Government Root Certification Authority
Certification Practice Statement
Version 1.6

Administrative Organization: National Development Council
Executive Organization: ChungHwa Telecom Co., Ltd.
June 14, 2019

Version Revision Log

Version	Effective Date	Description of Revised Content
1.6	2019/06/14	Update to RFC3647

Contents

Summary

In compliance with the provisions of the Electronic Signatures Act and its bylaws Regulations on Required Information for Certification Practice Statement, the following is a description of key aspects of the Government Root Certificate Authority Certification Practice Statement (GRCA CPS):

1. Competent Authority Approval Number: Jing Shang no.

2. Certificate Issuance:

(1) Types: Self-signed certificates, self-issued certificates and subordinate CA certificates issued to subordinate CAs and cross-certificates issued to subject CAs by the Government Root Certificate Authority (GRCA).

(2) Assurance level: The five types of identification assurance level certificates defined by the (Certificate Policy for the Government Public Key Infrastructure hereinafter referred to as Certificate Policy)

(3) Scope of Use:

A. The self-signed certificate is used to establish the trust anchor of the GPKI.

B. The self-issued certificate is the certificate issued during GRCA rekey or for CP requirements and used to establish a trust pathway between old and new keys or CP interoperable certificates.

C. Subordinate CA certificates are used to build mutual trust relationships between infrastructure building CAs

and certificate trust pathways needed for the interoperability of CAs.

D. Cross-certificates are used to build mutual trust relationships between different PKI building CAs and certificate trust pathways needed for the interoperability of CAs.

3. Major Liability Matters:

(1) The GRCA assumes no liability for any consequences arising from the use of certificates by subordinate CAs, subject CAs and relying parties outside the scope of the CPS.

(2) Regarding liability of the GRCA to the cross-certified CA for damages arising from the issue or use of certificates, the liability of the GRCA for damages shall be limited to that set down in the CPS and related contracts.

(3) The GRCA assumes no liability for any damages arising from a force majeure and other events not attributable to the GRCA.

(4) In the event that the GRCA needs to temporarily halt part of its certification services due to system maintenance, conversion or expansion, the GRCA will post a notice the repository and notify the Certification Authorities. Relying parties and subject CAs may not use this event as a reason to request compensation from the GRCA.

4. Other Important Matters:

(1) The GRCA accepts certificate registration and revocation

requests so no separate Registration Authority has been established.

(2) The subordinate CA and subject CA must describe the assurance level of the request certification when submitting the subordinate CA certificate request or cross-certification request for GRCA issued certificates based on the scope of use of the different assurance levels.

(3) Self-generated private keys must be properly kept and used by the CA requesting the subordinate CA certificate or cross-certificate.

(4) Acceptance of a cross-certificate issued by the GRCA indicates confirmation of the correctness of the content of the certificate by the CA.

(5) If the subordinate CA or subject CA finds it necessary to revoke certificates, the GRCA should be promptly notified and CPS procedures should be followed. However, appropriate actions should first be taken to limit the impact on subordinate CAs, subject CAs or relying parties and assumption of all liability arising from use of the certificates prior to the subordinate CA or subject CA certificate revocation status.

(6) Trusted parties which are using GRCA should first check the accuracy, validity, assurance level and use restrictions of the certificate.

(7) The National Development Council commissions a trusted third party to conduct external compliance audits of the

GRCA in accordance with the Government Procurement Act.

1 Introduction

The Government Root Certification Authority Certification Practice Statement (GRCA CPS) is stipulated to follow the Certificate Policy for the Government Public Key Infrastructure (CP) and related international standards (such as IETF RFC 3647) and comply with the bylaws of the Electronic Signatures Act and the Regulations on Required Information for Certification Practice Statements. The CPS delineates how the Government Root Certificate Authority (GRCA) proceeds in accordance with the Fourth Assurance Level (High) to issue and manage self-signed certificates, self-issued certificates, subordinate CA certificates and cross-certificates.

1.1 Overview

According to the regulations of the CP, the GRCA is the highest level CA in the hierarchical structure of the GPKI. The GRCA is the trust anchor of the GPKI and is stipulated as having the highest assurance level as defined in the GPKI. This means that relying parties can trust the GRCA directly.

The CPS delineates how the GRCA acts in accordance with the Fourth Assurance Level (High) in the CP to issue and manage certificates.The CPS stated in this CPS only applies to entities related to the GRCA community, such as the GRCA, subordinate certification authority, subject certification authority, Relying Parties and Repository.

The GRCA and subordinate CAs or subject CAs having certificates issued by server application software shall comply the official version of the Baseline Requirements for the Issuance and Management of

Publicly-Trusted Certificates published by the CA/Browser Forum. With regard to the effective date of each item of information in the official version, the GRCA shall be in compliance (see Appendix 3).

The National Development Council (NDC) is the administration organization of the GRCA. The establishment and any modification to the GRCA CPS may go into effect only after obtaining the permission of the Electronic Signatures Act competent authority (MOEA) and announcement. The CPS is not authorized to be used by CAs outside the GRCA. The CA shall be solely responsible for any problems arising from the use of the CPS by other CA.

1.2 Document Names and Identification

This CPS is referred to as the Government Root Certification Authority Certification Practice Statement (GRCA CPS). This is version 1.6. The date of publication is June 14, 2019 . The latest version of the CPS can be obtained from:

https://grca.nat.gov.tw/download/GRCA_CPS_v1.6.pdf

The CPS is set down in accordance with the CP. Operation of the GRCA proceeds according to the Fourth Assurance Level (High). The name Object Identifier (OID) is id-tw-gpki-certpolicy-class4Assurance and OID value is {id-tw-gpki-certpolicy 4} (refer to GPKI CP).

1.3 Key Participants

The key participants of this CPS include:

(1) Government Root Certification Authority

(2) Subordinate certification authority

(3) Subject certification authority

(4) Relying parties

(5) Other related parties including contracted entities authorized by the NDC to establish the GRCA and maintain and operate the system.

1.3.1 Certification Authority

1.3.1.1 Government Root Certification Authority

The GRCA is the trust anchor of the GPKI and is stipulated as having the highest assurance level as defined in the GPKI. This means that relying parties can trust the GRCA directly.

The GRCA is the trust anchor of the GPKI operating at the Fourth Assurance Level. Its duties are as follows:

(1) Responsible for self-signed certificates, self-issued certificates, cross certificates and level 1 subordinate CA certificate issuance and management.

(2) Publish the issued certificates and certification authority revocation list (CARL) on the repository and ensure the regular operation of the repository.

(3) The GRCA shall not establish a separate registration authority (RA).

1.3.1.2 Subordinate Certificate Authority

The subordinate certificate authority is another type of CA established in the GPKI. Their duties are as follows:

(1) Primarily responsible for the issuance and management of end entity (EE) certificates.

(2) Establishment of a hierarchical GPKI may be used as an establishment method if necessary. A level 1 subordinate CA issues certificates to level 2 subordinate CA or a level 2 subordinate CA issues certificates to a level 3 subordinate CA. A multi-level PKI framework is established according to this principle. However, the subordinate CA may not directly perform cross-certification with CAs outside this infrastructure.

(3) Establishment shall be done by the subordinate CA in accordance with CP-related regulations and a contact window shall be set up to be responsible for interoperability work between the GRCA and subordinate CA.

1.3.1.3 Subject Certification Authority

The Subject Certification Authority refers to the cross-certifying conducted between the CA and GRCA including Level 1 subordinate CA and CA outside the GPKI.

Requests by the subject CA made to the GRCA must conform to cited CP assurance level security regulations and possess public key infrastructure, digital signature and certificate issuance technology establishment and management capabilities and must set down related responsibilities and obligations for CA, RA and relying parties.

1.3.2 Registration Authority

The GRCA directly accepts certificate registration and revocation requests, is responsible for collecting and authenticating subordinate CA

and subject CA identities and certificate-related information. No separate RA is established.

1.3.3 Subscriber

(1) Refers to entities identified by a certificate subject name. The entity has a private key that corresponds with the certificate public key.

(2) For types of certificates with incapacitated application software, hardware or equipment, the certificate subscriber refers to individual or organization requesting the certificate.

(3) The CA identified by the cross-certificate subject name is called the subject CA and is not considered a subscriber.

1.3.4 Relying Parties

The relying party is the entity that relies on the binding relationship of the certificate subject name to a public key.

1.3.5 Other Related Parties

If the GRCA selects other trusted service agencies to serve as operation partners, an interoperation mechanism and mutual rights and obligations should be established in the CPS to ensure the effectiveness and reliability of GRCA service. Relevant information shall also be posted on the GRCA website.

1.3.5.1 Certification Service by Outsourcing

The NDC has commissioned ChungHwa Telecom Co., Ltd. (CHT) to perform the establishment, operation and maintenance work for the

GRCA.

1.4 Applicability

1.4.1 Usage of Issued Certificates

The GRCA issues four kinds of certificates: self-signed certificates, self-issued certificates, subordinate CA certifications and cross-certificates.

(1) Self-signed certificates

Used to establish a trust anchor for the GPKI. The issuance counterpart of self-signed certificates is the GRCA itself. It contains the GRCA public key which can be used to verify GRCA issued self-issued certificate, subordinate CA certificate, cross-certificate and CARL digital signatures.

(2) Self-issued certificates

Certificates issued for GRCA re-key or due to CP requirements that are used to establish a trust pathway between the new and old key or CP interoperation certificates.

(3) Subordinate CA certificates

Used to establish a trust relationship between CAs in the infrastructure in order to set up the certificate trust pathways required for CA interoperation. The issuance counterpart of the subordinate CA is the subordinate CA established under the GPKI. The subordinate CA certificate contains a subordinate CA public key which can be used with certificate and CARL digital signatures used to verify certificates issued by a subordinate CA.

(4) Cross-certificates

Used to establish trust pathways between different PKI CAs. The issuance counterpart of cross-certificates is CAs performing cross-certification with the GRCA including level 1 subordinate CA established under this infrastructure and CAs outside the infrastructure. The cross-certificate contains subject CA public keys which can be used with certificate and CARL digital signatures issued to verify certificates issued by a subordinate CA.

1.4.2 Certificate Use Restrictions

Relying parties shall obtain the trusted GRCA's public key or self-signed certificate via a secure channel as stipulated in section 6.1.4 GRCA Secure Transmission of Public Keys to Relying Parties for use to verify the digital signatures of self-issued certificates, subordinate CA certificates, cross-certificates and CARLs.

Relying parties should carefully select a secure computer environment and trusted application system for verification of the digital signature on self-issued certificates, subordinate CA certificates, cross-certificates and CARLs issued by the GRCA to ensure that the GRCA public key or self-signed certificate will not be comprised or replaced.

The certificates issued to the subordinate CA by the GRCA should contain the assurance levels of certificates which the subordinate CA can issue so the relying parties may use this information to determine whether or not they want to trust the subordinate CA and the certificates it issues.

The cross-certificates issued to the CA by the GRCA should contain

the assurance levels of certificates which the CA can issue and then at what levels cross-certification may be conducted with other CAs so relying parties may use this information to determine whether they want to trust the CA and the certificates it issues. In addition, the cross-certificates issued by a CA outside the GPKI should contain the policy mapping relationship between its CP and the CP used by the CA. The relying parties has the power to decide whether they want to trust the CA and the certificates it issues based on this relationship.

The relying parties must carefully read the CPS before using the certification services provided by the GRCA, follow CPS regulations and watch for any modifications made to this CPS.

1.4.3 Scope of Prohibited Certificate Uses

(1) Crime

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

(3) Operation of nuclear equipment

(4) Aviation and control system

1.5 Contact Details

1.5.1 Organization Establishing and Administering the CPS

The GRCA is responsible for establishing the various provisions of the CPS. The CPS and its modifications are announced and implemented following approval by Electronic Signatures Act competent authority (MOEA).

1.5.2 Contact Information

E-mail address：gca@gca.nat.gov.tw

The phone numbers, postal address of the GRCA can be found at https://grca.nat.gov.tw/GRCAeng/index.html.

1.5.3 Person Determining Certificate Practice Statement Suitability for the Policy

The CPS review shall adhere to the following procedure:

(1) The GRCA shall check if the CPS conforms to related regulations in the CP. The CPS shall be reviewed and approved by Government Electronic Certification Steering Committee.

(2) The CPS shall be reviewed by the competent authority of the Electronic Signatures Act.

1.5.4 CPS Modification Procedure

The GRCA shall announce the CPS after it is reviewed by the MOEA competent authority of the Electronic Signatures Act. The corresponding modifications made to the CPS after CP modifications are announced shall be submitted to the MOEA competent authority of the Electronic Signatures Act for review.

The CPS modifications shall take precedence, unless stipulated otherwise, if there is any conflict between the revised contents and original CPS after the CPS modifications take effect. If the modifications are made by attached document and the content of the attached documents conflict with the original CPS, the content of the attached document shall take precedence.

1.6 Definitions and Acronyms

See Appendix 1 Definitions and Acronyms and Appendix 2 English Terms and Acronyms.

2 Publishing and Repository Responsibilities

2.1 Repository

The repository is responsible for the publishing of GRCA issued certificates, certification authority revocation list (CARL) and other certificate-related information and providing 24-hour round-the-clock services. The Internet address of the GRCA repository is: http://grca.nat.gov.tw/. The repository will resume normal operation within two working days if unable to operate normally for some reason.

The responsibilities of the GRCA repository are as follows:

(1) Regularly publish issued certificates, CARL and other certificate-related information in accordance with chapter 2 Publishing and Repository Responsibilities.

(2) Publish the latest CP and CPS information.

(3) Maintain access control of the repository in accordance with the provisions in section 2.4 Access Controls.

(4) Guarantee the accessibility status and availability of the repository information.

2.2 Publication of Certificate Information

The following are published by the GRCA repository:

(1) CP and Technical Specifications.

(2) This CPS.

(3) CARLs.

(4) Self-signed certificates of the GRCA (until the expiry of all certificates issued with the private key corresponding to that certificate's public key).

(5) GRCA self-issued certificate cross-signed with the new and old keys (until the expiry of all certificates issued with the private key corresponding to that certificate's public key).

(6) Subordinate CA certificates.

(7) Subject CA certificates.

(8) Privacy protection policy.

(9) Utility program downloading.

(10) The latest audit results.

(11) The latest GRCA news.

With regard to SSL certificate issuance services provided by subordinate CA belonging to the GRCA or cross-checking subject CA, the GRCA shall request that CA issuing the SSL certificate publish the website address of the three SSL certificates used for Application Software Provider testing in the repository. Use valid, revoked and expired SSL certificates to individually test the Application Software Provider if the SSL certificates can be used to link to GRCA self-issued certificates.

2.3 Time or Frequency of Publication

(1) One CARL is issued by the GRCA at least once per day and

published in the repository.

(2) The modified CPS is published in the repository within 10 calendar days and takes effect on the date the modified CPS is published.

2.4 Access Controls

The GRCA host and repository host are installed without any network connection. The certificates and CARL issued by the GRCA cannot be directly transmitted to the repository host by network connection. When certificates and CARLs need to be published in the repository, authorized GRCA personnel that publish the issued certificates use manual off-line methods to store the certificates and CARLs to be published on portable media and then copy the files to the repository for publication.

The information published in the repository as described in section 2.2 Certificate Information Publication is primarily provided for searches by subordinate CA, subject CA and relying parties. Therefore, the information is open for public viewing and downloading. Access controls have been implemented to guarantee repository security and maintain its accessibility and availability.

