

Certificate Policy for the Government
PKI
Version 1.1

Administration Organization:

Research, Development And Evaluation Council, Executive Yuan

Execution Organization:

Chunghwa Telecom Co., Ltd.

January 9, 2003

Table of Contents

1 INTRODUCTION	1
1.1 OVERVIEW.....	3
1.1.1 Certificate Policy (CP).....	3
1.1.2 Relationship between CP(certification policy) and CPS(certification practice statement)	3
1.1.3 How CAs should cite CP OID	3
1.2 IDENTIFICATION	4
1.3 COMMUNITY AND APPLICABILITY	4
1.3.1 Government electronic certification steering committee	4
1.3.2 Government root certification authority	5
1.3.3 Subordinate CA.....	5
1.3.4 RA(registration authority).....	6
1.3.5 Repository	6
1.3.6 Other related authorities.....	6
1.3.7 End entities.....	6
1.3.8 Applicability.....	7
1.4 CONTACT DETAILS.....	9
1.4.1 Specification administration organization	9
1.4.2 Contact Person	9
1.4.3 Person determining Certification Practice Statement suitability for the policy.....	9
2. GENERAL PROVISIONS	11
2.1 OBLIGATIONS.....	11
2.1.1 CA Obligations	11
2.1.2 RA Obligations	11
2.1.3 Subscriber Obligations.....	12
2.1.4 Relying Party Obligations.....	12
2.1.5 Repository Obligations	13
2.2 Liability.....	13

2.2.1 CA Liability	13
2.2.2 RA Liability	14
2.3 FINANCIAL RESPONSIBILITY	14
2.3.1 Indemnification by Relying Parties and Subscribers.....	14
2.3.2 Administrative Processes	14
2.4 INTERPRETATION AND ENFORCEMENT	15
2.4.1 Governing Law	15
2.4.2 Severability of Provision, Survival, Merger and Notice	15
2.4.3 Dispute Resolution Procedures.....	15
2.5 Fees	15
2.5.1 Certificate Issuance or Renewal Fees	15
2.5.2 Certificate access fees	15
2.5.3 Revocation or status information access fees	15
2.5.4 Fees for other services such as policy information.....	15
2.5.5 Refund Policy.....	16
2.6 Publication and Repository	16
2.6.1 Publication of CA Information	16
2.6.2 Frequency of publication	16
2.6.3 Access Controls.....	17
2.6.4 Repositories.....	17
2.7 Compliance audit	17
2.7.1 Frequency of entity compliance audit.....	17
2.7.2 Identity and qualifications of auditor.....	18
2.7.3 Auditor's relationship to audited party	18
2.7.4 Topics covered by audit	18
2.7.5 Actions taken as a result of deficiency	19
2.7.6 Communication of results	19
2.8 CONFIDENTIALITY	20
2.8.1 Types of information to be kept confidential.....	20
2.8.2 Types of information not considered confidential	20
2.8.3 Disclosure of certificate revocation/suspension information	20
2.8.4 Release to law enforcement officials	21
2.8.5 Release as part of civil discovery	21

2.8.6 Disclosure upon owner's request	21
2.8.7 Other information release circumstances.....	21
2.9 Intellectual Property Rights	21
3 IDENTIFICATION AND AUTHENTICATION.....	22
3.1 INITIAL REGISTRATION.....	22
3.1.1 Types of names.....	22
3.1.2 Need for names to be meaningful.....	22
3.1.3 Rules for interpreting various name forms	22
3.1.4 Uniqueness of names	22
3.1.5 Name claim dispute resolution procedure	23
3.1.6 Recognition, authentication and role of trademarks	23
3.1.7 Method to prove possession of private key	23
3.1.8 Authentication of organization identity	24
3.1.9 Authentication of individual identity	27
3.1.10 Authentication of Component Identities.....	30
3.2 CERTIFICATE RENEWAL AND ROUTINE RE-KEY.....	31
3.2.1 Routine Rekey.....	31
3.2.2 Certificate Renewal.....	32
3.3 Rekey after Revocation.....	32
3.4 REVOCATION REQUEST	33
4 OPERATIONAL REQUIREMENTS	34
4.1 Certificate Application.....	34
4.2 Certificate Issuance.....	34
4.3 Certificate Acceptance	35
4.4 Certificate Suspension and Revocation	36
4.4.1 Circumstances for revocation	37
4.4.2 Who can request revocation.....	38
4.4.3 Procedure for revocation request.....	38
4.4.4 Revocation request grace period.....	39
4.4.5 Circumstances for suspension.....	39
4.4.6 Who can request suspension	39
4.4.7 Procedure for suspension request	39
4.4.8 Limits on suspension period	40

4.4.9 CARL/CRL issuance frequency	40
4.4.10 CARL/CRL Checking Requirements	41
4.4.11 On-line revocation/status checking availability.....	41
4.4.12 On-line revocation checking requirements	42
4.4.13 Other forms of revocation advertisements available	42
4.4.14 Checking requirements for other forms of revocation advertisements.....	42
4.4.15 Special requirements to Key Compromise	42
4.5 Security Audit Procedures	42
4.5.1 Types of event recorded	43
4.5.2 Frequency of processing log	49
4.5.3 Retention period for audit log.....	50
4.5.4 Protection of audit log.....	50
4.5.5 Audit log backup procedures	51
4.5.6 Audit collection system.....	51
4.5.7 Notification to event-causing subject	51
4.5.8 Vulnerability assessments	52
4.6 Records Archival.....	52
4.6.1 Types of event recorded	52
4.6.2 Retention period for archive	53
4.6.3 Protection of archive	54
4.6.4 Archive backup procedures.....	54
4.6.5 Requirements for time-stamping of records	54
4.6.6 Archive collection system.....	54
4.6.7 Procedures to obtain and verify archive information	55
4.7 Key changeover	55
4.7.1 Key Changeover of CA.....	55
4.7.2 Key Changeover of Subscriber	55
4.8 Compromise and Disaster Recovery	56
4.8.1 Computing resources, software, and/or data are corrupted ..	56
4.8.2 Entity public key is revoked	56
4.8.3 Entity key is compromised	57
4.8.4 Secure facility after a natural or other type of disaster.....	57
4.9 CA Termination.....	57

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	58
5.1 Physical Controls	58
5.1.1 Site location and construction.....	58
5.1.2 Physical access.....	58
5.1.3 Power and air conditioning.....	59
5.1.4 Water exposures	60
5.1.5 Fire prevention and protection.....	60
5.1.6 Media storage.....	60
5.1.7 Waste disposal.....	60
5.1.8 Off-site backup.....	61
5.2 Procedural Controls	61
5.2.1 Trusted roles.....	61
5.2.2 Allocation of roles	64
5.2.3 Number of persons required per task.....	64
5.2.4 Identification and authentication for each role	64
5.3 Personnel Controls.....	65
5.3.1 Background, qualifications, experience, and clearance requirements.....	65
5.3.2 Background check procedures	65
5.3.3 Training requirements	66
5.3.4 Retraining frequency and requirements.....	66
5.3.5 Job rotation frequency and sequence.....	66
5.3.6 Sanctions for unauthorized actions.....	66
5.3.7 Contracting personnel requirements	67
5.3.8 Documentation supplied to personnel	67
6 TECHNICAL SECURITY CONTROLS	68
6.1 Key Pair Generation and Installation.....	68
6.1.1 Key pair generation.....	68
6.1.2 Private key delivery to entity.....	69
6.1.3 Public key delivery to certificate issuer.....	70
6.1.4 CA public key delivery to users.....	70
6.1.5 Key sizes	71
6.1.6 Public key parameters generation.....	72

6.1.7	Parameter quality checking.....	72
6.1.8	Hardware/software key generation	73
6.1.9	Key usage purposes (as per X.509 v3 key usage field)	73
6.2	Private Key Protection	74
6.2.1	Standards for cryptographic module.....	74
6.2.2	Private key (n out of m) multi-person control	75
6.2.3	Private key escrow	75
6.2.4	Private key backup.....	75
6.2.5	Private key archival	76
6.2.6	Private key entry into cryptographic module	76
6.2.7	Method of activating private key	76
6.2.8	Method of deactivating private key	76
6.2.9	Method of destroying private key	76
6.3	Other Aspects of Key Pair Management	77
6.3.1	Public key archival.....	77
6.3.2	Usage periods for the public and private keys.....	77
6.4	Activation Data	79
6.4.1	Activation data generation and installation	79
6.4.2	Activation data protection.....	79
6.4.3	Other aspects of activation data	80
6.5	Computer Security Controls	80
6.5.1	Specific computer security technical requirements	80
6.5.2	Computer security rating	81
6.6	Life Cycle Technical Controls.....	81
6.6.1	System development controls	81
6.6.2	Security management controls.....	82
6.6.3	Life cycle security ratings.....	83
6.7	Network Security Controls	83
6.8	Cryptographic Module Engineering Controls	83
7	CERTIFICATE AND CARL/CRL PROFILES	84
7.1	Certificate Profile.....	84
7.1.1	Version numbers.....	84

7.1.2 Certificate extensions.....	84
7.1.3 Algorithm object identifiers.....	84
7.1.4 Name forms.....	85
7.1.5 Name constraints.....	85
7.1.6 Certificate policy Object Identifier.....	85
7.1.7 Usage of Policy Constraints extension.....	85
7.1.8 Policy qualifiers syntax and semantics.....	85
7.1.9 Processing semantics for the critical certificate policy extension.....	86
7.2 CARL/CRL Profile.....	86
7.2.1 Version Numbers.....	86
7.2.2 CARL/CRL and CARL/CRL entry extensions.....	86
8. SPECIFICATION ADMINISTRATION.....	87
8.1 Specification change procedures.....	87
8.1.1 Items of Change That Will Not be Notified.....	87
8.1.2 Items of Change That Will be Notified.....	87
8.2 Publication and notification policies.....	89
8.3 CPS approval procedures.....	89
APPENDIX : GLOSSARY.....	90

1 Introduction

The Government Public Key Infrastructure, (hereinafter abbreviated as the GPKI) is established based on the e-government implementation plan (from 2001 to 2004). The purpose is to establish a secure and trusted electronic certification system in order to strengthen the e-government infrastructure. Based on the ITU-T X.509 hierarchical Public Key Infrastructure (hereinafter abbreviated as PKI) model, the GPKI comprises the trust anchor, Government Root Certification Authority (hereinafter abbreviated as the GRCA), and the subordinate certification authority (hereinafter abbreviated as the CA) established by the government. The GRCA shall accept the certificate application of CA that is established based on e-government electronic certification service divisional responsibility. Certificates will be applied to various applications of the e-government so as to provide more convenient and faster network service to people, to enhance government administration efficiency, and to step up the development of e-government and e-commerce applications.

Based on the international common practice, each PKI will have a management authority so as to ensure its proper operation. For GPKI, the Research, Development and Evaluation Council of Executive Yuan (hereinafter abbreviated as the RDEC) is the management authority. The RDEC also established the Government Electronic Certification Steering Committee (hereinafter abbreviated as the GECSC) to assist the RDEC to conduct the management of the GPKI. The responsibilities of the GECSC are described in Section 1.3.1.

This Certificate Policy (hereinafter abbreviated as the CP) is a technical policy document stipulated according to the provision of the Electronic Signature Act and related international standard (RFC 2527 etc.) so that the policy can be a basis for stipulation of CPSs for government CAs. Totally this certificate policy defines five assurance levels. In proper order, there are Level 1, Level 2, Level 3 and Level 4, where higher level ranking indicates higher level of assurance. In addition, there is a Test Level which is provided only for testing. Based on the X.509 standard, it is required to have the assurance level be represented by a CP Object Identifier, (hereinafter abbreviated as CP OID) and these CP OIDs will be asserted in the certificatePolicies

extensions.

Assurance level refers to the level of confidence by the Relying Party on the following aspects:

- (1) How well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate; Note that when a CP OID is asserted in the certificate Policies extensions, there can be two different interpretations. If the certificate is issued to an end entity (refer to Section 1.3.7), the CP OID represents the assurance level, based on which the identity authentication and certificates issuance are performed to the subscriber. If the certificate is issued to a CA, then in the certificate there may be multiple CP OIDs, indicating the assurance levels of which the subject CA is allowed to sign certificates to end entities .()
- (2) How securely the system which was used to produce the certificate and (if appropriate) deliver the private key to the subscriber performs its task;
- (3) How well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate. For example, subscribers may use software or hardware to store their private keys.

