic modules, the data must be rewritten on the memory or storage media originally occupied by the signature private key. For hardware cryptographic modules, zeroization must be performed, but physically destruction is not required.

6.3 Other Aspects of Key Pair Administration for Subscribers

It is technically feasible to use a single key pair for signature and encryption but issuance of two key pair certificates to the subscriber regardless what assurance level is used is recommended unless the old version application system complies with section 6.1.9. One key pair certificate is for data encryption and the other is for digital signature and identity authentication.

The escrow, archiving and backup of private keys used by the subscriber for signature and identification authentication is absolutely

prohibited. The CA to which the subscriber is subordinate may request the escrow, archiving or backup of encryption private keys used for job duties.

6.3.1 Public Key Archiving

Public key archiving may not be performed subsequently after certificate archiving.

6.3.2 Usage Periods for Public and Private Keys

6.3.2.1 Usage Periods for CA Public and Private Keys

CA public and private keys have different key strengths and assurance levels and their usage periods are as follows:

(1) For 4096 bit RSA or other types of public key pairs with an equivalent security strength (such as 300 bit ECC), the maximum validity period for public and private keys is 30 years. However, the usage period for private keys used for certificate issuance may not exceed 15 years.

(2) For 3072 bit RSA or other types of public key pairs with an equivalent security strength (such as 256 bit ECC), the maximum validity period for public and private keys is 30 years. However, the usage period for private keys used for certificate issuance may not exceed 15 years.

(3) For 2048 bit RSA or other types of public key pairs with an equivalent security strength (such as 224 bit ECC), the maximum validity period for public and private keys is 20 years. However, the usage period for private keys used for certificate issuance may not exceed 10 years.

(4) For 1024 bit RSA or other types of public key pairs with an equivalent security strength (such as 161 bit ECC), the maximum

validity period for public and private keys is 10 years. However, the usage period for private keys used for certification issuance may not exceed 5 years.

For signature private key used by the GRCA to sign certificates, the key lifespan may not exceed half of the lifespan of the self-signed certificate. The lifespan of its self-signed certificates may not exceed 30 years.

The total of the certificate lifespan of certificates issued by the GRCA to subordinate CA plus the lifespan of signature private key used by the GRCA to sign certificates may not exceed the lifespan of GRCA self-signed certificates.

The lifespan of the two self-issued certificate issued by GRCA in response to signature key changeover may not exceed the lifespan of the old certificates.

6.3.2.2 Usage Periods for Subscriber Public and Private Keys

The usage periods for subscriber keys are determined based on key size. The following regulations were established regarding their renewal:

(1) For keys with a security strength equivalent to 1025 bit RSA, the private key usage period shall be a maximum of 5 years in principle. After the CA evaluates legality, convenience, security and cost effect requirements, the renewal period for 1024 bit RSA keys may not exceed 3 years and the usage period after renewal may not extended beyond December 31, 2018.

(2) For keys with a security strength equivalent to 2048 bit RSA 2048, the private key usage period shall be a maximum of 10 years.

In accordance with key security strength requirements, CAs must stop issuance of certificates with a security strength equivalent to 1024 bit RSA by December 31, 2010 at the latest but the certificates that were issued prior to this date may be used until their expiry date.

6.4 Activation Data Protection

6.4.1 Activation Data Generation

The CA or subscriber private keys used to decrypt activation data and other related access control systems must be given adequate protection. For CAs operating under assurance levels 1, 2 or 3, the activation data is selected independently by subscriber. CAs operating under assurance level 4 must be able to receive biometric data from the subscriber or use the strengthened security systems of the cryptographic module. If passwords are used as activation data, password generation must comply with information security management guidelines and regulations of the Executive Yuan and other subordinate agencies. Appropriate secure channels must be used if the activation data needs to be transmitted.