3 Identification and Authentication

3.1 Names

3.1.1 Types of Names

(1) The subject name of the certificate issued by the GRCA conforms to the Distinguished Name (DN) of X.500.

(2) Only this DN format is used for the self-signed certificates, self-issued certificates of the GRCA and subordinate CA certificates and CA cross-certificates.

3.1.2 Need for Names to be Meaningful

The subordinate CA and subject CA certificate subject names in the application should comply with:

(1) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates guidelines issued by CA / Browser Forum.

(2) Relevant naming rules in related national laws and the names should be able to represent and identify the certification authority.

3.1.3 Anonymous or False Names of Subscribers

The GRCA does not issue anonymous certificates or certificates with false names.

3.1.4 Rules for Interpreting Various Name Forms

Name format are based on GPKI certificate and CRL profiles. The rules for interpreting various name forms should comply with the name attribute definition of ITU-T X.520.

3.1.5 Uniqueness of Names

The GRCA reviews the uniqueness of the names applying to become ubordinate CA and subject CA names. If a duplicate name is found, then the applying CA is asked to change the name.

The first and second generation self-signed certificates of the GRCA uses the following name form:

C=TW,

O=Government Root Certification Authority

Since the same subject names on GRCA first and second generation self-signed certificate may result in cross-signed self-issued certificates being mistaken as self-signed certificates which can cause errors during browser verification of certificate trust pathways, the the GRCA generates 1.5 generation keys, issues self-issued certificates, re-establishes first and second generation trust pathways and uses the following formats:

C=TW,

O= Executive Yuan,

CN=Government Root Certification Authority - G1.5

In favor of international interoperability, the 3rd generation self-signed certificate of the GRCA uses the following name form:

C=TW,

O= Executive Yuan,

CN=Government Root Certification Authority - Gn

Where n=3,4…

In addition, the certificate issuer name and subject name is identical on the self-signed certificate of the GRCA.

3.1.6 Recognition, Authentication and Role of Trademarks

Not applicable.

3.1.7 Name Claim Dispute Resolution Procedure

The NDC is authorized to handle name claim disputes.

3.2 Initial Registration

3.2.1 Method to Prove Possession of Private Keys

When the CA makes a certificate request, a PKCS#10 certificate request file is generated by the CA. The GRCA uses the CA's public key to check the signature and prove this CA is in possession of the corresponding private key.

3.2.2 Authentication Procedure for Organization Identity

The subordinate CA applications submitted by a subordinate CA or cross-certificate application submitted by a subject CA shall include information such as the organization name, location and representative which is adequate to identify the organization. The application

information shall be combined with the documentation and sent in electronic or paper form to the NDC. The GRCA then verifies the correctness of the documentation.

If the documentation and cross-certificate application submitted by a CA operator that is not a ROC government agency, the GRCA shall verify the existence of the CA and confirm the documentation, the authorized person's identity and that the authorized person has the right to represent the organization for the certificate application. The authorized person shall appear in person at the time of certificate application.

3.2.3 Authentication Procedure for Individual Identity

Individual identity authentication procedures do not need to be followed for governing agencies. However, non-governmental organizations which apply for cross-certification need to have a representative named in the documentation (individual authorized to apply for cross-certification) to apply for CA certificate. The identity authentication procedure is as follows:

(1) The representative must prove his/her identity in person.

(2) Cross-check the written application form and representative's identification documentation.

The representative should present his / her ROC ID card or passport during certificate application so that the GRCA may authenticate the representative's identity.

(3) Review the representative's authorization document.

3.2.4 Unauthenticated Subscriber Information

Unauthenticated subscriber information may not be written onto the certificate.

3.2.5 Validation of Authority

When the certificate applicant applies for a certificate and makes a revocation request during the certificate lifecycle, the GRCA, subordinate CA or its RA should perform a validation of authority to verify that the certificate applicant can represent the certificate entity. The verification method is as follows:

(1) Verify the existence of the organization by means of a third-party identity authentication service, database verification, government agency or documents from a credible group.

(2) Verify that the certificate applicant is employed by the certificate subject (an organization or company) by means of telephone, mail, e-mail or other contact method and is authorized to represent the certificate subject.

(3) Verify the certificate applicant represents the organization by means of in-person face-to-face checking or other trusted communication methods.

3.2.6 Interoperability Standards

No regulations.

3.2.7Authentication Procedures for Information and Communication Devices or Server Application Software

Not applicable.

3.3 Key Change Request Identification and Authentication

The private key of the GRCA is 4,096 bits long. The validity of self-issued certificate is limited to 10 years. The validity of public key certificates is 30 years. The situations in which the GRCA shall perform key changes and new self-signed certificate issues are as follows:

(1) The current key has expired.

(2) Security of the current key is dubious due to suspected or confirmed compromise of the key.

3.3.1 Routine Key Change Identification and Authentication

The subordinate CA or subject CA should apply for new certificates from the GRCA when conducting a key change. The GRCA identifies and authenticates the CA applying for cross certification as stipulated in section 3.2 Initial Registration.

3.3.2 Certificate Rekey after Revocation Identification and Authentication

For the identification and authentication process for new certificate applications after CA certificate revocation, follow the regulations in section 3.2 Initial Registration when performing the new initial registration.

3.3.3 Certificate Extension Rekey Identification and Authentication

Self-signed certificates, self-issued certificates, Subordinate CA certificates and cross-certificates may not be extended.

3.4 Certificate Revocation Request Identification and Authentication

For the authentication process for GRCA self-signed certificates, Subordinate CA certificates and cross-certificates revocation requests, follow the regulations in section 3.2.2 Organization Identification and Authentication and section 3.2.3 Individual Identification and Authentication Procedure.

3.5 Certificate Suspension and Resumption Identification and Authentication

Not applicable.

4 Certificate Lifespan Operational Requirements

4.1 Certificate Application

4.1.1 Certificate Applicants

Certificate applicants include:

(1) GRCA.

(2) Subordinate CA.

(3) Root Certificate Authorities outside the GPKI.

4.1.2 Registration Procedure and Obligations

4.1.2.1 GRCA Obligations

(1) Operate in accordance with CP assurance level 4 regulations and the CPS.

(2) Determine subordinate CA application and CA cross-certification application procedures.

(3) Accept subordinate CA certificate registration and revocation request.

(4) Accept subject CA cross-certificate registration and revocation request.

(5) Implement Subordinate CA application and CA cross-certification application identification and authentication

procedures.

(6) Issue and announce certificates.

(7) Revoke certificate.

(8) Issue and announce CARLs.

(9) Implement CA personnel identification and authentication procedures.

(10) Secure generation of the GRCA private key.

(11) Protect GRCA private keys.

(12) Replace the GRCA self-signed certificate key and issue self-issued certificate.

4.1.2.2 Subordinate CA Obligations

(1) Follow the provisions of the CPS . The subordinate CA may be held liable when failure to abide by these provisions results in damages to a relying party.

(2) The certificates issued by the GRCA have different applicability based on the different assurance levels of the GPKI CP. The assurance level must be described in the certification application when the certificate application is submitted by the subordinate CA.

(3) The subordinate CA certificate application should be handled in accordance with the provisions in section 4.2 Certificate Application Procedure and the correctness of the application information should be verified.

(4) The subordinate CA should follow the provisions of section 4.4 Certificate Acceptance Procedure after the GRCA approval and issuance of the subordinate CA certificate.

(5) The acceptance of a certificate issued by the GRCA by subordinate CA implies confirmation of the correctness of the content of the certificate and the provisions of section 4.5 Key Pair and Certificate Usage are followed during certificate use.

(6) The subordinate CA should follow the provisions of Chapter 6 Technical Security Controls for self-generated private keys.

(7) The subordinate CA should ensure the safekeeping and proper usage of private keys.

(8) The subordinate CA certificate acceptance, validity and unrevoked status must be confirmed before the digital signature generated by the subordinate CA.

(9) Immediate notify the GRCA and follow the provisions of section 4.9 Certificate Suspension and Revocation when a certificate must be revoked by a CA due to private key compromise or loss. However, the subordinate CA is still liable before the revocation status information of its own certificates is published by the GRCA.

(10) In the event that regular services cannot be provided by the GRCA, the subordinate CA shall promptly seek out other means to fulfill their legal obligations to other parties and not use the GRCA's inability to provide services as a defense to other parties.

4.1.2.3 Subject CA Obligations

(1) Follow the provisions of this CPS and the Cross-Certification Agreement. The subject CA may be held liable when failure to abide by these provisions results in damages to a relying party.

(2) The certificates issued by the GRCA have different applicability based on the different assurance levels of the GPKI CP. The assurance level must be described in the certification application when the certificate application is submitted by the CA.

(3) The CA cross-certificate application should be handled in accordance with the provisions in section 4.2 Certificate Application Procedure and the correctness of the application information should be verified.

(4) The CA should accept the certificate in accordance with the provisions of section 4.4 Certificate Acceptance Procedure after the GRCA approval and issuance of the cross-certificate by the CA.

(5) The acceptance of a certificate issued by the GRCA by the subject CA implies confirmation of the correctness of the content of the certificate and the provisions of Section 4.5 Key Pair and Certificate Usage are followed during certificate use.

(6) The CA applying for cross-certification should follow the provisions of Chapter 6 Technical Security Controls for self-generated private keys.

(7) The subject CA should ensure the safekeeping and proper usage of private keys.

(8) The CA certificate acceptance, validity and unrevoked status must be confirmed before the digital signature is generated by the CA.

(9) Immediate notify the GRCA and follow the provisions of section 4.9 Certificate Suspension and Revocation when a certificate must be revoked by a CA due to private key compromise or loss. However, the subject CA is still liable before the revocation status information of its own certificates is published by the GRCA.

(10) In the event that regular services cannot be provided by the GRCA, the subject CA shall promptly seek out other means to fulfill their legal obligations to other parties and not use the GRCA's inability to provide services as a defense to other parties.

4.2 Certificate Application Procedure

4.2.1 Implementation of Identification and Authentication Functions

(1) Application Delivery by Mail

- The subordinate CA sends the subordinate CA certificate application form together with the CPS and certificate application file in PKCS#10 format in formal document form by mail to the GRCA.
- The subject CA sends the subject CA certificate application form together with the CPS and certificate application file in PKCS#10 format in formal document

form by mail to the GRCA. If the CA adopts a certificate policy other than GPKI-CP, then the complying certificate shall also be included.

(2) Identification and Authentication

The GRCA shall perform identification and authentication of the CA applicant in accordance with the procedures stipulated in section 3.2.2 Organization Identification Procedure.

(3) Check items

A. The GRCA shall check if there are any technical incompatibilities between the subordinate CA or subject CA applicant and the GRCA.

B. If the CP followed by the CA requesting cross-certification is a non-GPKI CP, the corresponding relationship between this CP and GRCA CP should be examined.

C. The GRCA shall check if the CPS of the CA complies with the cited CP.

D. The GRCA shall check the PKCS#10 certificate request file submitted by the certificate applicant.

4.2.2 Certification Application Approval or Rejection

4.2.2.1 Examination

(1) Subordinate CA Application

The NDC has approval authority for government agency CA applications. If the application is approved, the GRCA is notified to

perform the subsequent certificate issuance procedure.

(2) Subject CA Application

A meeting of the GECSC shall be convened when non-governmental CA apply for cross-certification to review the related application documents and the GRCA examination results in accordance with the provisions in section 4.2.2.2 Arrangement to determine the appropriateness of the CA and GRCA cross-certification. The GRCA then decides based on the GECSC determination whether to proceed to the certificate issuance stage.

4.2.2.2 Arrangement

The following steps shall be followed when a GECSC meeting is convened by the NDC:

(1) The identity of the subject CA and its representative shall be checked and authenticated in accordance with section 3.2.3 Individual Identity Authentication Procedure.

(2) The applicable terms and conditions shall be negotiated with the CA applying for cross-certification.

(3) After determining whether the cross-certification application by the Subject CA can proceed, a Cross-Certification Agreement (CCA) is signed with the CA requesting the cross-certification.

(4) The GRCA then decides based on the GECSC determination whether to proceed to the certificate issuance stage.

4.2.3 Certification Application Processing Time

After the certificate application submitted by the CA passes examination, the GRCA shall complete certificate issuance within seven working days.

4.3 Certificate Issuance Procedure

4.3.1 CA Work During Certificate Issuance

The GRCA assigns suitable personnel to perform certificate issuance work in accordance with section 5.2 Procedural Controls.

4.3.2 CA Notification of Certificate Applicant During Certificate Issuance

A. After the certificate is issued, the GRCA notifies the CA by official document and attaches the issued certificate. If the certificate application is denied approval, the GRCA shall notify the CA applicant by official document and state the reason why the application was denied approval.

B. If the GRCA issues a self-signed certificate, the certificate shall be sent to the relying party in accordance with section 6.1.4 GRCA Public Key Secure Transmission to Relying Parties.

4.4 Certificate Acceptance Procedure

4.4.1 Certificate Acceptance Criteria

(1) After the GRCA and NDC check the content of the self-signed certificate and self-issued certificate and finds the content to be

error-free, the self-signed certificate and self-issued certificate are published in the repository.

(2) After the CA receives the approved certificate application documents, the official documents attached to the certificate must be examined to verify the correctness of the certificate content. If there are no errors in the certificate content, the CA shall reply by official document to complete the certificate acceptance procedure. The CA does not accept the certificate with 30 calendar days, it shall be deemed as refusal of acceptance. In this case, the GRCA shall revoke the certificate without further announcement.

4.4.2 GRCA Certificate Publication

After the GRCA receives a reply to the certificate acceptance document sent by the CA, the issued CA certificate is published in the repository.

4.4.3 GRCA Notifications to Other Entities

The GRCA performs new certificate notification work in accordance with various operating system, browser and software platform root certification program regulations.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

(1) Key pair generation should conform to the provisions of section 6.1.1 Key Pair Generation and the subscriber must have sole

possession of the private key control rights.

(2) The subscriber's private key may not used with the issued certificate.

(3) The subscriber shall protect against unauthorized use or disclosure of the private key.

(4) Ensure that the private key is used for recording key usages on the certificate extension field.

(5) Certificate must be used in accordance with CP stated on the certificate.

4.5.2 Relying Parties Public Key and Certificate Usage

(1) Relying parties must conform to the provisions of the CPS during certificate use.

(2) Relying parties shall check the CP of the issuing CA and subscriber certificate to verify the assurance level of the certificate.

(3) Relying parties shall verify the validity of the certificate status including the certificate and all CA certificates linking the certificate. Of these, the certificate status information may be obtained through CARL, CRL or OCSP inquiry services. The CARL or CRL download websites can be obtained from the CRL Distribution Point (CDP) extension field on the certificate. The OCSP inquiry service website may be obtained from the Authority Information Access (AIA) extension field on the certificate.

(4) The certificate can be used to perform the following work after certification validity is confirmed:

- Verify the integrity of the digital signature on electronic documents.
- Verify the identity of document signature generator.
- Establish a secure communication channel with the subscriber.

4.6 Certificate Extension

(1) CA certificates may not be extended.

(2) The CA may provide subscriber certificate extension service if so demanded. The subscriber certificate extension period is set according to the CP section 6.3.2.2 Subscriber Public Key and Private Key Usage Period.

4.6.1 Circumstances under which a Certificate may be Extended

Not applicable.

4.6.2 Certificate Extension Applicants

Not applicable.

4.6.3 Certificate Extension Procedure

Not applicable.