CAs in the GPKI should cite appropriate CP OID(s) so that interoperability can be conducted between various CAs. In addition, interoperability can be conducted further with commercial PKIs or foreign PKIs. These five assurance levels of this CP are only applicable to the management and interoperability within the GPKI. For other PKI domains, it is permitted to assert the CP OID(s) of the GPKI in the policy mapping extensions only when the equivalence of policy has been approved.

The terms and provisions of this CP shall be interpreted under and governed by applicable law. The term CA in this CP means all CAs in the GPKI. Based on the principle of mutual benefit with other domestic or foreign PKIs, after approved by the RDEC, the GRCA can conduct cross-certification with CAs outside the GPKI domain. Any

use of or reference to this CP by CAs outside the GPKI domain is completely at the using party's risk.

1.1 OVERVIEW

1.1.1 Certificate Policy (CP)

A certificate policy is a kind of guideline of information technology on electronic certification. According to the definition of X.509 standard, it is a name set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements.

In a certificate, the CP OID specifies the CP. The GPKI has five registered CP OIDs that can be chosen by CAs to label the assurance level of an issued certificate. CA can make direct reference to registered CP OIDs, which may be used by a relying party to decide whether a certificate is trusted for a particular purpose. At the same time, the five registered CP OIDs, if necessary, can be used for policy mapping between the GPKI domain and other PKI domain so as to facilitate the interoperability.

The GRCA's certificate is a self-signed certificate and is the trust anchor of the GPKI so a relying party can directly trust that certificate. Based on international standard and common practice, the certificate of GRCA does not contain any CP OID. However, since the GRCA must maintain significant trust by the public, it must be operated in accordance to assurance level 4 of this CP.

1.1.2 Relationship between CP(certification policy) and CPS(certification practice statement)

In a certification practice statement (hereinafter abbreviated as CPS), it is required to explain how to achieve the assurance level of the certificate policy.

1.1.3 How CAs should cite CP OID

The CAs in the GPKI should abide by this CP and are not allowed to define their own certificate policies. Any citation of this CP should be

approved by the RDEC. Please contact the RDEC for any suggestion on this CP.

1.2 IDENTIFICATION

There are five levels of assurance in this CP which are defined in subsequent Sections. Each level of assurance has an Object Identifier (OID), to be asserted in certificates (not including self-signed certificates) issued by the GRCA. The OIDs are registered under the id-tw-gpki arc as follows:

id-tw-gpki ::= {2 16 886 101 0}
id-tw-gpki -certpolicy ::= {id-tw-gpki 3}

Assurance Level	CP OID name	CP 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 COMMUNITY AND APPLICABILITY

1.3.1 Government electronic certification steering committee

In order to establish e-government electronic certification system, to drive the e-government PKI, and to speed up the development of the application of government network convenient public service, the RDEC established the GECSC. In GECSC there is one convener who will be undertaken concurrently by a deputy chairman assigned by the chairman of the RDEC. There will be one executive secretary who will be undertaken by the head of the Department of the Information Management of the RDEC. There will be fifteen to seventeen members who will be scholars, experts, member of business sector and authority

representatives and their tasks are as follows:

- (1) To survey and review the government CP and CPSs.
- (2) To survey and review the technical standards of the government electronic certificate.
- (3) To survey and review the framework of digital certificates.
- (4) To survey and review related administrative issue of digital certificates.

1.3.2 Government root certification authority

The GRCA is the most top level CA of the GPKI and its main work is as follows:

- (1) Responsible for the issuance and management of subordinate CA certificate.
- (2) Responsible for stipulating the procedure for cross-certifying CAs inside or outside of the GPKI domain, including issuing and managing the Level 1 subordinate CA certificates in the GPKI and other CA certificates outside the GPKI.
- (3) Responsible for publishing the issued certificates and the Certification Authority Revocation List (hereinafter abbreviated as CARL) in the repository and ensure the availability of the repository.

The GRCA should specify the cross-certification procedure in its CPS.

1.3.3 Subordinate CA

A subordinate CA is another kind of CA in the GPKI and it is mainly responsible for issuing and managing certificates of the end entities. If necessary, it can issue certificates to other CAs based on the hierarchical PKI model, namely, the Level 1 subordinate CAs may issue certificates to Level 2 subordinate CAs, and Level 2 subordinate CAs may issue certificate to Level 3 subordinate CAs, and so forth. The subordinate CAs are not permitted to process cross- certification directly with the CAs outside the GPKI.

The establishment and operation of subordinate CAs shall follow the provisions of this CP. A liaison mechanism in the subordinate CA shall be established which is responsible for the interoperability work with the GRCA and other subordinate CAs.

1.3.4 RA(registration authority)

A Registration Authority (hereinafter abbreviated as RA) is an entity that collects and verifies each Subscriber's identity and information that are to be entered into his or her public key certificate.

The GRCA shall undertake the role of RA on its own and carry out the work of RA based on its CPS. The subordinate CAs may establish their RAs separately and define their tasks in their CPSs.

1.3.5 Repository

The Repository provides inquiry and download service for the certificates, Certificate Revocation Lists (hereinafter abbreviated as CRL), and certificate status information, etc, issued by the CA. It will also publish the operation information of the CA, including CP and CPS.

A CA may operate its own repository, or it may delegate the operation of the repository to other authority. Each CA should have at least one repository. CAs shall document the network location of the repository in their CPS and ensure the availability, access control and integrity of the repository.

1.3.6 Other related authorities

Any CA can select other related administrative organization as the assistant such as the Compliance Audit Authority, Attribute Authority, Time Stamp Authority, Data Validation and Certification Authority etc. and relevant terms and operation system shall be specified in the CPS.

1.3.7 End entities

In the GPKI, End Entities (EE) include the following two types of entities:

- (1) Entities who are responsible for the custody and usage of private keys.
- (2) Entities (neither private key owners nor CAs) that trust certificates issued by the CA established in the GPKI.

1.3.7.1 Subscribers

To organizations and individuals, a subscriber is an entity whose name appears as the subject in a certificate and is an entity possessing corresponding private key of the public key. Subscriber, based on the certificate asserted in the CP, use the certificate legitimately. In addition, in regard to property category (for example, Application Process) and Device, as the property itself has no capacity, the subscriber shall be the individual or organization applying for the certificate.

In the GPKI, the upper level authority will issue certificate to the subordinate (level) CA. In this CP, the subordinate CA is not a subscriber.

To operation personnel of the CA (including RA) and possibly certain network or hardware devices such as firewalls or routers needed for infrastructure protection, CA can separately be issued and managed by internal CA entities. CA established due to the necessity of internal maintenance and operation cannot join the GPKI.

1.3.7.2 Relying parties

A relying party is an entity relying on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information.

The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, and to establish confidential communicates with the holder of the certificate. A Relying Party may use the information in the certificate (such as CP OID) to determine the suitability of the certificate for a particular use.

1.3.8 Applicability

CPs must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This CP specifies security requirements at five increasing, qualitative levels of assurance.

1.3.8.1 Applicability of the certificate

The certificate levels of assurance contained in this CP are set forth below, as well as a brief and non-binding description of the applicability for applications suited to each level.

Assurance level	Applicability
Test level	Only provided for test use and does not bear any legal responsibility on the transmitted data.
Level 1	A rudimentary level of assurance relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter when certificates having higher levels of assurance are unavailable. It is not applicable to on-line transaction that requires certification.
Level 2	A basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. It is not applicable to be signature of important document.
Level 3	A medium level of assurance relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk or involving access to private information where the likelihood of malicious access is substantial.
Level 4	A high level of assurance appropriate for use where the threats to data are high, or the consequences of the failure of security service is high. This may include very high value transactions or high levels of fraud risk.

1.3.8.2 Factors in determining usage

End entities shall select suitable certificate assurance level according to the security requirement in the application system.

During usage of the private key, any subscriber shall select secure and reliable computer environment and application system so as to avoid

theft of the private key resulting damage on his/her rights and interests. The application system shall base on the usage of key in Section 6.1.9 to use the key properly and to process the critical certificate extension.

1.3.8.3 Usage prohibition of certificate

Certificates issued by CAs of the GPKI are prohibited to be used in the following conditions:

- (1) Crime commitment
- (2) Military orders, battles, nuclear and chemical weapon controls.
- (3) Nuclear energy operation equipment.
- (4) Aviation flying and control system.

1.4 CONTACT DETAILS

1.4.1 Specification administration organization

RDEC(Research,Development and Evaluation Council), Executive Yuan.

1.4.2 Contact Person

If there is any suggestion on this CP, please contact the RDEC. For contact information, please refer to <http://grca.nat.gov.tw/> °

1.4.3 Person determining Certification Practice Statement suitability for the policy

CAs are responsible for determining whether their CPSs can conform to their CPs that will be submitted to the GECSC for examination and approved by the RDEC. Upon approval by the RDEC, CAs can officially cite the CP of the GPKI.

In addition, according to the provision of the Electronic Signature Act, approval for CPS specified by the CA shall be obtained from the administrative organization, Ministry of Economic Affairs before such CA can provide certification service.

The RDEC reserves the right to audit CPs' compliances (based on the provision in Section 2.7). Every CA shall also conduct audit periodically so as to prove that it operates according to the assurance level of the CP.

2. GENERAL PROVISIONS

2.1 OBLIGATIONS

2.1.1 CA Obligations

CAs are responsible for:

- (1) Issuing and publishing certificates.
- (2) Executing the authentication procedure provided in Chapter 3.
- (3) Publishing the information of revoked and suspended certificates.
- (4) Issuing and publishing CARLs or CRLs. (Not required for CAs operating at the test level).
- (5) Enforcing relevant controls in accordance with the provision in Chapter 4 and 6.
- (6) Publishing the CPS and stating the responsibilities of subscribers and relying parties.
- (7) Safekeeping the private key according to the provisions in Chapter 4, 5, and 6.
- (8) Ensuring the appropriate use of the CA private keys. Different assurance levels might require different CA private keys for signing certificates, CARLs, CRLs, digital signatures and information relevant to issuance of certificates.
- (9) Ensuring their CPSs to abide by this CP.

2.1.2 RA Obligations

No stipulation for the test level.

For other assurance levels, RAs are responsible for:

- (1) Enforcing relevant controls in accordance with the provisions in

Chapter 4, 5 and 6.

- (2) Conducting identification and authentication on the certificate application based on the provisions in Chapter 3.
- (3) Informing subscribers and relying parties of the obligations and responsibilities of CAs and RAs.
- (4) Informing subscribers and relying parties that they shall abide by the provisions of the CP when using or accepting the certificate issued by the CA.
- (5) Safekeeping the RA private keys according to the provisions in Chapter 4, 5 and 6.
- (6) Ensuring the RA private keys be used according to the provisions in Section 6.1.9. Without the consent from CA, it cannot be used in operation beyond certificate registration.

2.1.3 Subscriber Obligations

Subscribers who accept certificates from CAs are responsible for:

- (1) Abiding by the procedures provided in Chapter 3 and 4.
- (2) Using the certificate properly.
- (3) Safekeeping and using the private key properly. (No stipulation for certificates issued at the test level).
- (4) Notifying the CA immediately when the private key has been compromised. (No stipulation for certificates issued at the test level).

2.1.4 Relying Party Obligations

Relying parties using the certificate issued by CAs are responsible for:

- (1) Being aware of the application scope and assurance level of the certificate thoroughly.

- (2) Using the certificate based on the application scope of the certificate.
- (3) Correctly validating the digital signature of the certificate.
- (4) Correctly validating the certificate revocation and suspension list.
(No stipulation for certificates issued at the test level).

2.1.5 Repository Obligations

The repositories of CAs are responsible for :

- (1) Publishing the issued certificate periodically.
- (2) Publishing the revoked and suspended certificate information periodically.
- (3) Publishing the latest information of the CP and the CPS.
- (4) Ensuring the access of the repository being in accordance with the provisions in Section 2.6.3.

2.2 Liability

2.2.1 CA Liability

2.2.1.1 Warranties and Limitations on Warranties

In the certificate issued by the certification authority, if the CP OID of any assurance level specified by this CP is cited, the information of the issued certificate guaranteed by that CA complies with the provisions of this CP. Unless the CA can actually abide by the provisions of this CP, otherwise the CP OID of any assurance level specified by this CP should not be cited in the issued certificate.

