

**Government Root Certification Authority
Certification Practice Statement
Version 1.0**

Administrative Organization
**The Research, Development and Evaluation
Commission (RDEC) of Executive Yuan**

Executive Organization
ChungHwa Telecom Co., Ltd.

March 2004

| | | |
|---------|--|----|
| 1 | Introduction | 8 |
| 1.1 | Overview | 8 |
| 1.2 | Identification | 9 |
| 1.3 | Communicability and Applicability | 9 |
| 1.3.1 | Government Root Certification Authority (GRCA) | 9 |
| 1.3.2 | Repository | 10 |
| 1.3.3 | Subject Certification Authority | 10 |
| 1.3.4 | Relying Parties | 10 |
| 1.3.5 | Certification Service by Outsourcing | 11 |
| 1.3.6 | Applicability | 11 |
| 1.3.6.1 | Usage of Issued Certificates | 11 |
| 1.3.6.2 | Notifications of Using Certificate | 11 |
| 1.3.6.3 | Prohibits of Using Certificate | 12 |
| 1.4 | Contact Details | 13 |
| 1.4.1 | Specification Administration Organization | 13 |
| 1.4.2 | Contact Person | 13 |
| 1.4.3 | Person Determining Certification Practice Statement Suitability for the Policy | 13 |
| 2 | General Provisions | 15 |
| 2.1 | Obligations | 15 |
| 2.1.1 | GRCA Obligations | 15 |
| 2.1.2 | Subject CA Obligations | 15 |
| 2.1.3 | Relying Party Obligations | 17 |
| 2.1.4 | Repository Obligations | 18 |
| 2.2 | Liability | 18 |
| 2.2.1 | GRCA Liability | 18 |
| 2.2.1.1 | Warranties and Limitations on Warranties | 18 |
| 2.2.1.2 | Disclaimer of Warranties | 18 |
| 2.2.1.3 | Limitations of Liability | 18 |
| 2.2.1.4 | Other Exclusions | 19 |
| 2.3 | Financial Responsibility | 19 |
| 2.3.1 | Indemnification by Subject CAs and Relying Parties | 20 |
| 2.3.2 | Administrative Processes | 20 |
| 2.4 | Interpretation and Enforcement | 20 |
| 2.4.1 | Governing Law | 20 |
| 2.4.2 | Severability of Provisions, Survival, Merger, and Notice | 20 |
| 2.4.3 | Dispute Resolution Procedures | 20 |

| | | |
|-------|--|----|
| 2.5 | Fees | 21 |
| 2.5.1 | Certificate Issuance or Renewal Fees..... | 21 |
| 2.5.2 | Certificate Access Fees..... | 21 |
| 2.5.3 | Revocation or Status Information Access Fees | 21 |
| 2.5.4 | Fees for Other Services such as Policy Information | 21 |
| 2.5.5 | Refund Policy | 21 |
| 2.6 | Publication and Repository | 21 |
| 2.6.1 | Publication of CA Information..... | 21 |
| 2.6.2 | Frequency of Publication | 22 |
| 2.6.3 | Access Controls..... | 22 |
| 2.6.4 | Repositories | 23 |
| 2.7 | Compliance Audit..... | 23 |
| 2.7.1 | Frequency of Compliance Audit | 23 |
| 2.7.2 | Identity/Qualifications of Compliance Auditor..... | 23 |
| 2.7.3 | Compliance Auditor’s Relationship to Audited Party..... | 23 |
| 2.7.4 | Topics Covered by Compliance Audit | 24 |
| 2.7.5 | Actions Taken as a Result of Deficiency..... | 24 |
| 2.7.6 | Communication of Result | 24 |
| 2.8 | Confidentiality..... | 25 |
| 2.8.1 | Types of Information to be Kept Confidential | 25 |
| 2.8.2 | Types of Information not Considered Confidential..... | 25 |
| 2.8.3 | Disclosure of Certificate Revocation/Suspension Information..... | 25 |
| 2.8.4 | Release to Law Enforcement Officials..... | 26 |
| 2.8.5 | Release as Part of Civil Discovery | 26 |
| 2.8.6 | Disclosure Ipon Owner's Request | 26 |
| 2.8.7 | Other Information Release Circumstances..... | 26 |
| 2.8.8 | Privacy Protection | 27 |
| 2.9 | Intellectual Property Rights..... | 27 |
| 3 | Identification and Authentication | 29 |
| 3.1 | Initial Registration..... | 29 |
| 3.1.1 | Types of Names | 29 |
| 3.1.2 | Need for Names to be Meaningful | 29 |
| 3.1.3 | Rules for Interpreting Various Name Forms | 29 |
| 3.1.4 | Uniqueness of Names..... | 29 |
| 3.1.5 | Name Claim Dispute Resolution Procedure | 30 |
| 3.1.6 | Recognition, Authentication, and Role of Trademarks | 30 |
| 3.1.7 | Method to Prove Possession of Private Key | 30 |
| 3.1.8 | Authentication of Organization Identity | 30 |