4.6.4 Certificate Extension Issuance Notification to CA

Not applicable.

4.6.5 Certificate Extension Acceptance Criteria

Not applicable.

4.6.6 CA Certificate Extension Announcement

Not applicable.

4.6.7 Certificate Extension Issuance Notification by CA to Other Entities

Not applicable.

4.7 Certificate Rekey

4.7.1 Circumstances under which a CA Rekey is Performed

The CA private key must be regularly replaced in accordance with the provisions of the section 6.3.2 Public Key and Private Key Usage Period. After the CA certificate is revoked, use of its private key is terminated. After the key pairs are replaced, a new certificate can be applied from the GRCA in accordance with the provisions of section 4.2 Certificate Application Procedure.

GRCA rekey is performed and new self-signed certificates are issued under the following two circumstances.

(1) Lifecycle of the current key ends.

(2) Security risk exists for current key and certificate is revoked.

CA rekey is performed under the following two circumstances:

(1) Lifecycle of the current key ends.

(2) Security risk exists for current key and certificate is revoked.

4.7.2 Certificate Re-Key Applicants

The GRCA, subordinate CA or subject CA may submit a certificate re-key application. The applicant must be the responsible person of the certificate or an authorized representative.

4.7.3 Certificate Re-Key Procedure

When a new certificate application is submitted to the GRCA during CA re-key, the re-key procedure shall follow the regulations in section 3.2 Initial Registration, section 3.3 Re-Key Request Identification and Authentication and section 4.2 Certificate Application Procedure of CPS.

4.7.4 Notification of Certificate Re-Key Issuance to CAs

Certificate re-key notification from the GRCA to the CA is performed in accordance with the regulations in section 4.3.2 CA Notification to Certificate Applicants During Certificate Issuance. If the GRCA does not approve of the re-key or is not able to perform the CA certificate re-key, the reasons why the re-key may not be performed shall be stated clearly.

4.7.5 Certificate Re-Key Acceptance Criteria

The criteria for certificate re-key acceptance is the same as those

described in section 4.4.1 Certificate Acceptance Criteria.

4.7.6 Publication of Certificate Re-Key by the CA

The publication process for certificate re-key by the CA is the same as the process described in section 4.4.2 Certificate Publication by the GRCA.

4.7.7 Notification by the GRCA to Other Entities

The process for notification by the GRCA to other entities is the same as the process described in section 4.4.3 Notification by the GRCA to Other Entities.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the provision of a new certificate and a public key whose new certificate uses the old certificate's subject when the secondary attribute information (for example: updated e-mail addresses) inside modified certificates have the same certificate subject. However, the expiry date of the new certificate and the expiry date on the old certificate are the same. After certificate is modified, the old certificate should be revoked.

If the subject name or other key identification information is changed by the CA, an application for the new certificate must be submitted in accordance with related certificate applications with the modified organization name and the old certificate is revoked. This type of situation is not considered to be a certificate modification.

4.8.2 Who May Request Certificate Modification

Certificate applicants include the GRCA, subordinate CA and root certification authorities outside the GPKI.

For certificate modification requests submitted by the GRCA, subordinate CA or subject CA, the applicant must be the responsible person of the certificate or an authorized representative.

4.8.3 Certificate Modification Procedure

For certificate modification requests submitted by the CA, the GRCA performs identification, authentication and review work in accordance with section 4.2 Certificate Application Procedure. After the certificate modification request is approved, a new certificate is issued and the old certificate is revoked.

4.8.4 Notification of Certification Modification to CAs

After the GRCA issues the certification modification, the subordinate CA or subject CA is notified by official document.

If approval is not given by the GRCA to issue the certificate with the modifications, the subordinate CA or subject CA shall by notified by official document and the reason why issuance was denied shall be clearly stated.

4.8.5 Certificate Modification Acceptance Criteria

The certificate content must be checked and official reply is sent to the GRCA when the CA accepts the certificate modification. If the subscriber information on the certificate is found to be incorrect or contains errors, the GRCA shall be informed immediately.

4.8.6 Publication of the Certificate Modification by CAs

GRCA shall regularly publish the modified certificate at the repository.

4.8.7 Notification by CA to Other Entities

Not specified.

4.9 Certificate Suspension and Revocation

The GRCA does not provide suspension services. Certificate revocation information is published in the GRCA repository.

4.9.1 Circumstances under which a Certificate is Revoked

The GRCA must submit a certificate revocation request under the following circumstances (but not limited to) :

(1) Suspect or confirmed compromise of the private key including disclosure or loss of private key data.

(2) No need to use the certificate including termination of service by the GRCA.

The subordinate CA or subject CA must submit a certificate revocation request under the following circumstances (but not limited to):

(1) Suspect or confirmed compromise of the private key including disclosure or loss of private key data.

(2) Certificate is no longer needed for use including termination of service by the GRCA or ending of GRCA jurisdiction or cross-certification relationship.

(3) Original certificate request has not been authorized or cannot be authorized retroactively.

(4) Certificate subject information listed on the certificate must be modified.

The GRCA must get advance approval from the subordinate CA or subject CA for certificate revocation under the following circumstances:

(1) Check if any content listed on the certificate is untrue.

(2) Check if there is any misuse, counterfeiting and compromise of the subordinate CA and subject CA's signature private key or failure to conform to the provisions of section 6.1.5 Key Length and section 6.1.6 Public Key Parameter Generation and Quality Check.

(3) Check if there is revocation of the subordinate CA or subject CA certificates due to GRCA misuse, counterfeiting or compromise of the GRCA private key or systems.

(4) Check for failure to issue subordinate CA or subject CA certificates in accordance with CPS procedures.

(5) Check for violation of its CPS, CCA or other relevant laws and regulations by the subordinate CA and subject CA.

(6) Compliance with notification from subordinate CA or subject CA competent authority and relevant laws and regulations.

(7) Termination of service by the GRCA, subordinate CA or subject CA and failure to arrange another certificate CA to take over the terminated services.

(8) Check for misuse of GRCA, subordinate CA or subject CA certificates.

(9) Subordinate CA or subject CA does not reply to the certificate acceptance confirmation documents within the stipulated period.

(10) Revocation or suspension following expiry of the certificate issuance rights of the GRCA, subordinate CA or subject CA and repository is no longer maintained by the CA, CARLs are not published or inquiry services are no longer provided by the OCSP.

(11) Revocation due to GRCA CP or CPS requirements.

(12) The technical contents or format of a certificate demonstrate an unacceptable risk(s) to application software providers and relying parties (e.g. : CA/Browser Forum may determine some encryption algorithm, signature algorithm or key size could results in compromise of the certificate).

If the subject name mist be modified, the GRCA has the right to review and approve the certificate revocation request.

4.9.2 Who Can Request Certificate Revocation

(1) Subordinate CAs or subject CAs wishing to revoke the certificate.

(2) GRCA, subordinate CA or subject CA competent authorities.

(3) GRCA. The GRCA may submit a certificate revocation request or perform certificate revocation under the certificate revocation circumstances provided in section 4.9.1 Circumstances under

which a Certificate is Revoked.

Moreover, subscribers, application software providers, relying parties and other third-party organizations can provide certificate problem reports and submit certificate revocation requests to the GRCA. After the GRCA receives the certificate problem report, determination of whether the certification revocation request is granted based on section 4.9.5 Time Period for the CA to Process Certificate Revocation Requests.

4.9.3 Certificate Revocation Procedure

4.9.3.1 Initiation

(1) Written application

Submit application by official document and attach certificate revocation request.

(2) Identification and authentication

The GRCA performs subordinate CA or subject CA identification and authentication procedures in accordance with section 3.2.2 Organization Identity Authentication Procedure.

(3) Document review

The GRCA reviews the related submitted documentation and information to determine the appropriateness of the certificate revocation request.

(4) Review results

The GRCA performs subsequent work in accordance with the review results including: approval of certificate revocation request,

supplemental information for the request, denial of the certificate revocation request. When the certificate revocation request is denied, the subordinate CA or subject CA should be notified by official document which clearly states the reason why the request was not approved.

4.9.3.2 Announcement and Notification

The revoked certificate is added to the CARL and published in the repository before the next publication of the CARL by the GRCA at the latest. After certification revocation, the subordinate CA or subject CA and the competent authority or responsible unit is notified by official document. The certificate status information published in the repository shall include the revoked certificate until the certificate expires.

4.9.3.3 Certificate Problem Response Mechanism

The GRCA submits a certificate problem response guidelines and instructions to subscribers, applied software providers, relying parties and other third-party organizations in the event of a suspected private key compromise, certificate misuse or counterfeit, compromise, theft or improper use of certificates, a certificate problem report can be submitted to the GRCA.

Subscribers, applied software providers, relying parties and other third-party organizations may obtain the guidelines and instructions for related reported certificate problems and submit a certificate problem report to the GRCA in accordance with these instructions.

4.9.4 Certificate Revocation Request Grace Period

If there are certificate revocation circumstances are encountered by

the GRCA, subordinate CA or subject CA as described in section 4.9.1 Circumstances under which a Certificate is Revoked, the certificate revocation request must be submitted within 10 working days at the latest. If a certificate must be revoked key compromise is suspected or confirmed by the subordinate CA or subject CA or for other security events, it must be reported to the GRCA within one hour.

If the circumstances described in section 4.9.1 Circumstances under which a Certificate is Revoked occur, advance approval must be obtained from the subordinate CA or subject CA. The GRCA may directly revoke the certificate. After the GRCA confirms the certificate revocation circumstances, the certificate revocation request may be directly submitted and the subordinate CA or subject CA is notified.

4.9.5 Time Period for the CA to Process Certificate Revocation Requests

An investigation is conducted in accordance with the following guidelines within 24 hours of receipt of the certificate problem reports to determine if the certificate revocation request is valid. If the certificate revocation request is confirmed to be valid, certification revocation work is performed in accordance with section 4.9.3 Certificate Revocation Procedure.

(1) The claimed problematic content.

(2) The number of certificate project reports for that certificate or subscriber.

(3) The entity submits the certificate problem report.

(4) Articles of related laws.

After the GRCA receives the certificate revocation request, certificate revocation-related work must be completed with 7 working days at the latest.

4.9.6 Certificate Revocation Checking Requirements for Related Parties

Before using the CARL published in the repository by the GRCA, relying parties shall first check its digital signature to verify the correctness of the CARL. Regarding relying parties inquiries into information published in the repository, the requirements are provided in section 2.4 Access Controls.

4.9.7 CARL Issuance Frequency

The CARL issuance frequency is at least once per day and the issued CARL are valid for no more than 36 hours. Updated CARL are published in the repository.

When a certificate is revoked, the GRCA shall reissue the CARL within 24 hours after the certificate revocation work is completed. The certificate revocation information is added to the CARL and published on the repository.

4.9.8 Maximum Latency for CARL Publishing

The GRCA shall publish the CARL before the nextUpdate time listed on the latest CARL.

4.9.9 On-Line Certificate Revocation / Status Checking

The GRCA provides self-issued certificate, subordinate CA and

cross-certificate revocation / status inquiry by CARL and webpage certificate downloading. OCSP inquiry services are not provided.

4.9.10 On-Line Certificate Revocation Checking Regulations

Not applicable.

4.9.11 Other Forms of Revocation Announcements

Other forms of revocation announcements are not provided.

4.9.12 Other Special Requirements Related to Key Compromise

If a subordinate CA or subject CA's private key is compromised, the GRCA shall list key compromise as the reason for certificate revocation on the published CARL.

4.9.13 Circumstances under which a Certificate is Suspended

Certificate suspension services are not provided.

4.9.14 Who Can Request Certificate Suspension

Not applicable because certificate suspension services are not provided.

4.9.15 Procedure for Certificate Suspension

Not applicable because certificate suspension services are not provided.

4.9.16 Suspension Period Restrictions

Not applicable because certificate suspension services are not provided.

4.9.17 Procedure for Certificate Resumption

Not applicable because certificate suspension services are not provided.

4.10 Certificate Status Services

4.10.1 Service Characteristics

The GRCA submits the CARL and records the CRL distribution point on the issued self-issued certificates, subordinate CA certificates and cross-certificates.

The certificate revocation information on the CARL may only be removed once that revoked certificate expires.

4.10.2 Service Availability

The GRCA maintains 7 day 24 hour uninterrupted repository system service to provide CARL. Under normal operating conditions, the recovery time for the above certificate status inquiry service function is less than 10 seconds.

The GRCA has a 7 day 24 hour response mechanism to respond to high-priority certificate problem reports. The GRCA may report the case to law enforcement authorities if deemed necessary and revoke the problematic certificate.

4.10.3 Optional Features

Not stipulated.

4.11 End of Subscription

End of subscription refers to the termination of GRCA services used by subordinate CA and subject CA including termination of the services provided to the subordinate CA and subject CA by GRCA upon certificate expiry or service termination upon subordinate CA and subject CA certificate revocation.

The GRCA shall allow the subordinate CA or subject CA not to renew by certificate revocation or certificate expiry or terminate its certificate service agreement due to the invalidation of the provisions of the CCA.

4.12 Private Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

GRCA signature private keys may not be escrowed. The GRCA also does not support subordinate CA, subject CA and subscriber private key escrow and recovery.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The GRCA does not currently support session key encapsulation and recovery.

5 Infrastructure, Security Management and Operation Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The GRCA facility is located in the Chunghwa Telecom Data Communication Branch. The construction of facility housing is consistent with facilities used to house high value and sensitive information. The facilities possess other physical security mechanisms including access control, security, intrusion detection and video surveillance to prevent unauthorized access to GRCA-related equipment.

5.1.2 Physical Access

The GRCA facility operates in accordance with assurance level 4 physical control regulations. The facility has a total of four levels of access controls. On the first and second levels, security guards perform access control at the entrance and inside the building. On the third floor, access is controlled to this floor using a card access control system. On the fourth level, a fingerprint recognition control system is used to control access for facility personnel. The fingerprint scanner uses 3D sampling technology which is capable to detecting whether the fingerprint is from a live object by fingerprint depth and color.

The access control system is able to prevent unauthorized personnel from gaining access to the facilities. A monitoring system is also installed to control cabinet access which prevents unauthorized access to any hardware, software and hardware security module.

Portable storage devices that are brought into the facility housing are checked for computer viruses or any malicious software that could endanger the GRCA system.

Non-GRCA personnel entering the facility are required to sign the entry/exit log and must be accompanied throughout by GRCA personnel.

The following checks and records must be made when GRCA personnel leave the facility to prevent unauthorized personnel from entering the facility:

(1) Check if the system equipment is operating normally.

(2) Check if the cabinet doors are locked.

(3) Check if the access control system is operating normally.

5.1.3 Power and Air Conditioning

Besides municipal power, the power system at the GRCA facility is equipped with a generator (with enough fuel for six days of continuous operation) and uninterrupted power system. The system is capable of automatically switching between municipal and generator power. At least six hours of power can be supplied for backup of repository data.

The GRCA facility has a constant temperature and humidity system to provide an optimal operation environment for the facility.

5.1.4 Flood Prevention and Protection

The GRCA facility is located at the third or higher floor of a raised foundation building. This building has a water gate and water pump protection and no history of major damage caused by flooding.

5.1.5 Fire Prevention and Protection

The GRCA facility has an automatic fire detection and alarm system with self-activating extinguishing equipment. Switches are installed at every major entrance / exit of the facility to allow manual activation by on-site personnel during emergencies.