2.2.1.2 Disclaimers of Warranties

Any CA can assert disclaimers and limitations in its CPS so as to eliminate certain liabilities of such CA. However, the CA cannot disclaim the liability for damages caused by its negligence.

2.2.1.3 Other Exclusions

CAs can assert any force majeure or other causes that cannot be blamed on CAs such as natural disaster, incidental, emergent, or special events as exclusions in their CPSs. However, the CA cannot disclaim the liability for damages caused by its negligence.

2.2.2 RA Liability

CAs shall bear all responsibilities of RAs caused by executing the task of RAs. The responsibility of RAs shall be determined based on the agreement of respective rights and obligations with CAs. CAs shall assert the liability of RAs in the CPSs or in the contract or in the agreement with RAs.

2.2.2.1 Warranties and Limitations on Warranties

No stipulation.

2.2.2.2 Disclaimers and Limitations

No stipulation.

2.2.2.3 Other Exclusive Clauses

No stipulation.

2.3 FINANCIAL RESPONSIBILITY

2.3. Indemnification by Relying Parties and Subscribers

CAs shall assert the indemnity liability to subscribers and relying parties in the CPS.

2.3.2 Administrative Processes

Administrative processes of the CA shall be determined by the administration organization of CA.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing Law

The applicable laws of the Republic of China govern the provisions described in this CP and agreements entered into by CAs and other parties for the sake of requirements set forth in this CP.

2.4.2 Severability of Provision, Survival, Merger and Notice

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect based on the provision of Section 8.1.

2.4.3 Dispute Resolution Procedures

When any dispute on the interpretation of this CP arises, both parties in dispute shall negotiate for a consensus. If negotiation fails, both parties may seek for interpretation according to the dispute resolution procedure specified by the RDEC. CAs shall assert in their CPSs the dispute resolution procedures.

2.5 Fees

2.5.1 Certificate Issuance or Renewal Fees

No stipulation.

2.5.2 Certificate access fees

No stipulation.

2.5.3 Revocation or status information access fees

No stipulation.

2.5.4 Fees for other services such as policy information

No stipulation.

2.5.5 Refund Policy

No stipulation.

2.6 Publication and Repository

2.6.1 Publication of CA Information

Any CA shall publish the following information in its repository:

- (1) its CPS,
- (2) the CRLs it issues (or provide on-line certificate status inquiry), certificate revocation time,
- (3) the CA certificate of itself, which shall be available till the expiration of all certificates issued by the corresponding private key of that CA certificate,
- (4) all certificates it issues (including certificates issued to other CAs),
- (5) the CARLs it issues (if that CA issues any certificate to any other CA), and
- (6) privacy policy.

Apart from the above information, the CA shall publish necessary information, if any, to make sure that all its digital signatures can be verified.

The CPS of the CA shall assert the upper limit of the temporary out-of-service duration of the repository.

2.6.2 Frequency of publication

Publication frequency of CRLs shall be in accordance with the provisions in Section 4.4 and publication of CP shall be in accordance with the provisions in Section 8.

2.6.3 Access Controls

- (1) The access of this CP and CPSs of the CAs does not require access control.
- (2) Any CA may decide on its own whether the access of certificates requires access controls.

CAs shall protect any repository information not to be intended for public dissemination or modification. Public keys and certificate status information in the repository shall be publicly available through the Internet.

2.6.4 Repositories

According to the provisions in Section 1.3.5, repositories may be operated by CAs or other authorities. The CPS of a CA shall assert relevant information of its repository.

2.7 Compliance audit

CAs that issue certificates at assurance level 2, 3 and 4 must have an impartial compliance audit mechanism in place to ensure that the provisions of their CP/CPS are being implemented and enforced.

2.7.1 Frequency of entity compliance audit

CAs shall be subjected to a periodic compliance audit which is no less frequent than once a year for assurance level 3 and level 4, and no less than once every two years for assurance level 2. There is no audit requirement for CA operating at test level and assurance level 1.

CAs have the right to require periodic and aperiodic compliance audits or inspections of subordinate CA or RA operations to validate that the subordinate entities are operating in accordance with their

respective CPS.

If necessary, the RDEC may perform aperiodic compliance audits on subordinate CAs (and, when needed, their subordinate CAs) that interoperate with the GRCA. The RDEC shall state the reason for any aperiodic compliance audit.

2.7.2 Identity and qualifications of auditor

Compliance auditor either shall be a private firm which is independent from the entity being audited, or it shall be organizationally separated from the entity to provide an unbiased, independent evaluation.

The compliance auditor shall provide impartial and independent evaluation, whose qualification shall be approved by the RDEC, and must be familiar with requirements which the CA imposes on the issuance and management of their certificates. Before the compliance audit, CA shall perform identification and authentication on the compliance auditor.

2.7.3 Auditor's relationship to audited party

Based on the provisions in Section 2.7.2, the compliance auditor shall be independent from the entity being audited.

2.7.4 Topics covered by audit

Compliance auditor shall verify the following:

- (1) Whether the CA operates in accordance with its CPS.
- (2) Whether the CPS of the CA meets the requirements of this CP.

The compliance auditor may conduct compliance audit on relevant entities of the CA such as its RAs.

If any CA and its subordinate CA sign the cross-certification agreement, the scope of compliance audit shall cover whether the subordinate CA conforms to the provisions of the cross-certification

agreement.

2.7.5 Actions taken as a result of deficiency

When the compliance auditor finds a discrepancy on how the CA is designed or is being operated or maintained, and the requirements of this CP or cross-certification agreement, the following actions shall be performed:

- (1) The compliance auditor shall note the discrepancy;
- (2) The compliance auditor shall notify the administration organization of the CA of the discrepancy. If the discrepancy is judged by the administration organization of CA to be severe in nature, the administration organization shall notify the RDEC promptly.

Any CA that has discrepancy shall make corrections according to the compliance audit report and the CP or the provisions of the cross-certification agreement.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the RDEC may decide to halt temporarily operation of the GRCA, revoke the certificate of the subordinate CA issued by GRCA and relevant procedures shall be established by the RDEC.

2.7.6 Communication of results

Except information that may cause attack on the system, information relevant to the trustworthiness of certificates by the relying parties shall be made publicly available.

CA shall publish the latest compliance audit result.

2.8 CONFIDENTIALITY

2.8.1 Types of information to be kept confidential

- (1) Any individual or organization information provided to certificate application is confidential information. Without prior consent from the subscriber or unless otherwise required by applicable law, this information shall not be publicized.
- (2) Private keys and passwords utilized in the operation of CA are all confidential information and shall not be publicized.
- (3) The compliance audit reports shall not be made available as a whole, unless set forth otherwise in Section 2.7.6.

Any CA shall assert in its CPS the types of the confidential information.

2.8.2 Types of information not considered confidential

- (1) Certificates, CRLs and the revocation and suspension information shall not be deemed as confidential information.
- (2) Identification information or information recorded in the certificates, unless statutes or special agreements so dictate, shall not be deemed as confidential information.

Any CA shall assert in its CPS the types of non-confidential information.

2.8.3 Disclosure of certificate revocation/suspension information

Certificate revocation or suspension information is non-confidential information and shall be publicized.

2.8.4 Release to law enforcement officials

Any CA shall specify in its CPS provisions of availability of confidential information in Section 2.8.1 to law enforcement officials.

2.8.5 Release as part of civil discovery

Any CA shall specify in its CPS provisions of availability of confidential information in Section 2.8.1 to civil lawsuit.

2.8.6 Disclosure upon owner's request

Any CA shall specify in its CPS provisions of availability of confidential information in Section 2.8.1 to subscribers.

2.8.7 Other information release circumstances

To be conducted in accordance with the provisions of applicable laws.

2.9 Intellectual Property Rights

The RDEC and Chunghwa Telecom Co., Ltd. (hereinafter abbreviated as Chunghwa Telecom) co-retain all intellectual property rights in and to this CP. This CP can be downloaded from the GRCA repository for free, and can be, to the extent permitted by the Copyright Act, reproduced or distributed for free, and provide intact copy. Those who reproduce or distribute this CP should not charge a fee for this CP itself and should not restrict the access to this CP. In no event will the RDEC and Chunghwa Telecom be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any improper usage or distribution of this CP.

3 IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Types of names

The certificate entity name of the GPKI shall be X.500 distinguished name, DN.

When applying for certificate, any CA has the right to decide on whether to accept the subject alternative name. If the CA requests adding the subject alternative name in the certificate, then that extension shall be marked as a non-critical extension.

3.1.2 Need for names to be meaningful

The subject name of organization and individual shall be in accordance with relevant laws of R.O.C. on that subject name and officially registered name shall be used.

The certificate subject name of device or Server AP shall be the administrator name of that device or Server AP. At the same time, the common name is based on the principle of easy understanding. For example, name of module or sequence number or application process etc.

3.1.3 Rules for interpreting various name forms

Rules established by the RDEC for interpreting name forms shall be contained in the applicable certificate profile.

3.1.4 Uniqueness of names

Name uniqueness across the GPKI must be enforced. The RDEC is

responsible for establishing standards for CAs to use X.500 name space so as to ensure the uniqueness of names. In the CPSs, CAs shall assert how to use the X.500 name space. At the same time, during naming of the subject with same name, CAs shall assert how to ensure the uniqueness of the subject name (for example, in the same county and city, two persons with same name applying for certificate with the CA who shall ensure that these two persons can possess unique subject name).

3.1.5 Name claim dispute resolution procedure

Name ownership shall be processed based on the name rules in relevant laws of R.O.C. (such as Company Law, Name Law and Citizen Education Law etc.). CAs shall assert the dispute solution procedure in the CPSs. There is no stipulation for CAs operating at test level.

In the GPKI, the RDEC is the arbitration authority of name claim dispute.

3.1.6 Recognition, authentication and role of trademarks

No stipulation

3.1.7 Method to prove possession of private key

During application of certificate, any CA shall validate that the private key possessed by the applicant corresponds to the public key asserted in the certificate.

Different key generators shall adopt the following different methods that are recognized by this CP to prove possession of private keys:

(1) When any CA or RA generates key pair for subscribers:

Subscriber is not required to prove possession of private key but is required to accept identity authentication in accordance with provisions in Section 3.1.8, 3.1.9 and 3.1.10 so as to acquire the

private key and the activation data. In addition, private key shall be delivered to subscribers in accordance with the provisions in Section 6.1.2.

- (2) When the trusted third party (such as card issue center) generates key pair for subscribers:

Any CA or RA shall acquire the public key of the subscriber from the trusted third party through secure channel in accordance with the provisions in Section 6.1.3. Subscriber is not required to prove possession of the corresponding private key but the subscriber must accept identity authentication in accordance with the provisions in Section 3.1.8, 3.1.9 and 3.1.10 so as to acquire the private key and the activation data. In addition, the private key shall be delivered to subscribers in accordance with the provisions in Section 6.1.2.

- (3) When the subscriber generates key pair on its own:

Subscriber can use the private key to generate one signature and provide that signature to the CA or RA in accordance with the provisions in Section 6.1.3. Any CA or RA may use the public key of the subscriber to validate that signature so as to prove such subscriber possesses that private key. This CP permits usage of other method with equivalent secure level (such as various methods in RFC 2510 or RFC 2511) to prove the possession of private key.