GRCA CPS

| | | |
|--------|--|----|
| 3.1.9 | Authentication of Individual Identity | 31 |
| 3.1.10 | Authentication of Hardware Device or Server Software | 31 |
| 3.2 | Routine Rekey and Certificate Renewal | 31 |
| 3.2.1 | Routine Rekey of Certificates | 31 |
| 3.2.2 | Certificate Renewal | 32 |
| 3.3 | Rekey after Revocation | 32 |
| 3.4 | Revocation Request | 32 |
| 4 | Operations Requirement | 33 |
| 4.1 | Certificate Application | 33 |
| 4.2 | Certificate Issuance | 34 |
| 4.3 | Certificate Acceptance | 34 |
| 4.4 | Certificate Suspension and Revocation | 35 |
| 4.4.1 | Circumstances under which a Certificate may be Revoked | 35 |
| 4.4.2 | Who can Request Revocation of a Certificate Issued by GRCA | 36 |
| 4.4.3 | Procedure for Revocation Request | 36 |
| 4.5 | Security Audit Procedures | 38 |
| 4.5.1 | Types of Events Recorded | 38 |
| 4.5.2 | Frequency of Processing Data | 41 |
| 4.5.3 | Retention Period for Security Audit Data | 42 |
| 4.5.4 | Protection of Security Audit Data | 42 |
| 4.5.5 | Security Audit Data Backup Procedures | 42 |
| 4.5.6 | Security Audit Collection System (Internal vs. External) | 42 |
| 4.5.7 | Notification to Event-Causing Subject | 43 |
| 4.5.8 | Vulnerability Assessments | 43 |
| 4.6 | Records Archival | 43 |
| 4.6.1 | Types of Events Archived | 43 |
| 4.6.2 | Retention Period for Archive | 44 |
| 4.6.3 | Protection of Archive | 44 |
| 4.7 | Key Changeover | 45 |
| 4.8 | Compromise and Disaster Recovery | 45 |
| 4.9 | CA Termination | 46 |
| 5 | Non-Technical Controls | 47 |
| 5.1 | Physical Controls | 47 |
| 5.1.1 | Site Location and Construction | 47 |
| 5.1.2 | Physical Access | 47 |
| 5.1.3 | Electrical Power and Air Conditioning | 48 |
| 5.1.4 | Flood Prevention and Protection | 48 |
| 5.1.5 | Fire Prevention and Protection | 48 |

| | | |
|-------|--|----|
| 5.1.6 | Media Storage | 48 |
| 5.1.7 | Waste Disposal | 49 |
| 5.1.8 | Off-site Backup | 49 |
| 5.2 | Procedural Controls..... | 49 |
| 5.2.1 | Trusted Roles..... | 49 |
| 5.2.2 | Roles Assignments | 50 |
| 5.2.3 | Number of Persons Required Per Task..... | 50 |
| 5.2.4 | Identification and Authentication for Each Role..... | 51 |
| 5.3 | Personnel Controls | 52 |
| 5.3.1 | Background, Qualifications, Experience, and Security Clearance Requirements..... | 52 |
| 5.3.2 | Background Check Procedures | 52 |
| 5.3.3 | Training Requirements | 53 |
| 5.3.4 | Retraining Frequency and Requirements | 53 |
| 5.3.5 | Job Rotation Frequency and Sequence..... | 53 |
| 5.3.6 | Sanctions for Unauthorized Actions..... | 54 |
| 5.3.7 | Contracting Personnel Requirements | 54 |
| 5.3.8 | Documentation Supplied to Personnel | 54 |
| 6 | Technical Security Controls | 55 |
| 6.1 | Key Pair Generation and Installation | 55 |
| 6.1.1 | Key Pair Generation | 55 |
| 6.1.2 | Private Key Delivery to Cross-certified CAs..... | 55 |
| 6.1.3 | Public Key Delivery to GRCA..... | 55 |
| 6.1.4 | GRCA Public Key Delivery to Relying Parties | 55 |
| 6.1.5 | Key Sizes..... | 56 |
| 6.1.6 | Public Key Parameters Generation | 56 |
| 6.1.7 | Parameter Quality Checking | 57 |
| 6.1.8 | Hardware/Software Key Generation | 57 |
| 6.1.9 | Key Usage Purposes (as per X.509 v3 key usage field)..... | 57 |
| 6.2 | Private Key Protection | 57 |
| 6.2.1 | Standards for Cryptographic Module | 57 |
| 6.2.2 | Private Key (n out of m) Multi-person Control..... | 58 |
| 6.2.3 | Private Key Escrow | 58 |
| 6.2.4 | Private Key Backup..... | 58 |
| 6.2.5 | Private Key Archival | 59 |
| 6.2.6 | Private Key Entry into Cryptographic Module | 59 |
| 6.2.7 | Method of Activating Private Key | 59 |
| 6.2.8 | Method of Deactivating Private Key..... | 59 |