5.1.6 Media Storage

Audit records, archives and backups are kept in storage media. Besides the one copy kept at the GRCA facility, another copy is made and kept at a secure location off-site.

5.1.7 Waste Disposal

Sensitive information and documents as well as the magnetic tapes, hard drives, floppy disks, MO and other forms of memory no longer being used by the GRCA shall be destroyed in accordance with the standards and procedures announced by the relevant government agencies in accordance with section 9.3.1 Scope of Sensitive Information.

5.1.8 Off-Site Backup

The off-site backup site is located in Taichung which is over 30 km away from the GRCA facility. The backup content includes data and system programs. At least one full data backup is performed each month. Change of information backups shall be performed on the date of the change. The off-site backup system and GRCA system have identical security levels.

5.2 Procedural Controls

The GRCA implements procedural controls to specify the trusted roles of system operations, the number of people required for each task and how each role is identified and authenticated to ensure the security of system procedures.

5.2.1 Trusted Roles

The GRCA appropriately delineates related job responsibilities to prevent undetected malicious use of the system and the job scope of each trusted role is clearly specified for each system access task.

The five GRCA trusted roles are administrator, officer, auditor, operator and controller. Personnel control and management of each trusted role is done in accordance with section 5.3 Personnel Controls to prevent internal attacks. Each trusted role may be performed by multiple persons but one person in each group shall by assigned the chief role. The tasks performed by the five roles are as follows:

(1) The administrator is responsible for:

- Installation, configuration and maintenance of the GRCA system.
- Creation and maintenance of system user accounts.
- Setting of audit parameters.
- Generation and backup of GRCA keys.
- Publication of CARL in the repository.

(2) The officer is responsible for:

- Perform certificate issuance.
- Perform certificate revocation.

(3) The auditor is responsible for:

- Checking, maintenance and archiving of audit logs.
- Conducting or supervising internal audits to ensure the GRCA is operating in accordance with CPS regulations.

(4) The operator is responsible for:

- Daily operation and maintenance of system equipment.
- System backup and recovery.
- Storage media updating.
- Software and hardware updates outside the GRCA management system.
- Network and website maintenance: Set up protection mechanisms for system security and virus threats and network security event detection and reporting capability.

(5) The physical security controller is responsible for:

- System physical security controls (including facility access controls, fire prevention, flood prevention and air conditioning systems).

5.2.2 Number of Personnel Required for each Task

In accordance with security requirements, the number of people needed for each trusted role is as follows:

(1) Administrator: At least 3 qualified individuals are needed.

(2) Officer: At least 3 qualified individuals are needed.

(3) Auditor: At least 2 qualified individuals are needed.

(4) Operator: At least 2 qualified individuals are needed.

(5) Physical security controller: At least 2 qualified individuals are needed.

The number of people assigned to perform each task is as follows:

Assignments	Administrator	Officer	Auditor	Operator	Physical Security Controller
Installation, configuration and maintenance of the GRCA system	2				1
Establishment and maintenance of GRCA certificate management system user accounts	2				1
Set audit parameters	2				1
Generation and backup of GRCA keys	2		1		1
Perform certificate		2			1

Assignments	Administrator	Officer	Auditor	Operator	Physical Security Controller
issuance					
Perform certificate revocation		2			1
Publish CARLs in the repository	1				1
Checking, maintenance and archiving of audit logs			1		1
Daily operation and maintenance of system equipment				1	1
System backup and recovery				1	1
Storage media updating				1	1
Hardware and software updates outside the GRCA certificate management system				1	1
Maintenance of the network and website				1	1

5.2.3 Identification and Authentication for each Role

User account numbers, passwords, group account number management function and IC cards are used by the GRCA to identify and authenticate administrator, officer, auditor, operator roles and a central access system authorization setting functions are used to identify and authenticate the physical security controller.

5.2.4 Role Responsibility Assignment

The GRCA has defined five types of trusted roles in accordance with the provisions of section 5.2.1 Trusted Roles. Role assignment must conform to the following rules:

(1) A person may only assume one of the administrator, officer and auditor roles, but the person may also assume the role of operator.

(2) The physical security controller may not concurrently assume any of the other four roles.

(3) A person serving a trusted role is not allowed to perform self-audits.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience and Security Requirements

(1) Personnel selection and security evaluation on entry personnel

- Personality evaluation.

- Applicant experience evaluation.
- Academic and professional skills and qualifications evaluation.
- Personnel identity check.
- Trustworthiness evaluation.

(2) Personnel Evaluation Management

Qualification reviews of relevant GRCA personnel shall be performed prior to the initial time of employment to verify their qualifications and work capabilities. After formal employment, personnel must receive suitable instruction and training and sign a document accepting responsibility to perform certain duties. Qualifications are rechecked every year. Personnel which do not pass the qualification are reassigned to another position and a qualified person shall be assigned to serve in that position.

(3) Appointment, Dismissal and Transfer

Personnel are still required to fulfill their duty of confidentiality even if there are changes to the hiring terms, employment terms or contract especially severance and termination of employment contracts.

(4) Duty of Confidentiality Agreement

GRCA work personnel shall fulfill of duty of confidentiality and sign a confidentiality agreement stating that work personnel may not disclose sensitive information verbally or by photocopy, loan, delivery, publishing or other methods.

5.3.2 Background Check Procedures

The GRCA shall conduct qualification checks on the personnel performing the trusted roles defined in section 5.2.1 Trusted Roles to verify the identity, qualification and related certification documents prior to employment.

5.3.3 Education and Training Requirements

Trusted Role	Education and Training Requirements
Administrator	1. GRCA security certification mechanism 2. Installation, configuration and maintenance of the GRCA system. 3. Establishment and maintenance of operation procedures for system user accounts. 4. Operation procedure for audit parameter configuration. 5. Operation procedure for GRCA key generation and backup. 6. Post-disaster recovery and continuous operation procedure.
Officer	1. GRCA security certification mechanism. 2. GRCA system software and hardware use and operation procedure. 3. Certificate issuance operation procedure. 4. Certificate revocation operation procedure. 5. Post-disaster recovery and continuous operation rocedure.
Auditor	1. GRCA security certification mechanism.

	2. GRCA system software and hardware use and operation procedure. 3. GRCA key generation and backup operation procedure. 4. Audit log checking, upkeep and archiving procedure. 5. Post-disaster recovery and continuous operation procedure.
Operator	1. System backup and recovery operation procedure. 2. Maintenance procedure for the daily operation of system equipment. 3. Storage media upgrading procedure. 4. Post-disaster recovery and continuous operation procedure. 5. Network and website maintenance procedure.
Physical security controller	1. Physical access authorization setting procedure. 2. Post-disaster recovery and continuous operation procedure.

5.3.4 Retraining Requirements and Frequency

For hardware / software upgrades, work procedure changes, equipment replacement and amendments to related regulations, the GRCA shall schedule retraining for relevant personnel and record the training status to ensure that related work procedures and amended regulations are understood.

5.3.5 Job Rotation Frequency and Sequence

(1) Administrators may be reassigned to the position of officer or auditor after departure from their original position for one full year.

(2) Officers may be reassigned to the position of administrator or auditor after departure from their original position for one full year.

(3) Auditors may be reassigned to the position of administrator or officer after departure from their original position for one full year.

(4) Only operators with two full years of experience who have received the requisite training and passed review may be reassigned to the position of administrator, officer or auditor.

5.3.6 Sanctions for Unauthorized Actions

The GRCA shall take appropriate administrative and disciplinary actions against personnel who have committed violations of the CP, CPS or other procedures announced by GRCA. In the event of serious violations that have resulted in damages, appropriate legal action shall be taken.

5.3.7 Contract Personnel Regulations

In addition to signing related confidentiality agreements, the contract personnel employed by the GRCA must have sufficient knowledge and skills, follow the code of conduct and perform work in accordance with the provisions of the CPS.

5.3.8 Supplied Documentation

The GRCA shall provide the CP, technical specifications, this CPS, system operation manuals and documents related to the Electronic Signature Act to relevant personnel.

5.4 Security Audit Procedure

The GRCA shall keep security audit logs for all events related to GRCA security. The security audit logs shall be recorded by automatic system generation, in logbooks or by paper record. All security audit logs shall be retained and made available during compliance audits. Security audit logs are kept in accordance with the provisions in section 5.5.2 Retention Period for Archived Logs.

5.4.1 Types of Recorded Events

(1) Security audit

- Any changes to major audit parameters such as audit frequency, audit event types and the content of new / old parameters.
- Any attempts to delete or modify audit logs.

(2) Identification and Authentication

- Successful or failed attempt to set up a new role.
- Change of maximum number of identification attempts allowed.
- Maximum number of failed identification attempts by user logging into the system.
- Administrator fails a number of identification attempts and is locked out of account.
- Administrator changes the system identification system such as changing from access password to biometrics.

(3) Key generation

- During GRCA key generation.

(4) Private key importation and storage

- Importation of private key into system component.

(5) Addition, deletion or storage of a trusted public key.

- Change to addition, deletion or storage of a trusted public key.

(6) Private key export

- Export of private keys other than single use or single-use restricted keys.

(7) Certificate registration

- Certificate registration request procedure.

(8) Certificate revocation

- Certificate revocation request procedure.

(9) Certificate status change approval

- Approval or rejection of certification status change request.

(10) GRCA configuration

- GRCA security-related configuration changes.

(11) Account management

- Addition or deletion of roles or users.

- User account or role access authority modifications.

(12) Certificate profile management

- Certificate profile changes.

(13) CARL profile management

- CARL profile changes.

(14) Other

- Installation of operating system.
- Installation of GRCA system.
- Installation of hardware security modules.
- Removal of hardware security modules.
- Destruction of hardware security modules.
- System activation.
- Attempt to log into GRCA certificate management work.
- Hardware and software acceptance.
- Attempt to set access passwords.
- Attempt to modify access passwords.
- GRCA internal data backup.
- GRCA internal data recovery.
- File generation, renaming and transfer operations.
- Transfer to any information to storage in the repository.

- Access to GRCA internal database.
- Report of any certificate compromise.
- Loading certificate on token.
- Token passing.
- Token zeroization.
- GRCA or subject CA re-key.

(15) GRCA server setting modifications

- Hardware.
- Software.
- Operating system.
- Patches.
- Security profiles.

(16) Physical access and site security

- Personnel access to the GRCA facility.
- Access to the GRCA server.
- Known or suspected violation of physical security regulations.

(17) Anomalies

- Software error.
- Failure of software integrity check.

- Receipt of unsuitable information.
- Abnormal routing message.
- Suspect or confirmed network attack.
- Equipment failure.
- Improper electrical power.
- UPS failure.
- Significant or major network service and access failure.
- CP violation.
- Violation of this CPS.
- Reset of system clock.

5.4.2 Frequency of Log Processing

The GRCA shall review the audit log once per month as well as track and investigate major events. Review work includes checking the audit logs for tampering, reviewing all log items and checking the content for any alerts or abnormalities. The audit checking results shall be documented.

5.4.3 Retention Period for Audit Logs

Audit logs are retained for two months and the log retention management system shall be operated in accordance with the log retention management system regulations in section 5.4.4 Protection of Audit Log, section 5.4.5 Audit Log Backup Procedure, section 5.4.6 Audit Log Collection System and 5.5 Log Archiving.

Auditors are responsible for removing the data when the audit log retention period has ended. Other personnel may not perform this work on their behalf.

5.4.4 Protection of Audit Logs

(1) Use signature and encryption technology to preserve current and archived audit records and use CD-R or other non-modifiable media to store the audit logs.

(2) Private keys used to sign event logs may not be reused for other purposes. Audit system private keys are prohibited from being used for other purposes. Disclosure of audit system private keys is not permitted.

(3) Manually prepared audit logs must be kept in a secure location.

5.4.5 Audit Log Backup Procedures

Electronic audit logs are backed up once per month.

(1) GRCA event log backup cycle: The audit system performs daily, weekly and monthly automatic archiving of audit logs.

(2) The GRCA shall store the event logs in a secure location.

5.4.6 Audit Log Collection System

The audit system is established internally in the GRCA system. The audit procedure is initiated when the GRCA system is activated and only stops operation when the GRCA system is shut down.

If the automatic audit system cannot operate normally and the

security system which protects the integrity, confidentiality of system data is in a state of high risk, the GRCA shall suspend certificate issuance services and service shall only be resumed after the problem is solved.

5.4.7 Notification to Event-Causing Entity

The audit system does not need to notify the event-causing entity if the events that have recorded by the audit system.

5.4.8 Vulnerability Assessments

(1) Operating system vulnerability assessment.

(2) Physical facilities vulnerability assessment.

(3) Certificate management system vulnerability assessment.

(4) Network vulnerability assessment.

5.5 Record Archival

5.5.1 Types of Archived Records

(1) Reviews of GRCA accreditation information (provided it is used) by competent authorities.

(2) CPS.

(3) CCA.

(4) System and equipment configurations.

(5) System or configuration modifications and updates.

(6) Certificate application data.

(7) Revocation request data.

(8) Certificate acceptance confirmation documents.

(9) Issued or published certificates.

(10) GRCA re-key records.

(11) Issued or published CARLs.

(12) Audit logs.

(13) Other explanatory information or application program used for the verification and authentication of archived information.

(14) Documents requested by audit personnel.

(15) Organization and individual identification and authentication information defined in the provisions of section 3.2.2 Organization Identification and Authentication Procedure and section 3.2.3 Individual Identification and Authentication Procedure.

5.5.2 Retention Period for Archived Records

The retention period for GRCA file records is 20 years. The application programs used to process file records are kept for 20 years.

After the file record retention period ends, written information shall be destroyed in a safe manner. Information in electronic form must be backed up in other storage media. Suitable protection must be provided or the information must be destroyed in a safe manner.

5.5.3 File Record Protection

(1) Amendments, modifications or deletion of archived records is not allowed.

(2) Archived records may be transferred to another storage media as long as suitable protection is provided and its protection level is no lower than the original protection level.

(3) Archived records shall be kept is a secure location.

5.5.4 Archived Record Backup Procedure

Archived records shall be backed up at the off-site backup center in accordance with the provisions of section 5.1.8 Offsite Backup.

5.5.5 Record Timestamping Requirements

For records archived in electronic form such as certificates, CARLs and audit logs, the timestamping information on each record shall include the date and time information and use suitable digital signature protection which can be used to check the date and time information on the record for alternation. However, the date and time information on the electronic records is the date and time of the computer operating system and not the electronic timestamping information provided by a trusted third party. Calibration of all GRCA computer systems must be performed at regular intervals to ensure the accuracy and trustworthiness of the date and time information on electronic records.

Time information shall be recorded when necessary on archived written records containing date information. The date and time information on records may not arbitrarily altered. Audit personnel must

sign and verify if any alteration is needed.

5.5.6 Archived Record Collection System

The GRCA has no archived record collection system.

5.5.7 Procedures to Obtain and Verify Archived Records

Archived records may be obtained after a written application is submitted and formal authorization is received.

Audit personnel are responsible for verification of archived records. The authenticity of signatures and dates on electronic files must be verified.

5.6 Key Changeover

The GRCA may replace the key pair used to issue certificates and issue one new self-signed certificate and two self-issued certificates at the latest 3 months prior to the expiry of the private key use period. The newly issued self-signed certificate is sent to relying parties in accordance with section 6.1.4 GRCA Public Key Secure Transmission to Relying Parties. The self-issued certificates are published in the repository to allow downloading by relying parties.