3.1.8 Authentication of organization identity

In regard to the quantity of certificates required for authenticating the identity of the organization, authentication confirmation procedure and whether the confirmation procedure requires in-person proofing etc.,

there will be different provisions according to different level in the following table:

Assurance level	Identification requirements
Test level	No stipulation.
Level 1	No stipulation.
Level 2	No stipulation.
Level 3	<p>Organization identity authentication can be separated into the following two conditions :</p> <p>(1) Government authority or unit identity authentication:-</p> <p>Government authority or unit shall apply for certificate with official documents and any CA or RA must confirm that such authority or unit actually exists and authenticate the reality of such official documents.</p> <p>(2) Civil organization identity authentication:-</p> <p>Application information shall include the organization name, address and name of the representative etc. that is sufficient to identify that organization. Apart from verifying the application information and the reality of the identity of the representative, any CA or RA shall also verify that the representative has the right to apply for certificate on behalf of that organization. During application, the representative shall come to the CA or RA in person. If the representative cannot apply in person, the representative can use a written power of attorney to</p>

Assurance level	Identification requirements
	<p>consign an agent to apply on its behalf. However, the CA or RA shall confirm the correctness of that power of attorney (such as comparing the seal imprint of the representative on the power of attorney) in accordance with the provisions of Section 3.1.9 for assurance level 3 to authenticate the identity of the agent.</p> <p>The above so-called civil organization refers to private corporation, non-corporation or affiliate organization of the two.</p>
Level 4	<p>Organization identity authentication is separated into the following two conditions:</p> <p>(1) Government authority or unit identity authentication:-</p> <p>Government authority or unit shall use official documents to assign an individual authenticated by the CA or RA to represent that organization or unit to apply for certificate in person. CA or RA shall confirm such authority or unit actually exists and shall validate the reality of the official document and authenticate the identity of the individual of that organization or unit in accordance with the provisions in Section 3.1.9 for assurance level 4.</p> <p>(2) Civil organization identity authentication</p> <p>Application information shall include the</p>

Assurance level	Identification requirements
	<p>organization name, address and the representative name etc. that are sufficient to identify that organization. Apart from verifying the application information and the reality of the identity of the representative, any CA or RA shall also verify that representative has the right to apply for certificate on behalf of that organization. During the application, the representative shall come to the CA or RA in person to process.</p> <p>The above so-called civil organization refers to private corporation, non-corporation or affiliate organization of the two.</p>

For identity authentication of subordinate CAs established by government authority or unit, the GRCA shall process in accordance with the procedure of identity authentication on government authority or unit at assurance level 3 and above.

3.1.9 Authentication of individual identity

In regard to the number of credentials required for individual identity authentication, authentication confirmation procedure and whether the confirmation procedure requires in-person proofing etc., there are different provisions according to different assurance level as follows:

Assurance level	Identification Requirements
Test level	No stipulation

Assurance level	Identification Requirements
Level 1	<p>(1) No written credentials required.</p> <p>(2) Applicant may apply and receive a certificate by providing his or her e-mail address.</p> <p>(3) No need to attend in person.</p>
Level 2	<p>(1) No written credentials required.</p> <p>(2) Subscriber shall submit individual information, such as individual identification number (e.g. identity card no.) and name etc., and it is necessary to conduct comparison with the information approved by the CA.</p> <p>(3) No need to attend in person.</p>
Level 3	<p>(1) Credentials validation:</p> <p>During certificate application, subscriber shall at least show one approved original credential with photo (such as identity card) to the CA or RA to ensure its legitimacy.</p> <p>If the subscriber has no credential as above with attached photo (such as underage person), subscriber can provide written certifying document issued by the government that is sufficient to prove the identity of the subscriber as a substitute (e.g. household register) and one adult with capacity shall guarantee the identity of the subscriber in writing. The identity of the adult presenting the written</p>

Assurance level	Identification Requirements
	<p>guarantee shall go through the above authentication.</p> <p>(2) For the individual information of the subscriber (e.g. identity card number), name and address (e.g. domicile address) etc., comparison shall be conducted with the registered information of that information administrative organization (e.g. domicile information) or the registered information of the trusted third party that is approved by the administrative organization.</p> <p>(3) In-person proofing:</p> <p style="padding-left: 40px;">Identity may be established by in-person proofing before the CA or RA. If the subscriber cannot come in person, he/she can use a written power of attorney to consign an agent to apply in person on his/her behalf. However, the CA or RA shall confirm the correctness of that power of attorney (such as comparing the seal imprint of the subscriber on the power of attorney) and shall base on the above provision to authenticate the identity of the agent.</p>
Level 4	<p>(1) Credentials validation:</p> <p style="padding-left: 40px;">Credentials required are at least one approved original credential with photo (e.g. identity card) to CA or RA to ensure its legitimacy.</p> <p>(2) For the individual information of the subscriber</p>

Assurance level	Identification Requirements
	<p>(e.g. identity card number), name and address (e.g. domicile address) etc., comparison shall be conducted with the registered information in the administrative organization (e.g. domicile information).</p> <p>(3) Identity may be established by in-person proofing, before a CA or RA.</p>

3.1.10 Authentication of Component Identities

Some computing and communications components (e.g. routers, firewalls, servers etc.) will be named as certificate subject. In such cases, the component must have a human sponsor. The sponsor, an organization or an individual, shall apply for certificate application as a component administrator . Identity authentication shall be processed in accordance with the provisions in Section 3.18 and 3.19.

The sponsor is responsible for providing the following registration information:

- (1) Equipment or Server AP identification.
- (2) Equipment or Server AP public keys (in accordance with the provisions in Section 6.1.3)
- (3) Equipment or Server AP authorizations and attributes (if any are to be included in the certificate).
- (4) Contact information to enable the CA or RA to communicate with the sponsor

3.2 CERTIFICATE RENEWAL AND ROUTINE RE-KEY

3.2.1 Routine Rekey

Re-keying a certificate means that a new certificate that has the same characteristics and level as the old one is created. In addition, the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

When the subordinate CA re-keys the key pair, the CA that issues the certificate to the subordinate CA shall conduct identification and authentication in accordance with the provisions in Section 3.1.

Subscribers of subordinate CAs shall identify themselves for the purpose of re-keying as required in the table below.

Assurance level	Routine Rekey Identity Requirements for Subscriber Signature and Encryption Certificates
Test level	No stipulation.
Level 1	Identity may be established through use of current signature key.
Level 2	Identity may be established through use of current signature key, except that identity shall be re-established through initial registration process if the latest registration is over 15 yrsrs ago based on the provisions in Section 3.1.

Assurance level	Routine Rekey Identity Requirements for Subscriber Signature and Encryption Certificates
Level 3	Identity may be established through use of current signature key, except that identity shall be re-established through initial registration process if the latest registration is over 9 yrs ago based on the provisions in Section 3.1.
Level 4	Identity may be established through use of current signature key, except that identity shall be re-established through initial registration process if the latest registration is over 3 yrs ago based on the provisions in Section 3.1.

3.2.2 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number. A certificate may be extended if the certificate key pair has not reached the end of its validity period (based on the provisions in Section 6.3.2) and the private key has not been compromised, and the Subscriber name and attributes are unchanged.

Certificates of CAs cannot be renewed. Only certificates of subscribers can be renewed and the current signature key can be used to conduct authentication.

3.3 Rekey after Revocation

After the certificate has been revoked other than renewal or update, subscriber is required to go through the initial registration described in Section 3.1 to obtain a new certificate.

3.4 REVOCATION REQUEST

Revocation requests must be authenticated by a CA or RA. The CA or RA shall assert the authentication method in the CPS in accordance with the provisions in Section 4.4 so as to confirm that the applicant is the entity who has the right to submit certificate revocation.

Requests to revoke a certificate may be authenticated with certificate's associated private key, regardless of whether or not the private key is compromised.

4 OPERATIONAL REQUIREMENTS

4.1 Certificate Application

CAs must assert the application procedure for initial registration, certificate renewal and certificate re-key, application address or website in the CPSs..

The GRCA is required to accept application of CAs established based on e-government electronic certification service divisional responsibility so that these CAs can be the first level subordinate CAs of the GPKI. Its application procedure shall be specified separately by the RDEC and will be published in the CPS of the GRCA.

The procedure of applying for cross-certificate with the GRCA by CAs outside the GPKI shall be specified separately by the RDEC.

Unless otherwise agreed by its upper level CA, subordinate CAs of all levels in the GPKI cannot accept application from other CAs to become its lower level CA.

4.2 Certificate Issuance

Issuance of certificate by any CA shall be conducted in accordance with the provisions in Section 5.2 and the CPS and appropriate personnel shall execute the task of certificate issuance. After the certificate is issued, CA or RA shall notify the applicant in appropriate ways. CAs operating at assurance level 1, 2, 3 and 4 shall assert methods of notifying applicant after the certificate is issued in the CPSs.

If any CA or RA disagrees on the issuance of certificate, the applicant shall be notified in appropriate ways and the reason of disagreement on the issuance shall be advised. In addition to identity

identification and authentication of the applicant, the CA can disagree on the issue of certificate with other reason. CAs operating at assurance level 1, 2, 3 and 4 shall assert the method of notifying applicants on disagreement on the issuance of certificate in the CPSs.

The GRCA shall issue a self-signed certificate. After the RDEC has confirmed that the content of this certificate is correct, it will be delivered to the relying party in accordance with the provisions in Section 6.1.4.

4.3 Certificate Acceptance

After the issuance of certificate by CAs at assurance level 2, 3 and 4 and the applicant has examined the content and accepted the issued certificate, only by then can the issued certificate be published in the repository. After examination on the content, if the applicant refuses to accept the certificate, then the CA shall revoke that certificate. CAs operating at assurance level 2, 3 and 4 shall assert the followings in the CPSs:

- (1) Method of confirming accepting or refusing the certificate by the applicant.
- (2) Examination on the certificate fields by the applicant before deciding on accepting the certificate.
- (3) Certificate refusal process by the applicant.

Before deciding on accepting the certificate, the above applicant shall examine the certificate fields, at least on the subject name. For the refusal process of accepting the certificate by the applicant, if there is fee collection or refund problem, it shall be specified based on the Consumer Protection Law and fair trade principle.

The self-signed certificates of the GRCA may only be disseminated

to relying parties in accordance with the provisions in Section 6.1.4 after the RDEC has confirmed its content.

4.4 Certificate Suspension and Revocation

Except CAs operating at test level, other CAs shall provide certificate revocation service. CAs may decide whether suspension service shall be provided in accordance with the certificate applicability and service quality.

For certificate suspension and revocation, CAs shall comply with the following provisions:

(1) CAs operating at assurance level 1 and 2 shall at least provide certificate revocation service within the legitimate office hours of the government authority.

(2) For CAs operating at assurance level 3 and 4, the certificate suspension and revocation service shall comply with one of the following provisions:

A. providing around-the-clock certificate revocation service.

B. providing around-the-clock certificate suspension service.

CAs that provide certificate revocation and suspension service shall assert the method of service to be provided, certificate revocation application procedure, application address, and website in the CPS.

After the certificate is revoked and suspended, at the latest, during the next publication of CARL/CRL, the CA shall include the revoked and suspended certificate in the CARL/CRL and posted it in the repository. The published certificate status information shall include revoked and suspended certificates until these certificates are due or reinstated.

4.4.1 Circumstances for revocation

There are three circumstances under which certificate may be revoked:

- (1) If the private key of a subscriber is proven or being suspicious of compromise (e.g. loss of IC card that the private key of the subscriber is stored).
- (2) If there is proof that the private key of the CA is compromised, then the certificate issued based on that private key shall be revoked.
- (3) If there is change on the subscriber information or attribute of the certificate (e.g. change in subscriber's name, certificate number or code, disappearance of subscriber identity due to disbandment or death). However, if the subject data recorded in the certificate of the CA needs to be changed, the RDEC shall evaluate whether the certificate shall be revoked.

Except the above circumstances that the certificate needs to be revoked, within the duration of the certificate, subscriber can submit certificate revocation application due to other reasons.

If any CA or RA proves that the subscriber has violated this CP or the subscriber obligation provided in the CPS, the CA can directly revoke the certificate of that subscriber.

If any CA proves or is suspicious that its own private key has been compromised, the CA may directly revoke all certificates issued with that private key.

If any upper level CA proves that any lower level CA violates the CP/CPS, then the CA may directly revoke the certificate of that lower

level CA.

If any CA proves that its cross-certification CA violates the CP/CPS, the CA can directly revoke the cross-certification of that CA.

If the RDEC decides that the self-signed certificate of the GRCA needs to be revoked (e.g. suspicion that the private key of GRCA is compromised), the RDEC can directly revoke the self-signed certificate of the GRCA.

4.4.2 Who can request revocation

When the certificate has to be revoked due to circumstances in Section 4.4.1 or other circumstances, the subscriber or entity in possession of private key may submit the certificate revocation application to the CA or RA within the duration of the certificate.

CAs can directly revoke the certificates of subscribers, subordinate CAs or cross-certification CAs in accordance with the provisions in Section 4.4.1.

4.4.3 Procedure for revocation request

Upon receipt of a revocation request, any CA or RA shall authenticate the applicant's identity in accordance with the provisions in Section 3.4 and the CPS. If the authentication is found correct, in principle, CA or RA shall approve its application unless the private key of CA is compromised.

If the certificate revocation application is agreed upon or the certificate revocation is conducted directly, CAs or RAs shall revoke the certificate in accordance with the provisions in Section 5.2 and the CPS. After the certificate is revoked, the CA or RA shall notify the subscriber

by appropriate means. CAs operating at assurance level 1, 2, 3 and 4 shall assert the method of notifying subscriber after the certificate is revoked in the CPS.