| | | |
|---------|--|----|
| 6.2.9 | Method of Destroying Private Key | 60 |
| 6.3 | Other Aspects of Key Pair Management for Cross-certified CAs | 60 |
| 6.3.1 | Public Key Archival | 60 |
| 6.3.2 | Usage Periods for the Public and Private Keys..... | 60 |
| 6.3.2.1 | Usage Periods for GRCA Public Key and Private Key..... | 60 |
| 6.3.2.2 | Usage Periods for Cross-certified CA's Public Key and Private Key | 61 |
| 6.4 | Activation Data | 61 |
| 6.4.1 | Activation Data Generation and Installation..... | 61 |
| 6.4.2 | Activation Data Protection | 61 |
| 6.4.3 | Other Aspects of Activation Data..... | 62 |
| 6.5 | Computer Security Controls..... | 62 |
| 6.5.1 | Specific Computer Security Technical Requirements..... | 62 |
| 6.5.2 | Computer Security Rating..... | 62 |
| 6.6 | Life Cycle Technical Controls..... | 63 |
| 6.6.1 | System Development Controls..... | 63 |
| 6.6.2 | Security Management Controls..... | 63 |
| 6.6.3 | Life Cycle Security Ratings | 63 |
| 6.7 | Network Security Controls..... | 63 |
| 6.8 | Engineering Controls | 64 |
| 7.1 | Certificate Profile | 65 |
| 7.1.1 | Version Numbers | 65 |
| 7.1.2 | Certificate Extensions | 65 |
| 7.1.3 | Algorithm Object Identifiers | 65 |
| 7.1.4 | Name Forms | 65 |
| 7.1.5 | Name Constraints | 66 |
| 7.1.6 | Certificate Policy Object Identifier | 66 |
| 7.1.7 | Usage of Policy Constraints Extension..... | 66 |
| 7.1.8 | Policy Qualifiers Syntax and Semantics | 66 |
| 7.1.9 | Processing Semantics for the Critical Certificate Policy Extension | 66 |
| 7.2 | CARL Profile | 66 |
| 7.2.1 | Version Numbers | 66 |
| 7.2.2 | CARL Entry Extensions..... | 66 |
| 8 | Maintenance | 67 |
| 8.1 | Change Procedure | 67 |
| 8.1.1 | Items that can Change without Notification..... | 67 |
| 8.1.2 | Changes with Notification..... | 67 |
| 8.1.2.1 | Change Items..... | 67 |
| 8.1.2.2 | Notification Mechanism..... | 67 |

GRCA CPS

- 8.1.2.3 Comment Period..... 67
- 8.1.2.4 Mechanism to Handle Comments 68
- 8.1.2.5 Period for Final Change Notice..... 68
- 8.2 Publication and Notification Procedure 68
- 8.3 CPS Approval Procedures 68

1 Introduction

The Government Root Certification Authority Certification Practice Statement (GRCA CPS) is stipulated following the Certificate Policy (CP) for the Government Public Key Infrastructure (GPKI). Complying with the bylaws of the Taiwan Digital Signature Act, the GRCA CPS delineates how GRCA proceeds according to the Fourth Assurance Level (High) to issue and manage the cross certificates of subject CAs.

This GRCA CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework.

1.1 Overview

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

The GRCA CPS delineates how GRCA proceeds according to the Fourth Assurance Level (High) to issue and manage the cross certificates of subject CAs. This CPS only applies to the entities related to the community of GRCA, such as GRCA, Repository, Subject CAs and Relying Parties etc.

The Research, Development and Evaluation Commission (RDEC) of the Executive Yuan is the administrative organization of GRCA. The establishment and any modification of GRCA CPS may go into effect only after obtaining the permission of RDEC and the Ministry of Economic Affairs (MOEA).

The terms and provisions of this GRCA CPS shall be interpreted and governed by

applicable laws. The ROC Government disclaims any liability that may arise from the use of this GRCA CPS.