Subject CAs may replace the key pair used to issue certificates at the latest 2 months prior to the expiry of the CA's own certificate. After the subject CA replaces the key pair, a new certificate application may be submitted in accordance with section 4.1 Certificate Application.

5.7 Key Compromise or Post-Disaster Recovery

Procedure

5.7.1 Emergency and System Compromise Handling Procedure

The GRCA establishes reporting and handling procedures for emergency and system compromise. The related recovery procedures must be implemented based on the type of emergency or system compromise. Annual drills must be held each year in accordance with this procedure and data backup must be performed at regular intervals.

5.7.2 Computing Resources, Software and Data Corruption Recovery Procedure

The GRCA establishes recovery procedures for computer resource, software and data corruption and holds annual drills in accordance with this procedure.

If the GRCA's computer equipment is damaged or unable to operate but the signature key has not been destroyed, priority shall be given to restoring repository operation and rapidly reestablishing certificate issuance and management capabilities.

5.7.3 GRCA Signature Key Compromise Recovery Procedure

The GRCA establishes signature key compromise recovery procedure and holds annual drills in accordance with this procedure,

5.7.4 GRCA Post-Disaster Continuing Operations

The GRCA conducts annual post-disaster recovery drills to secure

facilities.

5.7.5 GRCA Revoked Signature Key Certificate Recovery Procedure

The GRCA establishes revoked signature key certificate recovery procedure and holds annual drills in accordance with this procedure.

5.8 GRCA Service Termination

The GRCA shall handle service termination matters in accordance with the provisions of the Electronic Signature Act during service termination.

The GRCA shall follow the items below in order to reduce the effect on subject CAs and relying parties during service termination:

(1) The GRCA shall notify the subject CA and publish to the repository three months prior to the scheduled service termination date except when notification cannot be made.

(2) The GRCA must revoke all unrevoked or unexpired certificates upon service termination and perform safekeeping and transfer work for file records in accordance with relevant provisions in the Electronic Signature Act.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The GRCA generates key pairs within the hardware security module in accordance with the provisions of section 6.2.1 Cryptographic Module Standards and Controls and adopts FIPS140 compliant random number generators and RSA key algorithms. After the private keys are generated within the hardware security module, key output and input must be performed in accordance with the provisions of section 6.2.2 Key Multi-Person Control and section 6.2.6 Private Key Transfer into and from a Cryptographic Module.

GRCA key generation is witnessed by relevant personnel who have signed a Key Initiation Witness document (public key corresponding to the generated key is listed) and video of the key generation process is kept. The public key is published via trusted channels to establish trust.

Subordinate CA and subject CA must perform key pair generation in accordance with the provisions of the CP.

The GRCA shall check the public check in the certificate application file when issuing a subordinate CA and subject CA to ensure the uniqueness of the CA's public key.

The GRCA only issues self-signed certificates, self-issued certificate, subordinate CA certificates and cross-certificates and does not issue subscriber certificates (including SSL certificates).

6.1.2 Private Key Delivery to Subordinate CA and Subject CA

The GRCA does not need to send private keys to subordinate CA and subject CA. The subordinate CA and subject CA must generate private keys on their own.

6.1.3 Secure Delivery of Public Keys to the GRCA

CAs must submit the certificate application in PKCS#10 certificate application file format for secure delivery of the public key to the GRCA.

6.1.4 GRCA Public Key Secure Delivery to Relying Parties

GRCA self-signed certificates contain its public key. There are the following types of distribution channels:

(1) After the GRCA gives the issued subordinate CA certificate to a subordinate CA or issued cross-certificate to a subject CA, the subordinate CA certificate or cross-certificate shall be delivered along with the GRCA self-signed certificate or public key to the CA. This CA stores the GRCA self-signed certificate or public key into the token (such as IC card) and then securely delivers the token to the CA's subscriber or relying party.

(2) GRCA self-signed certificates are stored in the built-in software issued by a trusted third party. Certificate users obtain this software via the secure channel (for example, purchase of a software installation CD from reliable distributors). After installation, the GRCA self-signed can be obtained.

(3) For large issues of CD-ROMs with GRCA self-signed public key

certificates, users who have obtained these CD-ROMs via secure channels will also receive the self-signed certificate from the GRCA.

(4) During GRCA activation, a public key shall be published concurrently. Related personnel shall sign GRCA public key witness forms and they shall be delivered by media for publication. Relying parties can compare the GRCA public key published through this media to the one contained in the GRCA self-signed public key certificate downloaded from the Internet.

6.1.5 Key Sizes

The GRCA uses 4096-bit RSA keys and SHA-256, SHA-384 or SHA-512 hash function to issue certificates and CARL.

First generation GRCA still provide SHA-1 and SHA-256 hash function CARL to provide relying parties with the ability to check issued SHA-1 and SHA-256 hash function subordinate CA certificate or cross-certificate status. SHA-1 hash function CARLs provided to first generation GRCA use SHA-1 hash function to issue subordinate CA and cross-certificate expiry dates or the subordinate CA and subject CA no longer provides certificate and CRL issuance service. Generation 1.5 and above GRCA use SHA-256, SHA-384 or SHA-512 hash functions to issue certificate and CARL.

Subordinate CAs and Subject CAs must select a suitable key length in accordance with CP regulations. The GRCA will check if the CA has selected the proper key size before issuing the subordinate CA certificate or cross-certificate.

If elliptic curve cryptography (ECC) is use to issue certificates, the

key size must conform to NIST P-256, P-384 or P-521.

6.1.6 Public Key Parameter Generation and Quality Checking

The public key parameter of the RSA algorithm is Null.

The GRCA and subordinate CA uses the ANSI X9.31 algorithm or FIPS 186-4 standard to generate the prime numbers used in the RSA algorithms. This method can guarantee that the generated prime numbers are strong prime.

Subject CA must perform quality checking of suitable key parameters using the algorithm it has selected.

According to NIST SP 800-89 section 5.3.3, the GRCA verifies that the public exponent value is greater than 3 odd numbers and this value is between $2^{16}+1$ and $2^{256}-1$. In addition, the modulus has an odd number, non-prime number exponential power and a factor no less than 752.

If ECC is used in the future to issue certificates, GRCA shall follow sections 5.6.2.3.2 and 5.6.2.3.3 in NIST SP 56A Revision 2 when checking all ECC Full Public Key Validation Routine and ECC Partial Public Key Validation Routine key validity periods.

6.1.7 Key Usage Purposes

The private key corresponding to the GRCA self-signed certificate can only be used for issuing certificates and CARLs. Newly issued self-signed certificates by second generation and above GRCA must contain the KeyUsage extension field.

For certificates issued by the GRCA to subordinate CA and subject

CA, the key usage bits in the certificate key usage extension field are set to keyCertSign and cRLSign.

6.1.8 Key Generation by Hardware / Software

The GRCA uses hardware cryptographic modules to generate random numbers, public keys and symmetric keys in accordance with the provisions of section 6.2.1 Cryptographic Module Standards and Controls.

Subordinate CA and subject CA must follow CP regulations when selecting suitable software and hardware for key generation. Before subordinate CA and cross-certificates are issued, the GRCA shall check if the CA has selected appropriate software and hardware.

6.2 Private Key Protection and Cryptographic Module Security Control Measures

6.2.1 Cryptographic Module Standards and Controls

In accordance with CP cryptographic module standards and controls, the GRCA uses hardware security modules with a FIPS140-2 assurance level 3 to generate random numbers and key pairs.

The subordinate CA and subject CA must follow CP regulations when selecting a cryptographic module. Before subordinate CA certificate and cross-certificate are issued, the GRCA shall check whether the CA has selected a cryptographic module with an appropriate security level.

6.2.2 Key Splitting Multi-Person Control

GRCA key splitting multi-person control uses m-out-of-n LaGrange Polynomial Interpolation. It is a type of perfect secret sharing method which can be used for private key splitting and recovery. Where, n and m must be values equal or greater than 2 and n must be less or equal to m. Use of this method can provide maximum security for GRCA private key multi-person control. It can also be used for private key activation.

If GRCA wishes to issue a private key for CA digital signature use with an assurance level 3 or 4, the multi-person control procedure must follow CP regulations. Before the subordinate CA certificate and cross-certificate is issued, the GRCA shall check if the multi-person control procedure used by the CA is appropriate.

6.2.3 Private Key Escrow

The GRCA private key used for signatures cannot be escrowed. The GRCA is not responsible for the safekeeping of subordinate CA and subject CA signature private keys.

6.2.4 Private Key Backup

According to the provisions of section 6.2.2 Key Splitting Multi-Person Control, the GRCA uses key splitting multi-person control methods to backup the private key. Highly secure IC cards are used as the storage media for secret sharing.

Subordinate CA and subject CA must follow CP regulations when selecting a suitable private key backup method. Before the subordinate CA or cross-certificate is issued, the GRCA shall check if the private key

backup method selected by the CA is appropriate.

The GRCA is not responsible for the safekeeping of the private key backups made by subordinate CAs and subject CAs.

6.2.5 Private Key Archiving

GRCA private keys used for digital signatures cannot be archived. The GRCA does not archive the signature private keys for the subordinate CA and subject CA.

6.2.6 Private Key Transfer into and from a Cryptographic Module

The GRCA must only import private keys into the cryptographic modules when performing key backup recovery or cryptographic module replacement. The multi-person control method should be used together with the generation and backup of GRCA key tasks to import private keys into the cryptographic module. Encryption or key splitting may be used as the private key import method to ensure that the key plain code is not exposed outside the cryptographic module during the importation process. The related secret parameters generated during the importation process must be completely destroyed.

If private key importation cryptographic module is needed, the subordinate CA and subject CA must select an appropriate private key importation method in accordance with CP regulations. Before the subordinate CA certificate or cross-certificate is issued, the GRCA must check if an appropriate private key importation method has been selected by the CA.

6.2.7 Private Key Storage in the Cryptographic Module

The GRCA shall store private keys in the cryptographic module in accordance with the provisions of section 6.1.1 Key Pair Generation and section 6.2.1 Cryptographic Module Standards and Controls.

6.2.8 Methods for Activating Private Keys

The GRCA RSA private key activation is controlled by m-out-of-n control IC cards. Control IC cards with different usages are kept by the administrator and officer.

Subordinate CA and subject CA must follow CP regulations when selecting an appropriate private key activation method. Before the subordinate CA certificate or cross-certificate is issued, the GRCA must check if an appropriate private key activation method has been selected by the CA.

6.2.9 Methods for Deactivating Private Keys

The GRCA key pairs are kept in an deactivated state to prevent illegal use of private keys.

After the issuance and related management work for each certificate is completed, the private key shall be deactivated using the m-out-of-n method.

Subordinate CA and subject CA must follow CP regulations when selecting a suitable private key deactivation method. Before the subordinate CA certificate or cross-certificate is issued, the GRCA must check if an appropriate private key deactivation method has been selected by the CA.

6.2.10 Methods for Destroying Private Keys

In order to prevent the theft of old GRCA private keys which could affect the authenticity of certificates, the old GRCA private keys must be destroyed once they expire. When the GRCA completes the key changeover and obtains the new certificate and the old private key is no longer used to issue any other certificates or CARLs, zeroization is performed on the old private key stored inside the hardware cryptographic module to ensure that the old private key inside the cryptographic module is destroyed.

Subordinate CA and subject CA must follow CP regulations when selecting a suitable private key destruction method. Before the subordinate CA certificate or cross-certificate is issued, the GRCA must check if an appropriate private key destruction method has been selected by the CA.

6.2.11 Cryptographic Module Level

The cryptographic module level is determined in accordance with the provisions of section 6.2.1 Cryptographic Module Standards and Controls.

6.3 Other Key Pair Management Regulations

The subordinate CA and subject CA must administer key pairs on their own. The GRCA is not responsible for the safekeeping of the subordinate CA and subject CA private keys.

6.3.1 Public Key Archiving

The GRCA shall perform certificate archiving work in accordance

with section 5.5 Record Archiving and implement security controls on the archiving system. No further public key archiving is performed.

6.3.2 Usage Periods for Public and Private Keys

6.3.2.1 Usage Periods for GRCA Public and Private Keys

The RSA key sizes for GRCA public and private keys are 4096 bits. The maximum usage period is 30 year and the maximum usage period for private keys used for certificate issuance is 10 years.

6.3.2.2 Usage Periods for Subordinate CA Public and Private Keys

The RSA key sizes for subordinate CA public and private keys are 2048 bits. The maximum usage period for public key certificates and private keys is 20 years and maximum usage period for private keys used for certificate issuance is 10 years.

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

6.3.2.3 Usage Periods for Subject CA Public and Private Keys

The RSA key sizes for subject CA public and private keys are 2048 bits. The maximum usage period for public key certificates and private keys is 20 years and maximum usage period for private keys used for certificate issuance is 10 years.

The total of the certificate lifespan for certificates issued by the GRCA to subject CA plus the lifespan of the signature private key that the

GRCA uses to sign certificates may not exceed the GRCA self-signed certificate lifespan.

6.4 Protection of Activation Data

6.4.1 Activation Data Generation and Installation

GRCA activation data is generated by the hardware security module and then stored in a m-out-of-n control IC card. The activation data in the IC card is directly accessed by built-in card readers in the hardware security module and the IC card PIN number is directly input using the keyboard contained in the hardware cryptographic module.

Subordinate CA and subject CA must follow CP regulations when selecting a suitable activation data generation method. Before the subordinate CA certificate or cross-certificate is issued, the GRCA must check if an appropriate activation data generation method has been selected by the CA.

6.4.2 Protection of Activation Data

GRCA activation data is protected by the m-out-of-n control IC card. IC card PIN numbers are kept by custodians. If there are over three failed logins, the IC card is locked and a new custodian must create new PIN numbers.

Subordinate CA and subject CA must follow CP regulations when selecting a suitable activation data protection method. Before the subordinate CA certificate or cross-certificate is issued, the GRCA must check if an appropriate activation data protection method has been selected by the CA.

6.4.3 Other Activation Data Rules

Not stipulated.

6.5 Computer Hardware and Software Security Measures

6.5.1 Specific Technical Requirements for Computer Security

The GRCA and related auxiliary systems provides the following security control functions by means of the operating system or jointly through the operating system, software and physical protection measures:

(1) Identity authentication login.

(2) Self-discretionary access control.

(3) Security audit capability.

(4) Access control restrictions to certificate services and trusted roles.

(5) Identify and authenticate trusted roles and identities.

(6) Ensure security of each communication and databases with password technology.

(7) Provide secure and reliable channels for trusted roles and related identification.

(8) Offer procedure integrity and security control protection.

6.5.2 Computer Security Rating

The GRCA uses computer systems with security strengths equivalent to C2 (TCSEC), E2 (ITSEC) or EAL3 (CC,ISO/IEC 15408) computer operating systems.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

GRCA system development follows the quality management standards of competent authorities to perform development and quality controls.

The GRCA hardware and software were designed for dedicated use and may only utilize components that have received security authorization. No unrelated hardware or devices, network connections or software components may be installed or operated to prevent malicious software from being introduced. Checks for malicious code are performed by the GRCA during each use.

6.6.2 Security Management Controls

The first time any software is installed, the GRCA checks that the vendor has provided the correct and unmodified version of the software. After installation into the system, the GRCA checks the software integrity during each use.

The GRCA shall record and control the system configuration, record any modifications or function upgrades and test for unauthorized modifications of system software or configurations.

6.6.3 Lifecycle Security Ratings

At least one key compromise risk assessment shall be conducted each year.