If the certificate revocation is not agreed upon, then the CA or RA shall notify the subscriber by appropriate means and advise the subscriber on the reason of disagreement on the revocation. CAs operating at assurance level 1, 2, 3 and 4 shall assert the method of notification on disagreeing on the certificate revocation in the CPS.

4.4.4 Revocation request grace period

CAs shall assert the processing period for certificate revocation request in the CPSs.

4.4.5 Circumstances for suspension

Depending on requirement, CAs can provide service of certificate suspension. The relevant provision shall be asserted in the CPS.

4.4.6 Who can request suspension

To be asserted in the CPSs of subordinate CAs that provide certificate suspension service.

4.4.7 Procedure for suspension request

To be asserted in the CPS of subordinate CAs that provide certificate suspension service.

4.4.8 Limits on suspension period

CAs shall assert the processing period of the request for certificate suspension and the period of the suspended certificate in the CPSs.

4.4.9 CARL/CRL issuance frequency

GRCA shall issue the CARL(certificate authority revocation lists) and subordinate CAs shall issue the CARLs/CRLs(certificate revocation lists). The contents of CARLs/ CRLs shall be checked before its issuance to ensure that all information is correct. This may be processed by software which scans the CARLs/CRLs looking for any evidence of an improperly manufactured CARL/CRL. CARL/CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation. CAs shall coordinate with the repositories to which they post certificate information to reduce latency between creation and availability. The CPS shall specify which repository is the main one for subscriber to obtain the latest certificate status information.

Expired certificate status information shall be removed from the repository system upon posting of the latest certificate status information. The following table provides CARL/CRL issuance requirements.

Assurance level	CARL Issuance Frequency	CRL Issuance Frequency
------------------------	--------------------------------	-------------------------------

Assurance level	CARL Frequency	Issuance	CRL Frequency	Issuance
Test level	Not applicable		No stipulation	
Level 1	Not applicable		No stipulation	
Level 2	Not applicable		At least once every three days	
Level 3	At least once each day		At least once each day	
Level 4	At least once each day		At least once each day	

4.4.10 CARL/CRL Checking Requirements

Any relying party who uses certificate at assurance level 2, 3 and 4 shall inquire on the present CARL/CRL before usage of his/her certificate so as to check the present status of the certificate. At the same time, it is necessary to verify the correctness and the integrity of the CARL/CRL. Any relying party shall consider the risk, responsibility and consequences for using a certificate and shall decide on its own the interval to obtain the new certificate revocation information. The relevant obligation is as the provision in Section 2.1.4.

4.4.11 On-line revocation/status checking availability

In addition to provision of CARLs/CRLs, CAs may optionally provide on-line certificate status checking to relying parties. Subscribers using on-line certificate status inquiry need not obtain or process CARLs/CRLs. Any CA shall assert whether it will provide or how to provide on-line status checking of certificates in the CPS.

4.4.12 On-line revocation checking requirements

If any relying party using assurance level 2, 3 and 4 certificate does not check the CARLs/CRLs, then he/she can confirm the certificate status by means of on-line status checking.

4.4.13 Other forms of revocation advertisements available

No stipulation.

4.4.14 Checking requirements for other forms of revocation advertisements

No stipulation.

4.4.15 Special requirements to Key Compromise

When the key is compromised, please process in accordance to relevant provisions in Section 4.4.1, 4.4.2 and 4.4.3.

4.5 Security Audit Procedures

CAs operating at test level do not possess security audit capability. CAs that issue certificates of other assurance level shall possess appropriate security audit logs on security events. Audit log files shall be generated for all events via the system automatically. If it cannot be generated by the system, then logbook, paper form or other physical mechanism can be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audit. The security audit logs for each auditable event shall be maintained in accordance with *Retention Period for Archive*, Section 4.6.2.

4.5.1 Types of event recorded

All security auditing capabilities of CAs shall include the security audit on the management system and its operation system. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- (1) The type of event.
- (2) The identity of the entity and/or operator that caused the event.
- (3) The place or position the event occurred.
- (4) The date and time the event occurred.
- (5) A success or failure indicator when performing certificate issuance or revocation by any CA.

When event occurs, CA can decide on its own whether the audit log is to be recorded in digital or physical form. The following explains the auditable events that shall be recorded by CA operating based on various assurance levels. As these auditable events require recording or responding processing by CA, therefore it is also called as auditable event:

Auditable Event/assurance level	Level 1	Level 2	Level 3	Level 4
A.1 SECURITY AUDIT				
A.1.1 Any change to the audit parameters, e.g., audit frequency, type of event audited and new and old parameters content etc.		✓	✓	✓

Auditable Event/assurance level	Level 1	Level 2	Level 3	Level 4
A.1.2 Any attempt to delete or modify the audit logs		✓	✓	✓
A.2 IDENTIFICATION AND AUTHENTICATION				
A.2.1 Successful and unsuccessful attempts to assume a role		✓	✓	✓
A.2.2 Change in the value of maximum authentication attempts		✓	✓	✓
A.2.3 Maximum number of unsuccessful authentication attempts during user login		✓	✓	✓
A.2.4 An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		✓	✓	✓
A.2.5 An administrator changes the type of authenticator, e.g. from password to biometrics		✓	✓	✓
A.3 KEY GENERATION				
A.3.1 Whenever any CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	✓	✓	✓	✓
A.4 PRIVATE KEY LOAD AND STORAGE				

Auditable Event/assurance level	Level 1	Level 2	Level 3	Level 4
A.4.1 The loading of private keys to components	✓	✓	✓	✓
A.4.2 All access to private keys of certificate subjects retained within CAs for key recovery purpose	✓	✓	✓	✓
A.5. TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE				
A.5.1 All changes to the trusted public keys, including additions and deletions	✓	✓	✓	✓
A.6. PRIVATE KEY EXPORT				
A.6.1 The export of private keys (keys used for a single session or message are excluded)	✓	✓	✓	✓
A.7. CERTIFICATE REGISTRATION				
A.7.1 All certificate requests	✓	✓	✓	✓
A.8. CERTIFICATE REVOCATION				
A.8.1 All certificate revocation requests		✓	✓	✓
A.9. CERTIFICATE STATUS CHANGE APPROVAL				
A.9.1 The approval or rejection of a certificate status change request		✓	✓	✓
A.10. GRCA OR SUBORDINATE CA CONFIGURATION				
A.10.1 Any security-relevant changes to the configuration of CA		✓	✓	✓

Auditable Event/assurance level	Level 1	Level 2	Level 3	Level 4
A.11. ACCOUNT ADMINISTRATION				
A.11.1 Roles and users are added or deleted	✓	✓	✓	✓
A.11.2 The access control privileges of a user account or a role are modified	✓	✓	✓	✓
A.12. CERTIFICATE PROFILE MANAGEMENT				
A.12.1 All changes to the certificate profile	✓	✓	✓	✓
A.13. CARL/CRL PROFILE MANAGEMENT				
A.13.1 All changes to the CARL/CRL profile		✓	✓	✓
A.14. MISCELLANEOUS				
A.14.1 Installation of the operation system		✓	✓	✓
A.14.2 Installation of the CA system		✓	✓	✓
A.14.3 Installing hardware cryptographic modules			✓	✓
A.14.4 Removing hardware cryptographic module			✓	✓
A.14.5 Destruction of hardware cryptographic module		✓	✓	✓
A.14.6 System startup		✓	✓	✓
A.14.7 Login attempts to CA Apps		✓	✓	✓

Auditable Event/assurance level	Level 1	Level 2	Level 3	Level 4
A.14.8 Receipt of hardware/ software			✓	✓
A.14.9 Attempt to set passwords		✓	✓	✓
A.14.10 Attempt to modify passwords		✓	✓	✓
A.14.11 Backing up CA internal database		✓	✓	✓
A.14.12 Restoring CA internal database		✓	✓	✓
A.14.13 File manipulation (e.g. creation, renaming, moving etc.)			✓	✓
A.14.14 Posting of any material to a repository			✓	✓
A.14.15 Access to CA internal database			✓	✓
A.14.16 All certificate compromise notification requests		✓	✓	✓
A.14.17 Loading tokens with Certificates			✓	✓
A.14.18 transmission of Tokens			✓	✓
A.14.19 Zeroizing tokens		✓	✓	✓
A.14.20 Rekey of the CA	✓	✓	✓	✓
A.15. CONFIGURATION CHANGES TO THE CA SERVER				
A.15.1 Hardware		✓	✓	✓

Auditable Event/assurance level	Level 1	Level 2	Level 3	Level 4
A.15.2 Software		✓	✓	✓
A.15.3 Operating system		✓	✓	✓
A.15.4 Patches		✓	✓	✓
A.15.5 Security profiles			✓	✓
A.16. PHYSICAL ACCESS/SITE SECURITY				
A.16.1 Personnel access to room housing CA			✓	✓
A.16.2 Access to the CA server			✓	✓
A.16.3 Known or suspected violations of physical security		✓	✓	✓
A.17. ANOMALIES				
A.17.1 Software error conditions		✓	✓	✓
A.17.2 Software check integrity failures		✓	✓	✓
A.17.3 Receipt of improper message			✓	✓
A.17.4 Misrouted message			✓	✓
A.17.5 Network attacks (suspected or confirmed)		✓	✓	✓
A.17.6 Equipment failure	✓	✓	✓	✓
A.17.7 Electrical power outages			✓	✓
A.17.8 Uninterruptible power			✓	✓

Auditable Event/assurance level	Level 1	Level 2	Level 3	Level 4
supply (UPS) failure				
A.17.9 Obvious and significant network service or access failures			✓	✓
A.17.10 Violations of certificate policy	✓	✓	✓	✓
A.17.11 Violations of certification practice statement	✓	✓	✓	✓
A.17.12 Resetting operating system clock		✓	✓	✓

4.5.2 Frequency of processing log

Audit logs shall be reviewed in accordance to the table below and all significant events shall be explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation on any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

Assurance level	Review Audit Log
Test level	No stipulation
Level 1	No stipulation
Level 2	No stipulation
Level 3	At least once every two months. significant security audit records generated by CAs since the last review shall be examined, as well as a

Assurance level	Review Audit Log
	reasonable search for any evidence of malicious activity
Level 4	At least once per month. significant security audit records generated by CAs since the last review shall be examined, as well as a reasonable search for any evidence of malicious activity

4.5.3 Retention period for audit log

No stipulation for CAs operating at test level and level 1.

For CAs operating at assurance level 2, 3 and 4, the audit logs shall be retained on site for at least two months and shall be processed based on provisions of record retention management system in Section 4.5.4, 4.5.5, 4.5.6 and 4.6.

When the retention period of the audit log expires, if that data needs to be removed, it shall be done by the security auditor instead of other personnel.

4.5.4 Protection of audit log

No stipulation for CAs operating at test level and level 1.

For CAs operating at level 2, 3 and 4, the Electronic Audit Log System shall include the protection system. Manual security audit data shall also be protected so as to ensure that it will not encounter unauthorized reading access, modification and deletion.

4.5.5 Audit log backup procedures

Assurance level	Security audit data backup procedure
Test level	No stipulation
Level 1	
Level 2	Audit logs and audit summaries shall be backed up at least monthly.
Level 3	
Level 4	Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site in accordance with the CPS on a monthly basis.

4.5.6 Audit collection system

The audit system may or may not be external to the CA system. Audit processes shall be invoked at system startup, and cease only at system shutdown.

Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then it is necessary to determine whether to suspend the CA operation until the problem is remedied.

4.5.7 Notification to event-causing subject

When an event occurs and is recorded by the audit system, the audit system is not required to advise the entity who caused that event that such event has been recorded.

4.5.8 Vulnerability assessments

No stipulation for CAs operating at test level, level 1 and level 2. CAs operating at assurance level 3 and 4 shall execute routine security control vulnerability assessment.

4.6 Records Archival

4.6.1 Types of event recorded

According to security requirement of various assurance levels, the following data shall be archived (no stipulation for CAs operating at test level).