6.4.2 Data Activation Protection

Private keys used for decrypting activation data must combine the password with the access control security system to protect against disclosure. The activation data may be stored in biometric or memory form. If records need to be kept, a cryptographic module with a security level equivalent to the data must be used to ensure its security. If the number of failed login attempts exceeds the maximum setting in CPS, the protection system must immediately freeze the account number and terminate the application.

6.4.3 Other Data Activation Rules

Not specified

6.5 Computer Hardware and Software Security Controls

6.5.1 Technical Requirements for the Security of Specific Computers

CAs operating under assurance levels 3 and 4 and their related auxiliary systems must provide the following functions by means of the operating system or jointly through the operating system, software and physical protection measures. The functions are:

(1) Identity authenticated login
(2) Self-discretionary access controls.
(3) Security audit capability.
(4) Access control restrictions for each certificate services and PKI trusted roles.
(5) Identify and authenticate PKI trusted roles and related identities.
(6) Ensure security of communications and databases with encryption technology.
(7) Provide secure and reliable channels for PKI trusted roles and related identities.
(8) Offer procedure integrity and security control protections.

CA equipment must be built upon an operation platform which has undergone a security evaluation and CA related systems (hardware, software, and operating systems) must operate through configurations which have undergone a security evaluation.

6.5.2 Computer Security Rating

Not specified

6.6 Lifespan Technical Controls

6.6.1 System Development Controls

CA system development control measures are as follows:

Table 6-4 System Development Control Measures

Assurance Level	System Development Control Measures
Test level	Not specified
Level 1	Not specified
Level 2 Level 3 Level 4	(1) The software used by CAs must be developed with good software engineering development methods such as the capability maturity model (CMM). (2) CA hardware and software must be designed for dedicated use and other non-related applications may be installed or operated (including hardware devices, network connection or software components). (3) Action must be taken to prevent the installation of malicious software in CA equipment. Only components authorized by the security policy may be used for CA operations. ◦ (4) RA hardware and software must checked for malicious programs during initial use and

	routinely scanned afterwards.

6.6.2 Security Management Controls

Table 6-5 Security Management Control Regulations

Assurance Level	**Security Management Control Measures**
Test level	Must record and control related CA system configurations and any modifications or function upgrades. Must be able to detect unauthorized modifications of CA software and system configurations. Must check if the supplier has provided the correct, unmodified version during initial installation of CA software.
Level 1	
Level 2	
Level 3	
Level 4	Must record and control related CA system configurations and any modifications or function upgrades. Must be able to detect unauthorized modifications of CA software and system configurations. Must check if the supplier has provided the correct, unmodified version during initial installation of CA software. CAs must check the integrity of CA software at least once per month.

6.6.3 Lifespan Security Ratings

Not specified

6.7 Network Security Controls

The GRCA host and the internal repository may not have any external network connections. The GRCA external repository is connected to the Internet to provide uninterrupted service (except when maintenance or backup is required). Information in the internal repository is transferred manually from the internal repository to the external repository and all information (certificates and CARLs) are protected by electronic signature. The external repository prevents denial of service and intrusion attacks with system patch file updates, system vulnerability scanning, intrusion detection systems, firewall systems and filtering routers.

6.8 Cryptographic Module Security Controls

Follow the regulations in sections 6.1 and 6.2.

7 Profile

7.1 Certificate Format Profile

7.1.1 Version Number

CAs must issue version X.509 v3 certificates. The version number field is 2.

7.1.2 Certificate Extension Fields

Regulations concerning the use, processing method and field setting of certificate extensions are specified in the certificate formal profile. The certificate infrastructure is adequately controlled through the certificate format profile to provide sufficient flexibility to comply with the requests of various CAs and communities.

Certificates issued by the GRCA must follow GPKI certificate and CRL format profile regulations. If the certificates issued by subordinate CAs are assurance level 3, certificate and CRL format profile regulations must be followed. If the certificates are level 1 or 2, RFC 5280 regulations must be followed. If self-defined extension fields must be used, it should be stated in the CPS. For critical self-defined extension fields, application services must be able to achieve interoperability with its community.