6.7 Network Security Controls

GRCA servers and its internal repository are not connected to external networks. The external repository is connected to the Internet to permit uninterrupted provision of certificate and CARL search services except when necessary maintenance or backup is being performed.

The information in the GRCA internal repository (including certificates and CARLs) is protected by digital signature and transferred manually from the internal repository to the external repository.

The GRCA external repository prevents denial of service attacks and intrusions with system patch file updates, system vulnerability scanning, intrusion detection, firewall systems and filtering routers.

6.8 Time Stamping

The GRCA regularly conducts system synchronization with a reliable time source to maintain the correctness of system time and ensure the accuracy of the following times:

(1) Certificate issuance times.

(2) Certificate revocation times.

(3) CARL issuance times.

(4) System event occurrence times.

Automatic or manual procedures may be used to adjust the system time. Clock synchronizations must be audited.

6.9 Cryptographic Modules Security Controls

GRCA cryptographic module security controls are handled in accordance with the provisions of section 6.1 Key Pair Generation and Installation and section 6.2 Private Key Protection and Cryptographic Modules Security Controls.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

The certificates issued by the GRCA conform to the current versions of the ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, IETF PKIX Working Group RFC 5280 and other regulations.

The GRCA uses a cryptographically secure pseudorandom number generator (CSPRNG) to generate the certificate serial numbers. These serial numbers are non-sequential positive integers at least 64 bits in size.

7.1.1 Version Numbers

The GRCA issues X.509v3 version certificates in accordance with RFC5280 and ITU-T standards.

7.1.2 Certificate Extensions

The certificate extensions of the certificates are issued by the GRCA in accordance with ITU-T X.509, CA/Browser ForumBaseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and IETF PKIX Working Group RFC 5280 regulations.

There are four types of certificates issued by the GRCA: self-signed certificates, self-issued certificates, subordinate CA certificates and cross-certificates. The required extensions used by each type of certificate, its critical fields and content are described in GPKI and CRL profile documents.

When other optional extension fields are used under different

situations, they are used in accordance with the above standards. If a new extension field must be added, the GPKI and CRL profile is revised with the newly added extension field use, criticality, handling method and field setting.

In addition, the GRCA is not allowed to sign certificates under the following two circumstances:

(1) The certificate extension field contains settings that cannot be applied to the public internet. For example, extended key usage extension fields that include private network service settings.

(2) The certificate content may mislead the relying parties into believing certificate information contains semantics which have already been verified by the GRCA.

The GRCA does not perform subscriber certificate issuance work and does not conduct pre-certificate issuance as defined in RFC 6962.

7.1.3 Algorithm Object Identifiers

The algorithm OIDs used for signatures on GRCA issued certificates are:

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

(OID：1.2.840.113549.1.1.11)

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

(OID：1.2.840.113549.1.1.12)

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

(OID：1.2.840.113549.1.1.13)

The algorithm OID used for the subject keys in GRCA issued certificate is:

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

(OID：1.2.840.113549.1.1.1)

7.1.4 Name Forms

The subject and issuer fields of the certificate must use the X.500 distinguished name and name attribute type shall comply with the current version of the ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and IETF PKIX Working Group RFC5280 or other regulations.

The content of the issuer fields of the GRCA issued self-issued certificates, subordinate CA certificates and cross-certificates must be the same as the subject field content of the self-signed certificate.

In order to facilitate international interworkability, the GRCA plans to include the commonName, organizationName and countryName in the subject distinguished name starting from third generation self-signed certificates.

(1) commonName

Used to record the identifiable GRCA name. This name is the unique identifier of this certificate which can be used to distinguish it from other certificates.

(2) organizationName

Used to record the formal organization name subordinate to the GRCA. Organization identity authentication is performed in accordance with section 3.2.2 Organization Identity Authentication Procedure.

There may be some slight differences between the organizationName and name being verified during identity authentication. For example, abbreviations of some words in organization names may be adjusted to conform to the nationally accepted abbreviation methods.

(3) countryName

Used to record the country where the GRCA's place of business is located and expressed in a manner that conforms to the country codes specified in the ISO 3166-1 international standard.

The self-issued certificates, subordinate CA certificates and cross-certificates issued by the GRCA states that the verification was performed in accordance with procedures set forth in the CP and / or CPS have been followed prior to the certificate issuance date to ensure that all recorded subject information values are correct.

7.1.5 Name Constraints

Name constraints are not used on certificates issued by GRCA.

7.1.6 Certificate Policy Object Identifier

GRCA self-signed certificates do not contain the certificatePolicies

extension. The certificate policy field for GRCA self-issued certificates, subordinate CA certificates and cross-certificates not only must use the certificate policy object identifier field but also may contain OV SSL certificate OID 2.23.140.1.2.2 defined by the CA/Browser Forum.

7.1.7 Use of Policy Constraints Extension

Subordinate CA certificates and cross-certificates issued by the GSRCA may use the policy constraints extension when necessary.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by the GRCA do not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

A ‘critical or not’ note must be made for the CP extension field contained in GRCA issued certificates in accordance with the GPKI certificate and CARL profile regulations.

7.2 CARL Profile

7.2.1 Version Numbers

GRCA issues CARLs that comply with RFC5280 and version X.509 v2 version.

7.2.2 CARL and crlEntry Extensions

The CARLs, crlExtensions and crlEntryExtensions issued by the GRCA shall comply with the current versions of ITU-T X.509,

CA/Browser Forum issues Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, IETF PKIX Working Group RFC 5280 and other regulations.

The content of the CARL extension is described in GPKI certificate and CRL profiles.

7.3 OCSP Profile

The GRCA does not provide OCSP inquiry services which comply to IETF PKIX Working Group RFC 6960 and RFC 5019 standards.

7.3.1 Version Numbers

Not applicable.

7.3.2 OCSP Extensions

Not applicable.

8 Compliance Audit and Other Assessment Methods

8.1 Audit Frequency or Assessment Items

The GRCA receives one GPKI external audit and internal audit each year to ensure that related operations are in compliance with the security regulations and procedures in this CPS.

8.2 Identity and Qualifications of Audit Personnel

The NDC shall retain auditors who are familiar with related infrastructure regulations and GRCA operations to conduct the external compliance audit for the infrastructure in accordance with the Government Procurement Act in order to provide fair and impartial audit services. Their qualification must be approved by the NDC and the identity of the auditors are authenticated by the GRCA at the time of the audit.

8.3 Auditor Relationship to Audited Parties

In addition to audited personnel being independent from the audited GRCA, the audit shall be performed by independent and impartial third-party personnel. Their qualifications shall be handled in accordance with section 8.2 Audit Personnel Identity and Qualifications regulations.

8.4 Scope of Audit

(1) Whether or not GRCA operations comply with the CPS.

(2) Whether or not the CPS complies with CP regulations.

8.5 Response to Audit Results

If audit personnel find that the establishment and operation of the GRCA does not conform to the CP, CPS regulations or CCA. The following actions shall be taken:

(1) Record non-conformities.

(2) Notify the GRCA about the non-conformities.

(3) With regard to the non-conformities, the GRCA shall promptly make improvements and notify the original audit personnel to perform a recheck.

(4) The GRCA may choose to suspend operation, revoke the certificates issued to subject CA or other corresponding actions based on the type of non-conformity, severity and time needed to make the corrections.

8.6 Scope of Audit Result Publication

Except for circumstances resulting in system security risk and in accordance with section 9.3 Business Information Confidentiality, the GRCA shall publish the latest CA external audit results in the repository.

9 Other Business and Legal Matters

9.1 Fees

The GRCA reserves the rights to collect fees from CAs that apply for cross-certificates.

9.1.1 Certificate Issuance and Renewal Fees

No fees are currently collected.

9.1.2 Certificate Inquiry Fees

No fees are currently collected.

9.1.3 Certificate Revocation or Status Inquiry Fees

No fees are currently collected.

9.1.4 Other Service Fees

No fees are currently collected.

9.1.5 Refund Request Policy

No fees are currently collected and there is no refund request procedure.

9.2 Financial Responsibility

The GRCA operations are maintained with funding budgeted by the NDC. No insurance policies have taken out with insurance companies.

However, financial and accounting audits are performed by the National Audit Office each year. Other related financial liabilities are handled in accordance with related laws and regulations.

9.2.1Insurance Coverage

Not stipulated.

9.2.2 Other Assets

Not stipulated.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not stipulated.

9.3 Confidentiality of Business Information

9.3.1 Scope of Sensitive Information

The generation, receipt and safekeeping of information by the GRCA shall be deemed to be sensitive information. The scope of sensitive information is as follows:

(1) Private keys and passwords used for GRCA operations.

(2) GRCA key splitting safekeeping information.

(3) Subordinate CA application information that has not been approved by subordinate CA or does not conform to laws and regulations may not be disclosed publicly.

(4) Subject CA application information that has not been approved by subject CA or does not conform to laws and regulations may

not be disclosed publicly.

(5) Audit and tracking logs generated and kept by the GRCA.

(6) Audit logs and discoveries made by audit personnel during the audit process may not be fully disclosed.

(7) Operation-related documents listed as sensitive-level operations.

9.3.2 Information Not within the Scope of Sensitive Information

(1) Issued certificates, revoked certificates and CARLs published on the GRCA repository are not deemed to be sensitive information.

(2) Identification information and information listed on certificates, unless stipulated otherwise, is not deemed to be sensitive information.

9.3.3 Responsibility to Protect Sensitive Information

The GRCA shall handle GRCA, subordinate CA and subject CA application information in accordance with the Electronic Signatures Act, Trust Service Principles and Criteria for Certification Authorities standards, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security and Personal Information Protection Act.

9.4 Privacy of Personal Information

9.4.1 Privacy Protection Plan

The GRCA has posted its privacy rights protection policy on its website. The GRCA conducts privacy impact analysis and personal information risk assessments and also has established a privacy protection plan.

9.4.2 Types of Private Information

Any information listed on a certificate application is deemed private information and may only be disclosed with the consent of the subscriber and in accordance with related laws and regulations. The types of private information that require protection are as follows:

(1) Information not listed on the certificate and CRL.

(2) Subscriber information obtained through the certificate catalog service.

(3) Identifiable personal information to maintain the operation of CA trusted roles such as names together with palm print or fingerprint characteristics.

(4) Personal information in confidentiality agreements and contracts.

The GRCA implements security control measures to prevent personally identifiable information from unauthorized disclosure, leakage and damage.

9.4.3 Types of Information Not Deemed Private

Identification information or information listed on certificates, unless stipulated otherwise, is not deemed to be confidential and private information.

Issued certificates, revoked certificates, suspension information and CRLs published in the repository is deemed to be confidential and private information.

9.4.4 Responsibility to Protect Private Information

The personal information needed for GRCA operation, in either paper or digital form, must be securely stored and protected in accordance with the personal information and privacy rights declaration posted on the website and comply with related regulations in the Electronic Signatures Act, Trust Service Principles and Criteria for Certification Authorities standards, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security and Personal Information Protection Act.

9.4.5 Notice and Consent to Use Private Information

Pursuant to the Personal Information Protection Act, personal information shall not be used for other purposes by the GRCA without the consent of the CA or involved party or unless stipulated otherwise in the personal information protection and privacy rights declaration and CPS.

9.4.6 Disclosure for Judicial or Administrative Proceedings

If there are investigative or evidence collection requirements by

judicial, supervisory or law enforcement authorities which involves providing access to sensitive information, the GRCA shall follow relevant legal procedures. However, the GRCA reserves the right to collect reasonable fees from authorities requesting access to the information.

9.4.7 Other Information Disclosure Circumstances

Subordinate CA and subject CA may search application information. However, the GRCA reserves the right to collect reasonable fees from CAs requesting access to the information.

GRCA handles subordinate CA and subject CA application information in accordance with related laws and regulations of the domestic personal information protection system.

9.5 Intellectual Property Rights

The CPS is the intellectual property of the NDC. Related information can be freely downloaded from the GRCA repository, Copying and distribution may be done in accordance with copyright regulations, but it must be copied in full and the copyright must be listed as belonging to NDC. Fees may not collected from others for the copying and distribution of the CPS. The NDC shall not bear any legal liability for the improper use or distribution of the CPS.

GRCS issued certificates and CARLs are the intellectual property of the GRCA.

The subject names listed on GRCA issued self-signed certificates are the intellectual property of the GRCA.

The GRCA shall do its utmost to ensure the accuracy of subject CA

names. However, this is no indicator of who possesses the intellectual property for the subject CA name. In the event of a dispute over the trademark for the subject CA name, the subject CA shall handle the matter in accordance with legal procedures and submit the results to the GRCA to protect their rights.

9.6 Duties and Responsibilities

9.6.1 GRCA Representations and Warranties

The GRCA shall conduct operations in accordance with CP assurance level 4, follow the procedures set down in CPS regulations when issuing and revoking certificates, publishing CARLs and maintaining the normal operation of the repository. GRCA representations and warranties are as follows:

(1) Conduct operations in accordance with CP assurance level 4 regulations and the CPS.

(2) Establish subordinate CA application and CA cross-certificate application procedures.

(3) Perform identification and authentication for subordinate CA applications and CA cross-certificate applications.

(4) Acceptance of subcontractor CA certificate registration and revocation requests.

(5) Acceptance of subject CA cross-certificate registration and revocation requests.

(6) Issuance and publication of certificates.

(7) Revocation of certificates.

(8) Issuance and publication of CARLs.

(9) Perform CA personnel identification and authentication.

(10) Secure generation of GRCA private keys.

(11) Protection of GRCA private keys.

(12) Perform GRCA self-issued certificate key changeover and issuance of self-issued certificates.

9.6.2 Subordinate CA and Subject CA Representations and Warranties

9.6.2.1 Subordinate CA Representations and Warranties

Subordinate CA representation and warranty obligations are as follows:

(1) Follow CPS regulations and bear liability for damages suffered by relying parties due to failure to follow regulations.

(2) GSCA issued certificates have different usages for different assurance levels in accordance with CP regulations. Subordinate CA must state the assurance level of the requested certificate when the subordinate CA submits the certificate application.

(3) Subordinate CA shall apply for certificates in accordance with section 4.2 Certificate Application Procedure and verify the correctness of the application information.

(4) After the GRCA approves the subordinate CA application and

issues the certificate, the subordinate CA shall follow section 4.4 Certificate Acceptance Procedure.

(5) The subordinate CA accepts the GRCA issued certificate to indicate confirmation of the correctness of the certificate content and uses the certificate in accordance with section 1.4.1 Certificate Usage.

(6) Subordinate CAs self-generate private keys in accordance with Chapter 6 Technical Security Control regulations.

(7) Subordinate CAs shall properly safekeep and use private keys.

(8) The digital signature used with the private key that corresponds with the certificate public key is the subordinate CA digital signature. During generation of the digital signature, the subordinate CA must verify acceptance of the certificate and confirm that the certificate has not been revoked within the validity period.

(9) If a certificate needs to be revoked due to leakage or loss of private key data, the subordinate CA shall immediately notify the GRCA and perform the work in accordance with section 4.9 Certificate Suspension and Revocation regulations. However, the subordinate CA shall bear the legal liability for use of the certificate prior to publication of the certification revocation status.

(10) In the event that normal services cannot be provided by the GRCA, the subordinate CA shall promptly seek out other means to fulfill their obligations to other parties and not use GRCA inability to provide services as a defense to other parties.

9.6.2.2 Subject CA Representations and Warranties

Subject CA representation and warranty obligations are as follows:

(1) Follow CPS and CCA regulations and bear liability for damages suffered by relying parties due to failure to follow regulations.