Data To Be Archived/ Assurance Level	Level 1	Level 2	Level 3	Level 4
CA accreditation (if applicable)	✓	✓	✓	✓
Certificate practice statement	✓	✓	✓	✓
Contractual obligations	✓	✓	✓	✓
System and equipment configuration	✓	✓	✓	✓
Modifications and updates to system or configuration	✓	✓	✓	✓
Certificate requests	✓	✓	✓	✓
Revocation requests		✓	✓	✓
Subscriber identity authentication data as per Section 3.1.9		✓	✓	✓
Documentation of receipt and		✓	✓	✓

Data To Be Archived/ Assurance Level	Level 1	Level 2	Level 3	Level 4
acceptance of certificates				
Documentation of receipts of tokens		✓	✓	✓
All certificates issued or published	✓	✓	✓	✓
Record of CA changeover	✓	✓	✓	✓
All CARLs and CRLs issued and/or published		✓	✓	✓
All audit logs	✓	✓	✓	✓
Other data or applications to verify archive contents		✓	✓	✓
Documents required by the compliance auditors		✓	✓	✓

4.6.2 Retention period for archive

The minimum retention periods for archive data are as follows:

Assurance Level	Minimum Retention Period
Test level	No stipulation
Level 1	Three years
Level 2	Five years
Level 3	Ten years
Level 4	Twenty years

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archived data shall also be maintained for a certain period determined by the administrative organization of that CA.

Prior to the end of the archive retention period, CAs shall provide the archived data and the application necessary to read the archives to the administrative organization.

4.6.3 Protection of archive

No stipulation for archived data protection for CAs operating at test level and level 1.

For CAs operating at assurance level 2, 3 and 4, the archive data shall be stored in a safe, secure storage facility separated from the sites of CAs. The level of protection shall not be lower than the protection level of that CA.

4.6.4 Archive backup procedures

No stipulation

4.6.5 Requirements for time-stamping of records

No stipulation.

4.6.6 Archive collection system

No stipulation.

4.6.7 Procedures to obtain and verify archive information

Procedures detailing how to create, verify, package, transit and store the archive information shall be published in the CPS.

4.7 Key changeover

4.7.1 Key Changeover of CA

Private key of CA shall be changed periodically in accordance with the provisions in Section 6.3.2.

If the certificate of CA itself is revoked, the usage of its private key shall be suspended and the key pair shall be changed.

At the latest, three months before the self-signed certificate is due, the GRCA shall change the key pair for issuance of certificate and a new self-signed certificate shall be issued. After the content is confirmed by the RDEC, the new self-signed certificate shall be delivered to the relying party in accordance with the provisions in Section 6.1.4.

At the latest, two months before the self-signed certificate is due, the subordinate CA shall change the key pair for issuance of certificate and a new self-signed certificate shall be issued. After the subordinate CA has changed the key pair, new certificate shall be applied with upper CA in accordance with the provisions in Section 4.1.

4.7.2 Key Changeover of Subscriber

Private keys of subscribers shall be changed periodically in accordance with the provisions in Section 6.3.2.

After the certificate of the subscriber is revoked, usage of its private key shall be suspended. In addition, after the changeover of key pair, new certificate shall be applied from CA or RA in accordance with the provisions in Section 4.1.

If the certificate of any subscriber at assurance level 2, 2 has not been revoked, at the latest the subscriber has to change its key pair within one month before certificate is due and the subscriber shall apply for new certificate with CA or RA in accordance with the provisions in Section 4.1.

4.8 Compromise and Disaster Recovery

For disaster recovery of any CA, priority shall be given to recover the repository so as to generate certificate status information.

4.8.1 Computing resources, software, and/or data are corrupted

To fulfill the objective of continual operation, CAs shall perform various backup measures in accordance with the provisions of CP and CPS so as to reduce damages on computer resources, software or data to a minimum and to rapidly restore the certificate issuance and management operation.

CA operating at assurance level 3 and 4 shall at least conduct one exercise each year on corruption of computer resource, software and data.

4.8.2 Entity public key is revoked

CAs operating at assurance level 2, 3 and 4 shall assert the recovery

procedure in the CPS or relevant documents in the event that the signature keys of CAs are revoked so as to rapidly restore the certificate issuance and management operation capability.

CAs operating at assurance level 3 and 4 shall at least conduct one exercise each year on revocation of signature keys.

4.8.3 Entity key is compromised

CAs operating at assurance level 2, 3 and 4 shall assert the recovery procedure in the CPS after the signature key of the CA is compromised so as to rapidly restore the certificate issuance and management operation capability.

CAs operating at assurance level 3 and 4 shall conduct one exercise every year on signature key compromise.

4.8.4 Secure facility after a natural or other type of disaster

CAs operating at assurance level 2, 3 and 4 shall assert the steps of reestablishing the secure facilities of CAs after natural or other disaster in the CPS or relevant documents.

CAs operating at assurance level 3 and 4 shall at least conduct one exercise every year on the disaster recovery.

4.9 CA Termination

The termination service of CAs shall be conducted in accordance with relevant provisions of the Electronic Signature Act.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

No stipulation for CAs operating at test level and level 1. The location and construction of the facility housing the CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location, when combined with other physical security protection mechanisms such as door securities, guards and intrusion sensors and surveillance videos shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical access

No stipulation for CAs operating at test level and level 1. For CAs that operate on assurance level 2 and above, their equipment shall always be protected from unauthorized access, and especially while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tempering even when the cryptographic module is not installed and activated.

The physical security requirements for CAs operating at various assurance levels are as follows:

Physical security requirements for CAs operating at assurance level 1 and 2:

(1) Ensure no unauthorized access to the hardware is permitted.

(2) Ensure all movable media and paper containing sensitive plain-text information are stored in secure sites.

Physical security requirements for CAs operating at assurance level 3 and 4:

(1) Be manually or electronically monitored for unauthorized intrusion at all times.

(2) Ensure an access log is maintained and inspected periodically.

(3) Require two-person physical access control to both the cryptographic module and computer system.

As the GRCA is required to sign certificates for all assurance levels, therefore the security system of the equipment environment shall be in accordance with the provision of physical control of assurance level 4. For physical control on CA operating at test level, provision shall not be provided but shall be explained in the CPS.

A security check of the facility housing the CA equipment shall be taken in case that the facility is left unattended. At a minimum, the check shall verify the following:

(1) Any security container is properly secured.

(2) Physical security systems (e.g. door locks, door securities) are functioning properly.

5.1.3 Power and air conditioning

No stipulation for CAs operating at test level and level 1. CAs

operating at level 2 and higher shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. At the same time, uninterrupted power supply system that can provide at least six hours and more of emergency power supply shall be installed so that the repository can backup data (including issued certificates and CRLs).

5.1.4 Water exposures

The establishment location of any CA shall be free from water exposures.

5.1.5 Fire prevention and protection

No stipulation for CAs operating at test level and level. CAs operating at assurance level 2 and higher shall install automatic fire detection and pre-alert system that can automatically activate fire extinguishing equipment. Manual switches shall be installed in various main entrances so that site personnel can operate manually during emergency.

5.1.6 Media storage

No stipulation for CAs operating at test level and level 1. Media of CAs operating at assurance level 2 shall be protected so as to prevent it from accidental damage (water, fire, electromagnetic).

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

No stipulation for CAs operating at test level and level 1. For CAs operating at assurance level 2 and higher, backups are to be performed and stored off-site not less than once per week. Other periodical scheduling shall be asserted in the CPS.

Location of off-site backup shall be away from the CA equipment room at least 30 km and more. Backup contents shall at least contain data and system program. When there is abnormal condition, the backup facility shall be able to restore the system back to normal. The off-site backup system shall have similar security level as the CA.

5.2 Procedural Controls

5.2.1 Trusted roles

CAs shall arrange trusted roles to be responsible for executing tasks as the basis of reliability of the CA. If the security objective cannot be fulfilled due to accident or human negligence, then the impartiality of CAs may be reduced. Two approaches are taken to increase the likelihood that these roles can be successfully carried out:

- (1) Ensure that the person filling the role is trustworthy and properly trained.
- (2) Distributes the functions among more than one person so that any malicious activity would require collusion.

The provided trusted roles are as follows:

- (1) Administrator: authorized to install, configure and maintain the

CA; establish and maintain user accounts; configure profiles and audit parameters; and generate components keys.

(2) Officer: authorized to request or approve certificates or certificate revocation.

(3) Auditor: authorized to view and maintain audit logs.

(4) Operator: authorized to perform system backup and recovery.

5.2.1.1 Administrator

The administrator is responsible for:

(1) installation, configuration and maintenance of the CA;

(2) establishing and maintaining CA system accounts;

(3) configuring certificate profiles or templates and audit parameters;

(4) generating and backing up CA keys.

5.2.1.2 Officer

The officer is responsible for:

(1) registering new subscribers and requesting the issuance of certificates;

(2) verifying the identity of the subscribers and accuracy of information included in certificates;

(3) approving and executing the issuance of certificates;

- (4) requesting, approving and executing the revocation of certificates.

5.2.1.3 Auditor

The auditor is responsible for:

- (1) reviewing, maintaining, and archiving audit logs;
- (2) performing or overseeing internal compliance audits to ensure that CA is operating in accordance with its CPS;

5.2.1.4 Operator

The operator is responsible for:

- (1) physical security control of the system (such as door security management of the equipment room, fire prevention, flood prevention and air conditioning system etc.);
- (2) daily operation and maintenance of the system equipment;
- (3) system backup and recovery operation;
- (4) Storage media renewal;
- (5) system software and hardware update;
- (6) network and website maintenance: establishing system security and virus protection system and network security event detection and reporting etc.

5.2.2 Allocation of roles

The principle of allocation of roles for CAs shall be as follows:

Assurance level	Role allocation Rules
Test level	No stipulation
Level 1	No stipulation
Level 2	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, one individual shall not assume both the Officer and Administrator roles.
Level 3	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, an individual who assumes an Officer role may not assume an Administrator or Auditor role.
Level 4	<p>Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Personnel and role separation shall comply with the following provisions:</p> <p>(1) Individuals may assume only one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role.</p> <p>(2) Any one role is not permitted to execute self audit.</p>

5.2.3 Number of persons required per task

To best ensure the integrity of the CA equipment and operation, role arrangement shall be in accordance with the provisions in Section 5.2.2. The number of persons required per task shall be asserted in the CPS.

5.2.4 Identification and authentication for each role

At all assurance levels other than test level and level 1, an individual shall identify and authenticate him/herself before being permitted to

perform any action set forth for that role or identity.

5.3 Personnel Controls

CAs shall accurately master all personnel who perform the operation of CAs or RAs. The security control on the task assignment of personnel shall conform to the following provisions:

- (1) Assign tasks in writing.
- (2) Use law or contract to specify the terms of performing tasks.
- (3) Receive training on the mission.
- (4) Use law or contract to specify that sensitive information and subscribers' information cannot be disclosed.
- (5) The assigned task shall conform to the principle of declining interests and benefits.

5.3.1 Background, qualifications, experience, and clearance requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be citizen of Republic of China. The requirements governing the qualifications, selection and oversight of individuals and audit shall be set forth in the CPS.

5.3.2 Background check procedures

Background check procedures shall be asserted in the CPS.

5.3.3 Training requirements

All personnel performing duties with respect to the operation of CA shall receive comprehensive training. Training shall be conducted in the following areas:

- (1) CA/RA security principles and mechanisms.
- (2) All PKI software versions in use on the CA system.
- (3) All PKI duties they are expected to perform.
- (4) Disaster recovery and business continuity procedures.

5.3.4 Retraining frequency and requirements

All personnel of CA shall be aware of changes in the work procedures and regulations. Any significant change to the operations shall have a retraining and the execution of such retraining shall be documented. Examples of such changes are CA software or hardware upgrade, changes in work procedure and equipment replacement etc.

New employees shall be processed as above and each year CAs shall check on the training condition of personnel.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

CAs shall specify proper administrative method in the CPS so as to prevent personnel from accessing data without authorization. CAs shall

take appropriate administrative and disciplinary actions against personnel who have violated provisions in the CP or CPS.

Appropriate administration and disciplinary actions shall be taken against any personnel who have performed actions in the GRCA or its repository not authorized in this CP or CPS, or other procedures published by the GRCA.

5.3.7 Contracting personnel requirements

Contractor personnel employed to perform functions pertaining to CAs shall meet applicable requirements set forth in the CPS of CAs.

5.3.8 Documentation supplied to personnel

CA shall make available to its CA and RA personnel the certificate policies it support, relevant parts of the CPS, and any relevant statutes, policies or contracts.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Cryptographic module used in the certificate issued by CAs is required to go through the cryptographic module of equivalent security level approved by the RDEC to generate the key.