7.1.3 Algorithm Object Identifiers

The following algorithm OIDs must be used for the signatures of issued certificates:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}

The following OID must be used with the subject key algorithm for issued certificates:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name Forms

The subject and two issuer fields of the certificate must comply with X.500 distinguished name) and the attribute type of the name must comply with RFC 5280 regulations.

7.1.5 Name Constraints

Not specified

7.1.6 Certificate Policy Object Identifier

The certificate policy OID must be used for issued certificates and the certificate policy OID must also conform to the certificate assurance level.

7.1.7 Use of Policy Constraints Extension

Not specified

7.1.8 Policy Qualifier Syntax and Semantics

Issued certificates may not include policy qualifiers.

7.1.9 Critical Semantic Annotations for Certificate Policy Extension

Field

Critical semantic annotations for certificate policy extension fields used for issued certificates must follow certificate and CRL format profile regulations.

7.2 CARL / CRL Format Profile

7.2.1 Version Numbers

Issued certificate CARL and CRL must comply with X.509 v2 specifications.

7.2.2 CARL / CRL Extension Fields

The issued certificate CARL/CRL formal profile specifies that each extension field must follow certificate and CRL formal profile regulations.

8. CPS Maintenance

8.1 Change Procedure

The NDC shall review the CP at least once per year. CAs shall review the CPS at least once per year to maintain assurance. When revisions made to CPS do not affect certificate usage and assurance stated in the CP, the OID in the CP does not need to be changed and accompanying revisions should be made to the CPS.

8.1.1 Changes Allowed without Notification

New typographic layout changes to the CP and CPS may be made without notification.

8.1.2 Changes Requiring Notification

CAs shall make notification of changes as specified in the CPS.

8.1.2.1 Change Items

The NDC shall evaluate of the level of impact of the changes to the CP on subscribers and relying parties:

(1) Where there is a major impact, notification will be made 30 calendar days before the changes are made.

(2) Where there is a minor impact, notification will be made 15 calendar days before the changes are made.

8.1.2.2 Notification Mechanism

The NDC and CAs shall separately notify the GRCA and CA repositories about changes that may have a significant impact on subscribers. CAs shall state the change notification system in the CPS.

8.1.2.3 Comment Period

The comment period for section 8.1.2.1 changes is:

(1) If there is major impact as specified in section 8.1.2.1 (1), the comment period shall be within 15 calendar days from the announcement date.

(2) If there is a minor impact as specified in section 8.1.2.1 (2), the comment period shall be within 7 calendar days from the announcement date.

CAs shall specify the comment period in the CPS.

8.1.2.4 Comment Response Mechanism

The NDC is responsible for handling CP-related comments. The CAs shall specify the comment handling system in the CPS.

8.1.2.5 Period for Final Change Notice

Changes to the CP and their notification shall be made in accordance with sections 8.1.2.2 and 8.1.2.3. The changes shall be posted for 15 calendar days in accordance with section 8.1.2.1 until the CP change takes effect. CAs shall state the final notice period in the CPS.

8.2 Publication and Notification Procedure

The CP and subsequent revisions shall be posted within 7 calendar days after NDC approval to the GRCA repository. CAs shall state the publication and notification regulations in the CPS.

8.3 CPS Review Procedures

CA CPS must follow relevant laws and comply with CP regulations

and be subject to approval by the NDC and Electronic Signatures Act competent authority MOEA. After announcement of CP revisions, the CA CPS shall be revised accordingly and then submitted to the NDC and Electronic Signatures Act competent authority MOEA for approval.