(2) GSCA issued certificates have different usages for different assurance levels in accordance with CP regulations. CA must state the assurance level of the requested certificate when the CA submits the certificate application.

(3) CA shall apply for certificates in accordance with section 4.2 Certificate Application Procedure regulations and verify the correctness of the application information.

(4) After the GRCA approves the CA cross-certificate application and issues the certificate, the CA shall follow section 4.4 Certificate Acceptance Procedure.

(5) The CA accepts the GRCA issued certificate to indicate confirmation of the correctness of the certificate content and uses the certificate in accordance with section 1.4.1 Certificate Usage regulations.

(6) CAs self-generate private keys in accordance with Chapter 6 Technical Security Controls regulations.

(7) Subject CAs shall properly safekeep and use private keys.

(8) The digital signature used with the private key that corresponds with the certificate public key is the CA digital signature. During generation of the digital signature, the CA must verify acceptance of the certificate and confirm that the certificate has

not been revoked within the validity period.

(9) If a certificate needs to be revoked due to leakage or loss of private key data, the CA shall immediately notify the GRCA and perform the work in accordance with section 4.9 Certificate Suspension and Revocation regulations. However, the CA shall bear the legal liability for use of the certificate prior to publication of the certification revocation status.

(10) In the event that normal services cannot be provided by the GRCA, the CA shall promptly seek out other means to fulfill their obligations to other parties and not use GRCA inability to provide services as a defense to other parties.

9.6.3 RA Representations and Warranties

The GRCA does not establish RA.

9.6.4 Subscriber Representations and Warranties

The GRCA does not issue subscriber certificates.

9.6.5 Relying Parties Representations and Warranties

Relying parties using certificates issued by the GRCA shall bear the following obligations. If there is a violation, relying parties shall bear liable for damages within the scope of accountability:

(1) Relying parties shall follow relevant CPS regulations when using the certificates issued by the GRCA or checking the GRCA repository.

(2) Relying parties shall obtain the GRCA public key or self-signed

certificates through the self-signed certificate secure distribution channels in accordance with section 6.1.4 GRCA Public Key Secure Transmission to Relying Parties regulations.

(3) Relying parties shall first check the certificate assurance level before use of GRCA issued certificates to protect their rights.

(4) Relying parties shall first check the certificate usage restrictions before use of GRCA issued certificates to verify the use of the certificate conforms with the usage restrictions set down by the GRCA.

(5) Relying parties shall first check the CARL before use of GRCA issued certificates to confirm validity of the certificate.

(6) Relying parties shall obtain self-issued certificates from the GRCA repository when using issued certificates after GRCA re-key to establish a certificate trust pathway between the GRCA and the CA.

(7) Relying parties shall first check digital signature to verify if the certificate or CARL is correct when using GRCA issued certificates or CARLs.

(8) Relying parties shall select secure computer environments and reliable application systems. If the rights of relying parties are infringed upon due to the use of computer environments and application systems, the relying parties shall bear sole responsibility.

(9) If the GRCA is unable to operate normally for some reason, the relying parties shall speedily seek other ways for completion of legal acts and the inability of GRCA to operate normally shall

not be used as a defense to others.

(10) Relying party acceptance of a certificate issued by the GRCA indicates understanding and agreement to the GRCA legal liability clauses in accordance with section 1.4.1 Scope of Certificate Usage regulations.

9.6.6 Representations and Warranties of Other Participants

9.6.5.1 Representations and Warranties of Contracted Provision of Certificate Services

By accepting the appointment of the NDC, Chunghwa Telecom shall undertake and guarantee the work related to GRCA establishment and system maintenance and operation.

9.7 Disclaimer of Warranties

The consequences incurred by subordinate CA, subject CA and relying parties due to the failure to follow section 1.4.1 Scope of Certificate Usage regulations during certificate use shall be borne solely by the subscriber or relying party. The GRCA shall not bear any legal liability.

9.8 Limitations of Liability

If some certificate services must be suspended due to GRCA maintenance, conversion or expansion requirements, advance notification shall be posted in the repository and the subordinate CAs and subject CAs shall be notified. Subscribers and relying parties may not use service suspension as a reason to claim compensation from the GRCA.

The GRCA shall also issue and administer certificates in accordance with the regulations in formal version of the CA/Browser Form Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

If the subordinate CA, subject CA or the competent authority submits a certificate revocation request for the certificate revocation reasons provided in section 4.9 Certificate Suspension and Revocation regulations, the GRCA shall complete certificate revocation work and publish the CARL in the repository within 10 working days at the latest. Before the certificate revocation status is published, the CA shall take appropriate action to reduce the effect of relying parties and bear responsibility arising from use of the certificates.

9.9 Indemnities

9.9.1 GRCA Compensation Liability

If a CA, certificate subscriber or relying party claim compensation for damages suffered due to the intentional or unintentional failure of the GRCA to follow the CPS, relevant laws and regulations and contract provisions when performing certificate-related work, the GRCA shall be liable for compensation. Damage compensation liability of the GRCA is limited to the scope of liability set down in the CPS and related contracts.

9.9.2 Subordinate CA and Subject CA Compensation Liability

The GRCA must request that subordinate CA and subject CA bear compensation liability when direct damages are incurred under the following circumstances under relevant law and regulations:

(1) False or fraudulent descriptions are submitted when a subordinate CA or subject CA applies for a certificate which causes the GRCA to issue an incorrect CA certificate of cross-certificate.

(2) Failure by the subordinate CA or subject CA to properly safekeep the private key results in the compromise, disclosure, modification or unauthorized use of the private key.

(3) Violation of law, CP, CPS (such as failure to issue certificate with an appropriate assurance level in accordance with CPS regulations) or CCA regulations by the subordinate CA or 交 subject CA.

(4) If there is a violation by subordinate CA or subject CA of agreements signed with system, browser or software platform root certificate program participated in by the GRCA which affects the inclusion of the GRCA by the above application software suppliers or application for inclusion into CA trust lists, the GRCA may request the subordinate CA or bear compensation liability in accordance with the provisions of the CCA.

9.9.3 Relying Party Compensation Liability

Relying party compensation liability is determined based on relevant laws and regulations.

9.10 Term and Termination

9.10.1 Term

The CPS and any attachments take effect when published on the

GRCA website and repository following approval by the Electronic Signatures Act competent authority and remain in effect until replaced with a newer version.

9.10.2 Termination

The CPS and any attachments remain in effect until replaced by newer version that is approved and announced by the Electronic Signatures Act and the old version is terminated.

9.10.3 Effect of Termination and Survival

The conditions and effect of the CPS termination shall be communicated via the GRCA website and repository. In addition to stating which parties that are retained after CPS termination, preserving related responsibilities for the protection of confidential information following CPS termination shall be emphasized. It shall remain valid until the last issued certificate expires.

9.11 Individual Notices and Communication with Participants

The GRCA, subordinate CA, subject CA and relying parties shall take appropriate actions to establish notification and communication channels including but not limited to: official documents, letter, telephone, fax and e-mail.

9.12 Amendments

A regular annual review and assessment of the GPS is conducted by the GRCA. Amendments are made by amending the attached documents

or directly revising the content of the CPS.

The GRCA also performs a regular annual review of the guidelines in the official version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum (http://www.cabforum.org) to assess whether or not if the CPS needs to be amended. If the SSL certificate issuance management guidelines stated in CPS conflict with forum guidelines, the guidelines issued by the CA/Browser Forum shall prevail and the CPS shall be modified accordingly. The amended version shall be implemented following approval by the Electronic Signatures Act competent authority.

9.12.1 Procedure for Amendment

Amendments to the CPS are announced after passing Government Electronic Certificate Steering Committee review and approval is given by Electronic Signatures Act competent authority (MOEA).

9.12.2 Notification Mechanism and Period

9.12.2.1 Notification Mechanism

All modified items are posted in the GRCA repository. No additional notification is made to the subordinate CA and subject CA for non-material changes.

9.12.2.2 Modified Items

The draft version is published in the repository after passing Government Electronic Certificate Steering Committee review depending on what level of impact the modifications have on subordinate CA,

subject CA or relying parties. The notification period is as follows:

(1) Significant impact: Post 15 calendar days in the GRCA repository before submission to the Electronic Signatures Act competent authority (MOEA) for review.

(2) Less significant impact: Post 7 calendar days in the GRCA repository before submission to the Electronic Signatures Act competent authority (MOEA) for review.

No addition review and notification are performed for new layouts to the CPS.

9.12.2.3 Comment Reply Period

The reply period for comments on modified items is:

(1) Significant impact: The reply period is within 15 calendar days of the posting date.

(2) Less significant impact: The reply period is within 7 days of the posting date.

9.12.2.4 Comment Handling Mechanism

For comments on modified items, the reply method is posted in the repository and transferred to the GRCA before the end of the comment reply period. After the related comments are collected by the GRCA., assessment of the modified items is performed.

9.12.2.5 Final Notification Period

CPS amendments must be announced within 10 calendar days following approval by the Electronic Signatures Act competent authority.

9.12.3 Circumstances under which the OID Must Be Changed

If the CP is amended or the OID is changed, the CPS shall also be amended accordingly. The amendment method includes amendment of attached documents or direct revisions to the content of the CPS.

9.13 Dispute Resolution Procedure

In the event of a dispute between a CA and the GRCA, the parties shall first reach a consensus through negotiation. An interpretation of related provisions is provided by the GRCA. If litigation is necessary, the parties agree that the Taiwan Taipei District Court shall be the court of first instance.

9.14 Governing Law

For disputes involving GRCA issued certificates, related ROC laws and regulations shall govern.

9.15 Applicable Law

Related laws and regulations must be followed with regard to the interpretation and legality of agreements signed by the GRCA to meet cross-certificate requirements.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS constitutes the final and entire agreement between the key participants (GRCA, subordinate CA, subject CA and relying parties) and

supersedes all prior oral or written understandings relating to the same subject matter and this CPS represents the final agreement.

9.16.2 Assignment

Rights and obligations of the key participants described in the CPS may not be assigned in any forms to other parties without notifying the GRCA.

9.16.3 Severability

If any chapter of the CPS is found to be inaccurate or invalid, the remaining chapters of the CPS shall remain valid.

The GRCA follows the guidelines in the official version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum for the issuance and administration of GRCA certifications. However, if related guidelines are in conflict with national law or regulations, the GRCA may make minor adjustments to related methods to satisfy legal or regulatory requirements and notify the CA/Browser Forum about the modified sections before issuing new certificates. In the event of the following circumstances, the deleted or modified content of the original CPS shall pass Government Electronic Certificate Steering Committee review and receive approval from the Electronic Signatures Act competent authority (MOEA). The above work must be completed within 90 days.

(1) The related guidelines in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum that are in conflict with national laws and regulations have been modified or deleted.

(2) The CA/Browser Forum has modified relevant content in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates to make the guidelines compatible with national laws and regulations.

9.16.4 Enforcement

In the event that the GRCA suffers damages attributable to an intentional or unintentional violation or related CPS regulations by a subordinate CA, subject CA and relying parties, the GRCA may, besides seeking compensation for damages, request the responsible party to pay the attorney fees arising from handling this dispute or litigation.

The GRCA's failure to assert rights regarding the violation of CPS regulations does not waive the GRCA's right to pursue the violation of CPS regulations subsequently or in the future.

9.16.5 Force Majeure

In the event that damages are incurred due to a force majeure or other reasons not attributable to the GRCA, the GRCA shall not bear any legal liability.

9.17 Other Provisions

Not stipulated.

Appendix 1: Glossary

◆ A

- **Activation Data**: The private data required besides keys to access the cryptographic module (such as data used to activate the private key for signatures or encryption).

- **American Institute of Certified Public Accountants, (AICPA)**：Institution which jointly drafted The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy system standards with the Chartered Professional Accountants Canada for the WebTrust for CA and the SSL Baseline Requirement & Network Security mark.

- **Applicant**: A subscriber who requests certificates from a CA and has not yet completed the certificate procedure.

- **Archive**: A physically separate storage site for long-term information (storage site for important information) which can be used to support audit, usage and integrity services.

- **Assurance:** A reliable basis to determine that an entity conforms to certain security requirements.

- **Assurance Level**: A certain level possessing a relative assurance level.

- **Audit:** Assessment of whether system controls are adequate and ensure conforms with existing policy and operation procedures,

and independent checking and review of recommended required improvements to existing controls, policies and procedures.

- **Audit Log:** Activity logs of a system organized in the order of time of occurrence that can be used to reconstruct or investigate the time sequence or changes that occurred during a certain event.

- **Authenticate:** Authentication is the process by which a claimed identity is determined to be legitimate and belonging to the claimant.

- **Authentication**
  - The process of establishing a level of trust in the identity of users or information systems.
  - Security measures used for information transmission, messages, and ways to authorize individuals to receive certain types of information.

◆ **C**

- **Certificate**
  - Refers to verification information carrying a digital signature used to verify the identity and qualifications of the signer in electronic form.
  - Digital presentation of information. The contents include:
    - ✓ Issuing certificate authority.
    - ✓ Subscriber name or identity.
    - ✓ Subscriber public key.
    - ✓ Certificate validity period.

- ✓ Certificate authority digital signature.

- **Certificate Policy (CP)**： Refers to the dedicated profile administration policy established for the electronic transactions performed through the certificate administration. Certificate policy covers a variety of issues including the formation, generation, delivery, auditing, auditing, restoration after compromise and administration. The security services required for a certain application are provided through certificate policy and other related technology.

- **Certificate Revocation List (CRL)**
  - The revoked certificate list digitally signed by the certificate authority provided for relying party use.
  - List maintained by the certificate authority. The expiry dates of the above revoked certificates issued by the certificate authority are recorded by the list.

- **Certification Authority (CA)**
  - The agency that issues certificates.
  - The competent body trusted by the subscriber. Its functions are the issuance and administration of X.509 format public key certificates, CARLs and CRLs.

- **Certification Authority Authorization (CAA)**: According to RFC 6844 rules, the Certification Authority DNS Resource Record permits domain name owner in the DNS to designate one or more CAs to obtain authorization to help that domain with certification issuance. Posting of the CAA resource record allows publicly trusted CA to implement extra controls to reduce

unforeseen certificate mis-issuance risk.

- **Certification Authority Revocation List (CARL)**: A signed and timestamped list. The list contains the serial numbers of revoked CA public key certificates (including subordinate CA certificates and cross-certificates).

- **Certificate Modification:** Refers to providing a new certificate to replace the original certificate to the same certificate subject. However, the expiry date of the new certificate must be the same as that on the old certificate. The old certificate is revoked after certificate modification.

- **Certification Practice Statement (CPS)**
  - External notification by the external notification used to describe the practice statement of the certificate authority governing certificate issuance and processing of other certification work.
  - Announcement of a statement that certain procedures of the certificate authority for certificate work (including issuance, suspension, revocation, extension and access) comply with certain requirements (requirements described in certificate policy or other service contracts).

- **Chartered Professional Accountants Canada (CPA)**: Administration institution which jointly drafted the Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy system standard with the American Institute of Certified Public Accountants (AICPA) and the management organization for WebTrust for CA

and SSL Baseline Requirement & Network Security mark The Canadian Institute of Chartered Accountants is abbreviated as CICA.

- **Compromise**: Information disclosed to unauthorized persons or unauthorized intentional and unintentional disclosure, modification, destruction or loss of objects which constitutes a violated of information security policy.