For the random numbers adopted in the generation of key, even if the length and the degree of such random numbers can provide sufficient data and equipment, the similar random number array is computationally infeasible.

The private key stored in the cryptographic module shall be prevented from its disclosure from its cryptographic module. If the private key is generated inside the cryptographic module, that key shall be continuously kept in the cryptographic module or shall be encrypted and stored in the mainframe. If the private key is generated outside of the cryptographic module, that key shall not be transmitted to the cryptographic module without leaving the key generation environment. That environment shall guarantee that no person can obtain the generated private key with any method and under any un-detectable condition. When the private key is stored in the cryptographic module, that key shall be immediately removed from the key generation environment.

Any CA shall adopt appropriate measures to ensure that the public key of the subscriber is the only one in the PKI under the jurisdiction of

that CA.

6.1.2 Private key delivery to entity

If the private key is being generated and stored inside the cryptographic module of the subscriber, delivery of such private key is not needed.

If the private key is directly generated by the token owned by the entity (such as the certificate subscriber or IC card issuance center) or after another key producer has generated the key, then such key is delivered to the token of that entity. During the generation of the private key and its receipt, such entity shall be deemed as possession of that private key. However, if the above entity is not the certificate subject of the applied certificate, then the private key shall be delivered to the certificate subject by means of secure method that can be audited so as to complete the transfer of the private key.

For all assurance levels, when the hardware is transmitting delivering the stored key to subscriber, it is necessary to deliver the correct token and its activation data to the subscriber. Any CA shall maintain a copy of record confirming that the subscriber has received that token. When using any mechanism including confidentiality co-sharing (such as password or PIN number), then that system shall ensure that only the applicant or GRCA or the subordinate CA is the only entity possessing that secret.

If the private key is generated by the CA or RA or trusted third party, then this cryptographic module shall be delivered to the subscriber securely. Subscriber shall confirm the receipt of the private key. The

storage position and the tracing record of the status of the cryptographic module shall be kept properly till at least the subscriber has confirmed the receipt of that cryptographic module.

Under any circumstance, other person cannot acquire or control the signature private key except the subscriber. Any entity generating the signature private key for subscriber cannot retain the duplicate of that key.

6.1.3 Public key delivery to certificate issuer

When any CA is performing identity authentication on subscriber, subscriber shall delivery its public key to that CA and the delivery methods are as follows:

- (1) Via a certificate electronic request message from a RA.
- (2) When the key is generated by a third party, CA or RA shall acquire the public key of the subscriber via secure channel that can be audited.
- (3) Can be done via other secure electronic mechanism.
- (4) Can be done via secure and non-electronic means. These means may include, but not limited to, floppy disk (or other storage medium) sent via registered mail or courier.

6.1.4 CA public key delivery to users

The public key of GRCA can be acquired at any time. The subordinate CA shall deliver the self-signed certificate of the GRCA or the public key to the user. Reliable certificate delivery means are as follows:

- (1) The CA shall store the self-signed certificate of the GRCA or public key with token and deliver this to the relying party with secure means.
- (2) Deliver the self-signed certificate of the GRCA or public key via out-of-band channel.
- (3) Deliver the self-signed certificate of the GRCA or the random numbers of the public key or fingerprint for user to compare (the random numbers published in-band or fingerprint shall not be deemed as qualified secure channel).
- (4) Download the self-signed certificate of the GRCA or the public key from website with similar level or even higher secure assurance level.
- (5) Other means approved by the RDEC.

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

Certificate of the subordinate CA issued by the GRCA shall be published in the repository of that CA.

6.1.5 Key sizes

Assurance level	Symmetrical key	Public key
------------------------	------------------------	-------------------

Assurance level	Symmetrical key	Public key
Assurance level	Shall at least possess 3-DES (3 Keys) or other types of key with similar security (such as AES 128	Shall at least use 1024 bit RSA key or other types of key with similar security (such as ECC 161
Level 1	bit).	
Level 2		
Level 3		
Level 4		Shall at least use 2048 bit RSA key or other types of key with similar security (such as ECC 224 bit).

6.1.6 Public key parameters generation

In regard to RSA algorithms, public key parameters shall be null. For other algorithms, public key parameters shall base on relevant international standards.

6.1.7 Parameter quality checking

In regard to RSA algorithms, it is not necessary to check the parameter quality. However, prime number test is required. CAs shall describe how to perform relevant test in the CPS.

For other algorithms, it shall be based on relevant international standards and shall include prime number test.

6.1.8 Hardware/software key generation

Pseudo-random numbers used in any key generation shall be approved by the RDEC. Relevant requirements for subscriber's pseudo-random numbers, key pair and symmetric key generation, software or hardware shall be as follows:

Assurance level	Key generation mechanism
Test level	Software or hardware
Level 1	Software or hardware
Level 2	Software or hardware
Level 3	Software or hardware
Level 4	Hardware only

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

Public keys that are bound into certificates shall be certified for use in signing or encrypting. The use of a specific key is determined by the keyUsage extension in the X.509 certificate. In particular, certificates to be used for digital signature (including authentication) shall set the digitalSignature bits. Certificates to be used for data encryption shall set the keyEncipherment or dataEncipherment bit. CA Certificates shall set two key usage bits: cRLSign and CertSign.

Test level, level 1, 2 and 3 certificates may include a single key for use with encryption and signature in support of certain old version Secure multipurpose Internet Mail Extensions, S/MIME) applications. Such "dual-use" certificates shall be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such "dual use" certificates shall never assert

the non-repudiation key usage bit, and shall not be used for authenticating data signature certification. Subordinate CAs of all assurance levels shall issue two key pairs to subscribers, one for data encryption and one for digital signature and authentication.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

The RDEC shall determine the relevant standards of cryptographic module certification. The security requirements for cryptographic module are mainly based on FIPS 140 or standards with equivalent security. These standards shall be published by the RDEC. Cryptographic modules shall base on relevant certification standards to conduct equivalent security level certification. Additionally, the RDEC reserves the right to review technical documentation associated with any cryptomodule under consideration for use by the GRCA.

The following table summarizes the minimum requirement of the cryptographic modules; higher levels may be used. For the levels listed in the table, reference is made on the definition of the FIPS 140 series:

Assurance level	GRCA	Subordinate CA	Registration Authority	Subscriber
Test level	Not applicable	No stipulation	No stipulation	No stipulation
Level 1	Not applicable	Level 1 (Hardware or Software)	Level 1 (Hardware or Software)	No stipulation
Level 2	Not applicable	Level 2 (Hardware or Software)	Level 2 (Hardware or Software)	Level 1 (Hardware or Software)
Level 3	Not applicable	Level 2	Level 2	Level 1

		(Hardware)	(Hardware)	(Hardware or software)
Level 4	Level 3 (Hardware)	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

6.2.2 Private key (n out of m) multi-person control

Use of private keys of CAs at assurance level 3 and 4 shall require action by multiple persons as set forth in Chapter 5.

6.2.3 Private key escrow

Signature private keys cannot be escrowed.

6.2.4 Private key backup

6.2.4.1 CA's private key backup

For CAs operating at assurance level 3 and 4, the private signature keys shall be backed up under the multi-person control procedures and may be stored in the back up location. Procedures for CA's private key backup shall be asserted in the CPS.

6.2.4.2 Subscriber's Private Signature Key backup

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting assurance level 1, 2 and 3 certificate may be backed up or copied, but must be held in the Subscriber's control.

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting assurance level 4 may not be backed up or copied.

6.2.5 Private key archival

Private signature keys shall not be archived.

6.2.6 Private key entry into cryptographic module

The CA private keys may be backed up in accordance with Section 6.1.1.

6.2.7 Method of activating private key

The subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e. the data should not be displayed while it is entered).

Entry of activation data shall be protected from unauthenticated access.

6.2.8 Method of deactivating private key

After use, the cryptographic module shall be deactivated, e.g. via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.9 Method of destroying private key

Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificate to which they correspond expire or are revoked. For software cryptographic module, the data shall be

copied to the memory or storage media occupied by the signature private key. For hardware cryptographic modules, a “zeroize” command is needed. Physical destruction of hardware should not be required.

6.3 Other Aspects of Key Pair Management

It is technically possible to use the same key-pair for both digital signature and confidentiality. However, this CP discourages that condition in any assurance level, except to support old version application system in Section 6.1.9. Two types of key on the certificate are suggested to be issued to subscriber, one for encryption and one for digital signature and authentication.

A subscriber’s private key that is used for digital signature and authentication shall never be escrowed, archived or backed up. Any CA that the subscriber belongs to can request for escrow, archival or backup the private key used in encryption.

6.3.1 Public key archival

After the certificate is archived, it is not necessary to conduct public key archival.

6.3.2 Usage periods for the public and private keys

6.3.2.1 Usage periods for public and private keys of CA

Based on different security class, the usage periods of public and private keys of CA are as follows:

- (1) For RSA 4096 bit or other types of public key pair with

equivalent security (e.g. EEC 300 bit): the maximum usage period of private key is 15 years and the maximum usage period of public key certificate is 30 years.

(2) For RSA 2048 bit or other types of public key pair with equivalent security (e.g. ECC 244 bit): the maximum usage period of private key is 10 years and the maximum usage period of public key certificate is 20 years.

(3) For RSA 1024 bit or other types of public key pair with equivalent security (e.g. ECC 161 bit): the maximum usage period of private key is 5 years and the maximum usage period of public key certificate is 10 years.

The GRCA private signing keys will be used to sign certificates for not more than one-half of the lifetime. The self-signed certificate lifetime will be valid for not more than 30 years.

The sum of lifetime of certificate issued to subordinate CA by the GRCA and the lifetime of private signing keys of the GRCA used to sign certificates shall not exceed the lifetime of the GRCA self-signed certificate.

6.3.2.2 Usage periods of public and private keys of subscribers

The usage period of any subscriber is specified based on its key size. If the key is equivalent to RSA 1024 bit security, then the maximum usage period of the private key is 5 years. If the key is equivalent to RSA 2048 bit security, then the maximum usage period of the private key is 10 years. The total maximum duration of the certificate (including renewal) shall be the same as the key usage period.

6.4 Activation Data

6.4.1 Activation data generation and installation

The activation data used to unlock CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. For CAs at assurance level 1, 2 and 3, activation data may be user selected. For assurance level 4, it shall either entail the use of biometric data or satisfy the policy enforced by the cryptographic module. Where passwords are used as activation data, the password data shall be generated in conformance with the information security management essentials and standards of the Executive Yuan and its various subordinate authorities. If the activation data must be transmitted, it shall be via an appropriately protected channel.

6.4.2 Activation data protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanism. Activation data should either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CPS.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

CAs operating at assurance level 3 and 4 and its ancillary parts shall include the following functionality. The following computer security functions may be provided by the operation system or through a combination of operation system, software and physical safeguards:

- (1) Require authenticated logins.
- (2) Provide discretionary access control.
- (3) Provide a security audit capability.
- (4) Restrict access control to CA services and PKI roles.
- (5) Require identification and authentication of PKI roles and associated identities.
- (6) Ensure the security of communication and database with cryptographic technology.
- (7) Require a trusted path for identification of PKI roles and associated identities.
- (8) Possess procedure integrity and security control protection.

When CA equipment is hosted on evaluated platform in support of computer security assurance requirements, then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

The system development controls for CAs are as follows:

Assurance level	System development controls
Test level	No stipulation.
Level 1	No stipulation.
Level 2 Level 3 Level 4	<p>(1) Use software that has been designed and developed under a formal, documented development methodology e.g. the Capability Maturity Model (CMM).</p> <p>(2) The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications; hardware devices, network connections, or component software installed which is not part of the CA operation.</p> <p>(3) Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by secure policy.</p> <p>(4) RA hardware and software shall be scanned for malicious code on first use and periodically</p>

Assurance level	System development controls
	thereafter.

6.6.2 Security management controls

Assurance level	Security management controls
Test level Level 1 Level 2 Level 3	<p>The configuration of the CA system as well as any modification and upgrade shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CA software or configuration. The CA software, when first loaded, shall be verified as being that</p> <p style="text-align: center;">supplied from the vendor, with no modifications, and be the version intended for use.</p>
Level 4	<p>The configuration of the CA system as well as any modification and upgrade shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CA software or configuration. The CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The integrity of the software shall be verified by the CA at least monthly.</p>

6.6.3 Life cycle security ratings

No stipulation

6.7 Network Security Controls

The GRCA mainframe and the internal repository shall not be connected to any external network. The GRCA external repository shall be connected to the Internet to provide continuous service (except, when necessary, for brief periods of maintenance or backup). Internal repository information shall be transported to the external repository using manual mechanisms and all such information will be digitally signed (certificates and CARLs). The external repository shall be protected by system repair program update, vulnerability scanning, intrusion detection system, firewall or filtering router to guard against denial of service and intrusion attacks.