Appendix: Term Definitions

Access	Use the information processing capabilities of system resources.
Access Control	Authorization procedure for access to information system resources given to subscribers, programs, procedures and other systems.
Activation Data	Private data required besides keys to access cryptographic module (such as data used to activate private key for signatures or encryption)
Applicant	Subscribers who apply for certificates from a CA and have not completed the certificate procedure.
Archive	A physically separate storage site for long-term information (storage site for important information) can be used to support audit, usage and integrity services.
Assurance	A reliable basis to determine that an entity conforms to certain security requirements (standards in Chapter 1 and Chapter 2 Item 1 in the CPS)
Assurance Level	A level possessing a relative assurance level (standards in Chapter 1 and Chapter 2 item 2 in the CPS)
Attribute Authority	Authority to verify a certain entity or certain entity-related attributes based on business purpose.
Audit	Assessment of whether system controls are adequate, ensure conformance with existing policy and operation procedure and independent checking and review of recommended required improvements to current controls, policies and procedures.
Audit Data	Activity logs of a system organized in the order of time of occurrence that can be used to reconstruct or investigate the time sequence or changes that

	occurred during a certain event.
Authenticate	Determination of identity authenticity when an identity of a certain entity is shown.
Authentication	Security measures used for information transmission, messages and sources or authorization methods used to verify whether individuals have received certain types of information.
Backup	Information or program copying that can be used for recovery purposes when needed.
Binding	The process for binding (connection) two related information elements.
Biometric	The physical or behavioral attributes of a person.
CA Certificate	Certificates issued to CAs.
Certificate	(1) Refers to the verification information carrying a digital signature used to verify the identity and qualifications of the signer in electronic form (Article 2.6 of the Electronic Signature Act) (2) Digital presentation of information. The contents included: A. Issuing certificate authority. B. Subscriber name or identity. C. Subscriber public key. D. Certificate validity period. E. Certificate authority digital signature. The term 'certificate' referred to in the certificate policy specifically refers to X.509 v.3 format certificates which states the certificate policy object identifier in the 'certificate policy' field.
Certification Authority (CA)	(1) The agency or natural person that issues certificates. (Article 2.5 of the Electronic Signature Act) (2) The competent body trusted by the subscriber.

	Its functions are issue and administer X.509 format public key certificates, CARLs and CRLs.
Certification Authority Revocation List, (CARL)	A signed and time stamped list. The list contains the serial numbers of revoked CA public key certificates (including cross-certificates).
Certificate Policy (CP)	(1) Refers to a named set of rules that indicates the applicability to a certain community or class of application with common security requirements. (Article 2.3, Chapter in the Regulations on Required Information for Certification Practice Statements) (2) Certification policy refers to the dedicated profile administration policy established for electronic transactions performed through certificate administration. Certificate policy covers a variety of issues including the formation, generation, delivery, auditing, administration and restoration after compromise. Certificate policy indirectly controls the use and operation of certificate security systems to protect the transactions performed by communication systems. The security services required for certain application are provided through control of the certificate extension field method, certificate policy and related technology.
Certification Practice Statement (CPS)	(1) External notification by the certificate authority used to describe the practice statement of the certificate authority governing certificate issuance and processing of other certification work. (Electronic Signature Act Article 2.7) (2) Announcement of a statement that certain procedures of the certificate authority for certificate work (including issuance, suspension, revocation, renewal and access) comply with certain requirements (listed in the certificate policy or other service contracts).

Certificate Revocation List (CRL)	(1) Certificate revocation list digitally signed by the certificate authority provided for relying party use. (Article 2.8, Chapter 11 in the Regulations on Required Information for Certification Practice Statements) (2) List maintained by the certificate authority. The expiry date of above revoked certificates issued by the certificate authority are recorded on the list.
Component Private Key	Private keys associated with certificate issuance equipment functions as opposed to private keys associated with operators or administrators.
Compromise	Information disclosed to unauthorized persons or unauthorized intentional or unintentional disclosure, modification, destruction or loss of objects which constitutes a violation of information security policy.
Confidentiality	Information which will not be known or be accessed by unauthorized individuals or programs.
Cross-Certificate	A certificate issued from one certificate authority to another certificate authority which is used to establish a trust relationship between the two certificate authorities. The cross-certificate is a type of CA certificate.
Cryptographic Module	A set of hardware, software, firmware or combination of the above used to run cryptologic or programs (including cryptoalgorithms) and included within the cryptographic boundaries of the module.
Cryptoperiod	The validity period set for each key.
Data Integrity	Information that has not been subjected to unauthorized access or accidental modification, damage or loss.
Digital Signature	An electronic signature generated by the use of mathematic algorithm or other means to create a