- **Cross-Certificate:** A certificate used to establish a trust relationship between two root CA. This certificate is a type of CA certificate and not a subscriber certificate.

- **Cross-Certification:** The actions or procedures by which a public key certificate is issued by a CA in the public key infrastructure to another CA in the public key infrastructure.

- **Cross Certification Agreement (CCA)**: The items and individual responsibility and obligation assignment agreement which must be followed by the GRCA and the subordinate CA when the subordinate CA applies to join the GPKI.

- **Cryptographic Module**: A set of hardware, software, firmware or a combination of the above used to run cryptologic or programs (including crypto algorithms) and included within the cryptographic boundaries of the module.

◆ **D**

- **Digital Signature:** A digital signature is formed by digital information of a certain size calculated by mathematical

algorithm or other method that is encrypted with a signer's private key and verified with a public key.

- **Duration**: A certificate field made up of two subfields "start time of the validity period" and "end time of the validity period".

◆ **E**

- **End Entity (EE)**: The GPKI includes the following two types of entities:
  - Those responsible for the safekeeping and use of certificate private keys.
  - Third parties who trust the certificates issued by the GPKI CA (not holders of private keys and not a certificate authority). The end entities are subscribers and relying parties including personnel, organizations, accounts, devices and sites.

◆ **F**

- **Federal Information Processing Standard (FIPS)**: Except for military organizations in the US federal government system, the information processing standard for all government organizations and government subcontractors. The security requirement standard for the cryptographic module is FIPS no. 140 standard (FIPS 140). FIPS 140-2 divides the cryptographic module into 11 types of security requirements. Each security requirement type is then divided into 4 security levels.

◆ **G**

- **Government Root Certification Authority:** GPKI root

certification authority is the highest-level CA in the hierarchical structure of the GPKI. Its public keys serve as a trust anchor.

◆ **I**

- **Identity Assurance Level:** A certain level in corresponding assurance hierarchy used for identification.

- **Internet Engineering Task Force (IETF):** Responsible for the development and promotion of Internet standards. Its vision is the generation of high quality technical documents affects how persons design, use and manage the Internet and allows the Internet to operate smoothly. (official website: https://www.ietf.org)

- **Issuing CA:** For a particular certificate, the CA that issues the certificate is called the issuing CA.

◆ **K**

- **Key Escrow**: Storage of related information using the subscriber's private key and according to the terms of the escrow agreement (or similar contract). The terms of this escrow agreement require that one or more agencies are in possession of the subscriber key provided it is beneficial to the subscriber, employer or another party in accordance with the provisions of the agreement.

- **Key Pair:** Two mathematically linked keys possessing the following attributes:
  - One of the keys is used for encryption. This encrypted data

may only be decrypted by the other key.

- It is impossible to differentiate one key from another (from a mathematical calculation standpoint).

◆ M

- **Mutual Authentication**: Two parties authenticating one another during communication activities.

◆ O

- **Object Identifier (OID)**
  - One type of unique alphanumeric / numeric identified registered under the International Standard Organization registration standard which could be used to identify the uniquely corresponding certificate policy.
  - When a special form of code, object or object type is registered with the International Organization for Standardization (ISO), the unique code can be used as an identifier. For example, this code can be used in the public key infrastructure to indicate which certificate policy and cryptographic algorithms are used.

- **Online Certificate Status Protocol (OCSP)**: The Online Certificate Status Protocol is a type of online certificate checking protocol which allows the application software of relying parties to determine the status (such as revoked or valid) or a certain certificate.

- **Organization Validation (OV)**: In the SSL certificate approval

process, except for identification and authentication of subscriber domain name control rights, following the certificate assurance level to identify and authenticate the identity of subscriber organizations and individuals. Therefore, a connection to a website established by an Organization Validation SSL certificate is able to provide TLS encryption channels, in order to determine who the owner of the website is and ensure the integrity of the transferred information.

◆ P

- **Private Key:** The following keys must be kept secret under these two circumstances:
  - It is a key in the signature key pairs used to generate digital signatures.
  - It is a key in the encryption key pair used to decrypt sensitive information.

- **Public Key:** The following keys must be made public (usually in digital certificate form) under these two circumstances:
  - It is a key in the signature key pair used to verify the validity of the digital signature.
  - It is a key in the encryption key pair used for encrypting sensitive information.

- **Public Key Infrastructure (PKI):** A combination of laws, policies, standards, personnel, equipment, technology, processes, audits and services developed on a broad scale and management of asymmetric cryptography and public key certificates.

◆ **R**

- **Registration Authority (RA)**
  - Responsible for checking the identity and other attributes of the certificate applicant but does not issue or administer certificates. The nature and scope of obligations borne by the registration authority are set down in the applicable certificate policy or agreement.
  - The entity responsible for the identity identification and authentication of the certificate subject which does not issue certificates.

- **Re-key (a Certificate)**: Rekeying a certificate refers to the issuance of a new certificate that has the same attributes and assurance level as the old certificate. In addition to being a brand new certificate with a different public key (corresponding to the new and different private key) and different serial number, the new certificate may also be given a different validity period.

- **Relying Party**
  - Recipient of a certificate who relies on that certificate or a digital signature to verify the public key listed on the certificate or the counterpart to identify (or its attributes) of the subject named in a trusted certificate and public key listed in the certificate.
  - The individual or agency which receives information including a certificate and digital signature (the public key listed on the certificate may be used to verify the digital signature) and may rely on this information.

- **Renew a Certificate:** Refers to the issuance of a new certificate that has the same subject name, key and related information as the old certificate to extend the validity period of the certificate and provide a new serial number.

- **Repository**
  - A trustworthy system used to store and retrieve certificates and other information relevant to certification.
  - The database containing the certificate policy and certificate-related information.

- **Revoke a Certificate:** Termination of a certificate operations during its validity period.

- **Root Certification Authority (Root CA):** The highest-level CA in the GPKI. In addition to issuing subordinate CA certificates and self-signed certificates, application software providers are responsible for the distribution of its self-signed certificates. Can be called certificate root CA or top-level CA.

◆ **S**

- **Self-Issued Certificate:** Self-issued certificates are certificates issued during root CA re-key or due to CP requirements that are mutually issued with the private key used by two generations of root CAs used to establish a trust pathway between old and new keys or CP interoperable certificates.

- **Self-Signed Certificate:** Self-signed certificates are a type of certificate whose certificate issuer name is the same as the

certificate subject name. Even if the private key from the same key pair is used to issue certificates with its corresponding public key and other information, a self-signed certificate inside the PKI can serve as a trust anchors for certificate path. Its issuance counterpart is the GRCA itself, Self-signed certificates contain the GRCA public key and the certificate issuer name and certificate subject name are the same. They are provided to relying parties for GRCA issued self-issued certificate, subordinate CA certificate and CARL digital signature use. 。

- **Subject Certification Authority:** For a CA certificate, the certificate authority referred to in the certificate subject of the certificate is the subject CA for that certificate.

- **Subordinate Certification Authority:** In the public key infrastructure hierarchy, certificates that are issued by another certificate authority and the activities of the certificate authority are restricted to this other certificate authority.

- **Subscriber**
  - Refers to a subject named or identified in the certificate that holds the private key that corresponds with the private key listed in the certificate.
  - An entity possessing the following attributes including (but not limited to) individuals, organizations and network devices:
    - ✓ Subject listed on an issued certificate.
    - ✓ A private key that corresponds to the public key listed on the certificate.
    - ✓ Other parties that do not issue certificates.

◆ **T**

- **Trust Anchor**: The original certificate in the trust pathway which relying parties depend upon and which are obtained through secure and reliable transmission methods. Also called trust point.

- **Trustworthy System:** Computer hardware, software or programs which possess the following attributes:
  - Functions that protect against intrusion and misuse.
  - Provides reasonably accessible, reliable and accurate operations.
  - Appropriate implementation of preset functions.
  - Security procedures uniformly accepted by the general public.

◆ **Z**

- **Zeroize:** Method to delete electronically stored information. Storage of modified information to prevent recovery of information.

Appendix 2: English Acronyms

Acronym	Full Name
CA	Certification Authority
CARL	Certificate Authority Revocation List
CCA	Cross Certification Agreement
CARL	Certification Authority Revocation List
CP	Certificate Policy
CP OID	CP Object Identifier
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
EE	End Entities
FIPS	(US Government) Federal Information Processing Standard
IETF	Internet Engineering Task Force
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
UPS	Uninterrupted Power System

Appendix 3: BRs-Section 1.2.1 Revisions

Ver.	Ballot	Description	Adopted	Effective*	Implementation
1.0.0	62	Version 1.0 of the Baseline Requirements Adopted	22-Nov-11	01-Jul-12	-
1.0.1	71	Revised Auditor Qualifications	08-May-12	01-Jan-13	Compliant
1.0.2	75	Non-critical Name Constraints allowed as exception to RFC 5280	08-Jun-12	08-Jun-12	Compliant
1.0.3	78	Revised Domain/IP Address Validation, High Risk Requests, and Data Sources	22-Jun-12	22-Jun-12	Compliant
1.0.4	80	OCSP responses for non-issued certificates	02-Aug-12	01-Feb-13 01-Aug-13	Completed
--	83	Network and Certificate System Security Requirements adopted	03-Aug-13	01-Jan-13	Compliant
1.0.5	88	User-assigned country code of XX allowed	12-Sep-12	12-Sep-12	Compliant
1.1.0	--	Published as Version 1.1 with no changes from 1.0.5	14-Sep-12	14-Sep-12	-
1.1.1	93	Reasons for Revocation and Public Key Parameter checking	07-Nov-12	07-Nov-12	Compliant
1.1.2	96	Wildcard certificates and new gTLDs	20-Feb-13	20-Feb-13 01-Sep-13	Compliant
1.1.3	97	Prevention of Unknown Certificate Contents	21-Feb-13	21-Feb-13	Compliant
1.1.4	99	Add DSA Keys (BR v.1.1.4)	3-May-2013	3-May-2013	Compliant
1.1.5	102	Revision to subject domainComponent language in section 9.2.3	31-May-2013	31-May-2013	Compliant
1.1.6	105	Technical Constraints for Subordinate Certificate Authorities	29-July-2013	29-July-2013	Compliant
1.1.7	112	Replace Definition of “Internal Server Name” with “Internal Name”	3-April-2014	3-April-2014	Compliant
1.1.8	120	Affiliate Authority to Verify Domain	5-June-2014	5-June-2014	Compliant
1.1.9	129	Clarification of PSL mentioned in Section 11.1.3	4-Aug-2014	4-Aug-2014	Compliant
1.2.0	125	CAA Records	14-Oct-2014	15-Apr-2015	Compliant
1.2.1	118	SHA-1 Sunset	16-Oct-2014	16-Jan-2015 1-Jan-2016	Compliant

				1-Jan-2017	
1.2.2	134	Application of RFC 5280 to Pre-certificates	16-Oct-2014	16-Oct-2014	Compliant
1.2.3	135	ETSI Auditor Qualifications	16-Oct-2014	16-Oct-2014	-
1.2.4	144	Validation Rules for .onion Names	18-Feb-2015	18-Feb-2015	Compliant
1.2.5	148	Issuer Field Correction	2-April-2015	2-April-2015	Compliant
1.3.0	146	Convert Baseline Requirements to RFC 3647 Framework	16-Apr-2015	16-Apr-2015	-
1.3.1	151	Addition of Optional OIDs for Indicating Level of Validation	28-Sep-2015	28-Sep-2015	Compliant
1.3.2	156	Amend Sections 1 and 2 of Baseline Requirements	3-Dec-2015	3-Dec-2016	Compliant
1.3.3	160	Amend Section 4 of Baseline Requirements	4-Feb-2016	4-Feb-2016	Compliant
1.3.4	162	Sunset of Exceptions	15-Mar-2016	15-Mar-2016	Compliant
1.3.5	168	Baseline Requirements Corrections (Revised)	10-May-2016	10-May-2016	Compliant
1.3.6	171	Updating ETSI Standards in CABF documents	1-July-2016	1-July-2016	-
1.3.7	164	Certificate Serial Number Entropy	8-July-2016	30-Sep-2016	Compliant
1.3.8	169	Revised Validation Requirements	5-Aug-2016	1-Mar-2017	Compliant
1.3.9	174	Reform of Requirements Relating to Conflicts with Local Law	29-Aug-2016	27-Nov-2016	Compliant
1.4.0	173	Removal of requirement to cease use of public key due to incorrect info	28-July-2016	11-Sep-2016	Compliant
1.4.1	175	Addition of givenName and surname	7-Sept-2016	7-Sept-2016	Compliant
1.4.2	181	Removal of some validation methods listed in section 3.2.2.4	7-Jan-2017	7-Jan-2017	Compliant
1.4.3	187	Make CAA Checking Mandatory	8-Mar-2017	8-Sep-2017	Compliant
1.4.4	193	825-day Certificate Lifetimes	17-Mar-2017	1-Mar-2018	Compliant
1.4.5	189	Amend Section 6.1.7 of Baseline Requirements	14-Apr-2017	14-May-2017	Compliant
1.4.6	195	CAA Fixup	17-Apr-2017	18-May-2017	Compliant
1.4.7	196	Define “Audit Period”	17-Apr-2017	18-May-2017	-
1.4.8	199	Require commonName	9-May-201	8-June-2017	Compliant

		in Root and Intermediate Certificates 9	7		
1.4.9	204	Forbid DTPs from doing Domain/IP Ownership	11-July-2017	11-Aug-2017	Compliant
1.5.0	212	Canonicalise formal name of the Baseline Requirements	1-Sept-2017	1-Oct-2017	Compliant
1.5.1	197	Effective Date of Ballot 193 Provisions	1-May-2017	2-June-2017	Compliant
1.5.2	190	Add Validation Methods with Minor Corrections	19-Sept-2017	19-Oct-2017	Compliant
1.5.3	214	CAA Discovery CNAME Errata	27-Sept-2017	27-Oct-2017	Compliant
1.5.4	215	Fix Ballot 190 Errata	4-Oct-2017	5-Nov-2017	Compliant
1.5.5	217	Sunset RFC 2527	21-Dec-2017	20-Jan-2018	Compliant
1.5.6	218	Remove validation methods #1 and #5	5-Feb-2018	9-Mar-2018	Compliant
1.5.7	220	Minor Cleanups (Spring 2018)	30-Mar-2018	29-Apr-2018	Compliant
1.5.8	219	Clarify handling of CAA Record Sets with no "issue"/"issuewild" property tag	10-Apr-2018	10-May-2018	Compliant
1.5.9	223	Update BR Section 8.4 for CA audit criteria	15-May-2018	14-June-2018	Compliant
1.6.0	224	WhoIs and RDAP	22-May-2018	22-June-2018	Compliant
1.6.1	SC6	Revocation Timeline Extension	14-Sep-2018	14-Oct-2018	Compliant
1.6.2	SC12	Sunset of Underscores in dNSNames	9-Nov-2018	10-Dec-2018	Compliant
1.6.3	SC13	CAA Contact Property and Associated E-mail Validation Methods	25-Dec-2018	1-Feb-2019	Compliant
1.6.4	SC14	Updated Phone Validation Methods	31-Jan-20	31-Jan-20	Compliant
	SC15	Remove Validation Method Number 9	5-Feb-2019		
	SC7	Update IP Address Validation Methods	8-Feb-2019		
1.6.5	SC16	Other Subject Attributes	15-Mar-2019	16-April-2019	Compliant

* Effective Date and Additionally Relevant Compliance Date(s)