6.8 Cryptographic Module Engineering Controls

Requirements for cryptographic modules are in accordance with Section 6.1 and 6.2.

7 CERTIFICATE AND CARL/CRL PROFILES

7.1 Certificate Profile

7.1.1 Version numbers

CAs shall issue X509 v3 certificates whose filed of version number shall be value “2”.

7.1.2 Certificate extensions

Rules for the assignment of value, and processing of extensions are defined in the profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities.

Certificates issued by the GRCA shall comply with the 「Government PKI Certificate & CARL Profile.」 Certificates issued by subordinate CAs operating at assurance level 3 shall comply with the CA/CARL profile. Certificates issued by subordinate CAs operating at assurance level 1 and 2 shall comply with RFC 3280. Whenever private extensions are used, they shall be identified in a CPS. Critical private extensions shall be interoperable in their intended community of use.

7.1.3 Algorithm object identifiers

Certificates issued under this CP shall use the following algorithms
OIDs for signature:

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

Certificates issued under this CP shall use the following OIDs for identifying the algorithm for which the subject key was generated:

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

7.1.4 Name forms

When required as set forth above, the subject and issue fields of the base certificate shall make use of an X.500 Distinguished Name, with the attribute type as further constrained by RFC 3280.

7.1.5 Name constraints

No stipulation

7.1.6 Certificate policy Object Identifier

Certificate issued under this CP shall assert the OID appropriate to the level of assurance with which it was issued.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9 Processing semantics for the critical certificate policy extension

Processing semantics for the critical certificate policy extension used by the CA shall comply with CA and CRL profile.

7.2 CARL/CRL Profile

7.2.1 Version Numbers

CAs shall issue X.509 version two (2) CARLs/CRLs.

7.2.2 CARL/CRL and CARL/CRL entry extensions

Detailed CARL/CRL profile addressing the use of each extension shall conform to certificate and CRL profile.

8. SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

The RDEC shall review this CP at least once every year. CAs shall review its CPS at least once every year to maintain its assurance. When changes of the CP do not affect the certificate usage purpose and its assurance level asserted in the CP, the CP OID needs not to be changed. When there is change on the CP OID, the CPS shall conduct corresponding change.

8.1.1 Items of Change That Will Not be Notified

When the typesetting of CP and the CPS is to be conducted again, there will be no separate notification.

8.1.2 Items of Change That Will be Notified

CA shall assert the changes to be notified in the CPS.

8.1.2.1 Items of change

The RDEC will evaluate the level of effect on subscribers or relying parties by changes in the CP: :

(1)Revision shall be processed after publication for 30 calendar days for major effects.

(2)Revision shall be processed after publication for 15 calendar days

for minor effects.

8.1.2.2 Notification system

For changes that may generate major effects on subscribers, the RDEC and CA shall publish in the repository of the GRCA and CA respectively and CA shall assert such changes in the CPS.

8.1.2.3 Reply period of opinions

If there is opinion on the changes in Section 8.1.2.1, its reply period shall be:

- (1) When the level of effect is major according to Section 8.1.2.1 (1), the reply period is within 15 calendar days from the day of publication.
- (2) When the level of effect is minor according to Section 8.1.2.1 (2), the reply period is within 7 calendar days from the day of publication.

CA shall assert the reply period of opinion in the CPS.

8.1.2.4 Opinion processing mechanism

The RDEC will be responsible for processing opinions on this CP and CAs shall assert the opinion processing mechanism in the CPS.

8.1.2.5 Final publication period

Publication of changes in the CP shall be in accordance with Section 8.1.2.2 and 8.1.2.3 to conduct revision. Based on Section 8.1.2.1, the publication period shall be at least 15 calendar days until the CP revision

becomes effective. CAs shall assert the final publication period in the CPS.

8.2 Publication and notification policies

This CP and any subsequent change shall be publicly available within one week of approval. CA shall assert the provisions of publication and notification in the CPS.

8.3 CPS approval procedures

CPS of CAs shall conform to relevant laws and provisions of this CPS and shall be approved by the RDEC and the Electronic Signature Act administrative organization, Ministry of Economic Affairs. After this CP revision is published, the CPS of the CA shall cope with the revision that shall be sent to the RDEC and the Electronic Signature Act administrative organization, Ministry of Economic Affairs for approval.

APPENDIX : GLOSSARY

Access	Ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs or other systems
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e. unlock private keys for signing or decryption events).
Applicant	The subscriber is sometimes also called an “applicant” after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
Archive	Long term, physically storage place that that can be used for services e.g. backup, usability or integrity service etc.
Assurance	The foundation that based on this, the relying entity has conformed to the specific security essentials. (To be asserted in Chapter 1, Section 2, Item 1 of the CPS).
Assurance Level	Certain level that has corresponding assurance level. (To be asserted in Chapter 1, Section 2, Item 2 of the CPS).
Attribute Authority	An entity recognized by the PKI authority or comparable CA as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operation procedures, to recommend necessary changes in controls, policies and procedures, and to evaluate whether the

	system control is appropriate.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measures designed to establish the validity of a transmission, message, or originator, or a means of verifying the individual's authorization to receive specific categories of information.
Backup	Copy of files or programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioral characteristic of a human being.
Certificate	<p>A digital representation of information which at least:</p> <ol style="list-style-type: none">(1) Identifies the CA that issues it.(2) Names or identifies of its subscriber.(3) Contains the subscriber's public key.(4) Identifies its operational period.(5) Is digitally signed by the certification authority issuing it. <p>As used in this CP, the term "certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.</p>
Certification Authority, CA	<ol style="list-style-type: none">(1) Authority and corporation that issue certificates. (Article 2-5 of Electronic Signature Act)(2) An authority trusted by one or more users to

issue and manage X.509 format public key certificates and CARLs or CRLs.

Certification Authority Revocation List, CARL)

A signed and time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.

Certificate Policy, CP

(1) Specifies the applicable target of a certain certificate or a set of rules listed by condition. That target or condition can be a specific community or possesses application of common security requirement. (To be asserted in Chapter 1, Section 2, Item 3 of the CPS.
(2) A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, audit, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practice Statement(CPS)

(1) By announcing to outside by CA, it is used to explain the operating standards of certificate issuance and the process of other certification by CA. (Electronic Signature Act Article 2-7).
(2) A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e. requirements specified in this CP, or requirements specified in a contract for services).

Certificate Revocation List, CRL	(1) List of revoked certificates that can be provided to relying parties by CAs in the form of electronic signature. (To be asserted in Chapter 1, Section 2, Item 9 of the CPS). (2) A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security requirements of customers and the security attributes of products. Evaluation on information technology products and system security standards including functional and guarantee requirements.
Component Private Key	Private key associated with a function of the certificate issuing equipment, as opposed to associated private key of operator or administrator.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not being known to or acquired by unauthorized entities or processes.
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Cryptoperiod	Time span during which each key setting remains in effect.

Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of an electronic document by means of algorithm or other calculation method into digital information with certain size. The private key of the signing person is encrypted to become an electronic signature and the public key is being certified. (Article 2-3 of the Electronic Signature Act).
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields; “date of issue” and “date of next issue”.
E-commerce	The use of network technology (especially the Internet) to buy or sell goods and services.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic message, files, documents, or information or to establish or exchange a session key for these same purposes.
End Entity	Relying parties and subscribers including personnel, organization, account, installation or site.
Firewall	Gateway that limits access between networks in accordance with local security policy.
Inside Threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification and/or denial of services.
Integrity	Protection against unauthorized modification or destruction. A state in which information has remained unaltered from the point it was produced from a source during transmission, storage and

	eventual receipt by the acceptance party.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement (or similar contract) binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer or other party, upon provisions set forth in the agreement.
Key Exchange	The process of exchanging public keys in order to establish secure communication.
Key Generation Material	Random numbers, pseudo-random numbers, and other cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the following properties: (1) One key can be used to encrypt a message that can only be decrypted by using the other key. (2) Even knowing one key, it is computationally infeasible to discover the other key.
Cross Certification Agreement, CCA	The agreement that the GRCA and subordinate CAs shall abide by and its individual responsibilities and obligations when the subordinate CA applies to join the GPKI.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.

Technical non-repudiation refers to the assurance a Relying Party that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private key can be established.

Object Identifier, OID	<p>(1)A distinguished identifier composed of alphanumeric or numeric identifier that is registered based on the registration standard of international organization and can be used to identify the distinguished corresponding certificate policy. During revision of CP, its OID needs not to be changed. (To be stated in Chapter 1, Section 2, Item 4 of CPS.</p> <p>(2)A specialized formatted number that is registered with internationally recognized standard organization (ISO). When mentioning certain object or object category, this distinguished number can be used for identification. For example, in the PKI, they are used to specify the certificate policy and the cryptographic algorithm supported.</p>
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g. one party uses registered mail to communicate with another party when current communication is occurring on-line).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data and/or denial of service.
Government Electronic Certification Steering Committee GECSC	An organization established with purposes of: formulating the administration authority certificate policy and CPS, technical standards, electronic certificate system structure and other electronic certificate management.

Private key	<p>(1) The key of a signature key pair used to create a digital signature.</p> <p>(2) The key of an encryption key pair that is used to decrypt confidential information.</p> <p>In both cases, this key must be kept secret.</p>
Public Key	<p>(1) The key of a signature key pair used to validate a digital signature.</p> <p>(2) The key of an encryption key pair that is used to encrypt key pair that is used to encrypt confidential information.</p> <p>In both cases, this key is made publicly available. (in the form of digital certificate.)</p>
Registration Authority, RA	<p>(1) An entity that is responsible for confirming the identity or other attribute of the certificate applicant but does not issue and manage certificates. Its responsible behavior and the scope of its responsibilities shall be specified based on the applicable certificate policy or agreement. (To be asserted in Chapter 1, Section 2, Article 7 of the CPS).</p> <p>(2) An entity that is responsible for identification or authentication of certificate subjects but does not sign or issue certificates.</p>
Re-key (a certificate)	<p>To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.</p>
Relying Party	<p>(1) An entity that relies on the received certificate and the verified digital signature of the public key asserted in the certificate, or relies on the identity of the name subject in the certificate or the corresponding relationship of the public key asserted in the certificate. (To be asserted in Chapter 1, Section 2, Article 6 of the CPS).</p> <p>(2) A person or Agency who has received information that includes a certificate and a digital signature (verifiable with reference to a</p>

public key listed in the certificate) and is in a position to rely on them.

Renew (a certificate)	The act or process of extending the validity of the data binding(?) asserted by a public key certificate through issuing a new certificate.
Repository	(1)A trusted mechanism that is used to store and search for certificates or other information. (To be asserted in Chapter 1, Section 2, Item 8 of the CPS). (2)A database containing information and data relating to certificates as specified in this CP.
Revoke a Certificate	To prematurely end the operation period of a certificate effective at a specific date and time.
Government Root CA	The most top level in a hierarchical PKI and is the source of reliance of its public key.
Secret key	A “shared secret” used in symmetric cryptography, wherein users are authenticated based on a password, Personal Identification Number (PIN), or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed beforehand by the transacting parties.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signature (rather than encrypting data or performing other cryptographic function).
Subordinate CA	In a hierarchical PKI, a CA whose certificate is certified by another CA, and whose activities are constrained by that other CA.
Subscriber	A Subscriber is an entity that:

	<p>(1)the subject named or identified in a certificate issued to that entity;</p> <p>(2)holds a private key that corresponds to the public key listed in the certificate;</p> <p>(3) does not itself issue certificate to another party.</p> <p>This includes, but is not limited to, an individual, institution or network device.</p>
Technical Non-Repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, malicious modification of data and/or denial of service.
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a “trust anchor”.
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object exists at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (1)are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability and correct operation; (3)are reasonably suited to perform their intended functions; (4)adhere to generally accepted security procedures.
Update (a	Refer to Section 3.2.3 of this certificate policy.

certificate)

Zeroize

A method of erasing electronically stored data by altering the contents of data storage as to prevent the recovery of the data.