	certain length of digital data encrypted by the signatory's private key and capable of being verified by the public key.(Electronic Signature Act Article 2.3)
Dual-Use Certificate	Certificates that may be used for digital signatures or data encryption.
Duration	A certificate field made up on two subfields, "start time of the validity period" (notBefore) and "end time of the validity period" (notBefore).
E-commerce	Provision of goods for sale and other services through the use of network technology (specifically the Internet).
Encryption Certificate	A certificate including a public key used for encryption of electronic messages, files, documents or other information. This key can also be used to establish or exchange a variety of short-term secret keys used for encryption.
End Entity	Relying parties and subscribers including persons, organizations, accounts, devices and sites.
End-Entity Certificate	Certificates issued to end-entities.
Firewall	An access restriction gateway between networks which complies with near-end (local area) security policy.
Inside Threat	Possible damage to information systems through granting of authorization by means such as information destruction, disclosure, tampering or denial of service methods.
Integrity	Protecting information so that it is not subject to unauthorized modification or damage. Preserve information in an untampered state during transmission and storage following generation at its source until receipt by the final recipient.

Key Escrow	Storage of related information using the subscriber's private key and according to the regulations of the mandatory subscriber escrow agreement (or similar contract). The terms of this escrow agreement requires that one or more than one agencies have possession the subscriber key provided it is beneficial to the subscriber, employer or another party in accordance with the provisions of the agreement.
Key Exchange	Mutual exchange of keys to establish a secure communication processing procedure.
Key Generation Material	Random numbers, pseudo random numbers and other password parameters used to generate keys.
Key Pair	Two mathematically linked keys possessing the following attributes: (1) One of the keys is used for encryption. This encrypted data may only be decrypted by the other key. (2) It is impossible to determine one key from another (from a mathematical calculation standpoint).
Cross Certification Agreement (CCA)	The agreement containing the terms and individual liability and obligations that must be followed when the government root certification authority and subordinate certification authorities apply to join the government authority public key infrastructure.
Issuing CA	The CA that issues a certain certificate is the issuing CA.
Mutual Authentication	When two parties authenticate one another during communication activities (see authentication definition)
Naming Authority	A competent authority responsible for assigning a unique identifying name and ensuring that each unique identifying name is meaningful and unique within its field.

Non-Repudiation	Provide proof of delivery to the information sender and proof of sender identity to the receiver so the neither party may repudiate the processing of this information after the fact. Technically speaking, non-repudiation refers the guarantee that this signature must be signed by the corresponding private key if a certain key can be used to verify a certain digital signature for a trusting party. Legally speaking, non-repudiation refers to the establishment of possession and control system for private signature keys.
Object Identifier (OID)	(1) Refers to a unique alphanumeric / numeric identifier registered under the International Standard Organization registration standard and which could be used to identify the uniquely corresponding certificate policy; where the certificate policy is modified, the OID is not changed accordingly. (Article 2.4, Chapter 1 in the Regulations on Required Information for Certification Practice Statements) (2) When a special form of code, object or object type is registered with the International Standard Organization (ISO), the unique code may be used as an identifier. For example, this code can be used in the public key infrastructure to indicate what certificate policy and cryptographic algorithms are used
Out-of-Band	Delivery method other than the ordinary information delivery channels. If the delivery method is by electric cable, a special secure channel may be the use of physical registered mail.
Outside Threat	An external and unauthorized entity which could have potentially destructive effect on information systems (including information destruction, tampering, disclosure or denial of service).
Government	An organization whose founding mission is to:

Electronic Certification Steering Committee	Review the administration authority electronic certificate policy, certificate practice statement, related technical specifications, the electronic certificate system framework and other electronic certificate administration matters.
Private Key	(1) The key in the signature key pair used to generate digital signatures. (2) The key in the encryption key pair used to decrypt secret information. This key must be kept secret under these two circumstances.
Public Key	(1) The key in the signature key pair used to verify the validity of the digital signature. (2) The key in the encryption key pair used for encrypting confidential information. These keys must be made public (usually in a digital certificate form) under these two circumstances.
Registration Authority (RA)	(1) Responsible for checking the identity and other attributes of the certificate applicant but does not issue or administer certificates. The nature and scope of obligations borne by the registration authority are set down in the applicable certificate policy or agreement. (2) An entity responsible for the identification and authentication of the certificate subject identity which does not issue certificates.
Re-key (a certificate)	Use of a key value to change the cryptographic system application program. It is commonly achieved by issuing a new certificate for the new public key.
Relying Party	(1) Recipient of a certificate who acts in reliance of that certificate or a digital signature to verify the public key listed in the certificate, or the counterparty to identity (or its attributes) of the subject named in a trusted certificate and public key listed in the certificate. (Article 2.6, Chapter 1 in the

	Regulations on Required Information for Certification Practice Statements) (2) The individual or agency which receives information which includes a certificate and digital signature (the public key listed on the certificate may be used to verify this digital signature) and may rely on this information.
Renew (a certificate)	The procedure for issuing a new certificate to renew the validity of information bound together with the public key.
Repository	(1) A reliable system used to store and retrieve certificates or other information relevant to certifications. (Article 2.7, Chapter 1 in the Regulations on Required Information for Certification Practice Statements) (2) The repository containing the certificate policy and certificate-related information.
Revoke a Certificate	Termination of a certificate prior to its expiry date.
Government Root CA	The highest level certificate authority in public key infrastructure hierarchy and the trust anchor of public keys.
Secret Key	Shared secret in the symmetric cryptosystem, identity authentication of the subscriber is performed by sharing other secrets through password, PIN or remote host (or server). The single key is jointly held by two parties. The sender uses it to encrypt the transmitted information and the receiver uses it to decrypt this information. This jointly held key is generated with previously agreed upon algorithms.
Signature Certificate	Public key certificates which contains a digital signature public key used for verification purposes (not used for data encryption or other cryptographic uses).
Subject CA	For a CA certificate, the certificate authority

	referred to in the certificate subject of a certificate is the subject CA for that certificate.
Subordinate CA	In the public key infrastructure hierarchy, certificates that are issued by another certificate authority and the activities of the certificate authority are restricted to this other certificate authority.
Subscriber	(1) Refers to a subject named or identified in the certificate that holds the private key that corresponds with the public key listed in the certificate (Regulations on Required Information for Certification Practice Statements Chapter 1 Article 2.5) (2) An entity having the following attributes including (but not restricted to) individuals, organizations and network devices: (a) Entity listed on an issued certificate. (b) A private key that corresponds to the public key listed in the certification. (c) Other parties that do not issue certificates.
Technical Non-Repudiation	Technical evidence provided by the public key system to support non-repudiation security service.
Threat	Any status or event that may damage information systems (including destruction, malicious data tampering or denial of service).
Trust List	List of trusted certificates used by relying parties to authenticate certificates.
Trusted Certificate	Certificate trusted by relying party obtained through a secure and reliable transmission method. The public key contained in this type of certificate comes from a trusted path.
Trusted Timestamp	Digital signing by a trusted competent authority to prove that certain digital object exists at a certain time.
Trustworthy	Computer hardware, software and programs which

System	possess the following attributes: (1) Functions that protect again intrusion and misuse. (2) Provides reasonably accessible, reliable and accurate operations. (3) Appropriate implementation of preset function. (4) Security procedures uniformly accepted by the general public.
Zeroize	Method to delete electronically stored information. Storage of changed information to prevent information recovery.