1.2 Identification

This CPS is referred to as the GRCA CPS. This is version 1.0. Its date of publication is 15 August 2002. The newest version of the CPS can be gotten from <http://grca.nat.gov.tw/>.

The name Object Identifier (OID) of the certificate policy of GRCA is Id-tw-gpki-certpolicy-class4Assurance. Its OID value is {id-tw-gpki-certpolicy 4}. For more details, please refer the GPKI CP.

1.3 Communicability and Applicability

The following summarizes the roles relevant to the administration and operation of the GRCA.

- (1) Government Root Certification Authority
- (2) Repository
- (3) Subject Certification Authority
- (4) Relying Parties

1.3.1 Government Root Certification Authority (GRCA)

Operating in accordance with the High Assurance Level defined in the Certificate Policy of GPKI, GRCA is the trust anchor of GPKI. Acting as the interface between CAs within and without Government PKI, GRCA is responsible for carrying out cross-certification: issuing and managing the certificates of Level 1 subordinate **CAs'** within GPKI as well as the certificates of CAs from without.

The GRCA is responsible for the processing of firsthand certificate applications and revocations. There is no need to set up a Registration Authority (RA) of GRCA. The GRCA

accepts the applications from the subject CAs and authenticates them.

1.3.2 Repository

Providing service 7/24, the repository of GRCA is where information, such as certificates issued by GRCA and CARL (Certification Authority Revocation List), is posted. The web site of the repository is <http://grca.nat.gov.tw/>.

1.3.3 Subject Certification Authority

CAs, including principal CAs within and any CAs without Government PKI, that interoperate with GRCA through cross-certification are referred to as subject CAs. To get a grant from GRCA for cross-certification, the applicant CA must comply with the requirements of the Assurance level defined in the cited Certificate Policy. Additionally, the applicant CA must have the capabilities to establish and manage the following aspects:

(1) Public Key Infrastructure; (2) digital signatures and certificate issuing technology; (3) the corresponding responsibilities and obligations among CA, RA, and the relying party.

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding nature of the Subscriber's name to a public key.

The Relying Party is responsible for deciding how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate:

- (1) To verify the integrity of a digitally signed message,
- (2) To identify the creator of a message,
- (3) To establish confidential communications with the holder of the certificate.

1.3.5 Certification Service by Outsourcing

RDEC has delegated ChungHwa Telecom Co., Ltd. (CHT) (via fully outsourcing) to carry out the operations and maintenance of GRCA.

1.3.6 Applicability

1.3.6.1 Usage of Issued Certificates

The GRCA issues two kinds of certificates: the self-signed certificate and cross-certificate.

The self-signed certificate is used to establish the trust anchor of GPKI. The cross-certificate is used to build the trust relationship between interoperable CAs and helps in the certificate path processing within or without a PKI domain.

The subject of the self-signed certificate is GRCA itself and like any certificate this self-signed certificate includes the public key of GRCA. Anyone can use the self-signed certificate to verify the signature of the cross-certificate and Certification Authority Revocation List (CARL) issued by the GRCA.

The subject of a cross-certificate is one CA, which interoperates with the GRCA. This kind of CA is termed as Subject CA. The Subject CA will be more than one CA. The Subject CAs will include the Level 1 subordinate CAs within GPKI as well as the CAs from without. There is also a Subject CA's public key in the cross-certificate. Anyone can use the cross-certificate to verify the signature of the certificate and Certification Authority Revocation List (CARL) issued by the GRCA.

1.3.6.2 Notifications of Using the Certificate

Relying parties must first obtain the trusted GRCA's self-signed certificate or public key via a secure channel as described in section 6.1.4. Then relying parties can use the trusted

public key to verify the signature of cross-certificate and CARL that were signed by GRCA.

Relying parties should determine some trusted information environment such as secure computer operations system and trusted application system. This determination will avoid the replacement attack against the GRCA's self-signed certificate or public key.

The Relying parties must also make sure the GRCA's self-signed certificate or public key is correct and original before verifying the signature of the cross-certificate and CARL that were signed by GRCA.

The GRCA's cross-certificate will describe which assurance level of the Subject CA and how many levels that the Subject CA can issue cross-certificate to the other CA. And then relying parties can use this information to determine whether they want to trust the certificates issued by a Subject CA or not. Furthermore, in the content of the GRCA's cross-certificate that is issued to a Subject CA which is outside the GPKI, it will have a policy mapping field to describe the certificate policy mapping relation between the GRCA and the Subject CA. The relying parties can also be provided with this policy mapping field to determine whether or not they want to trust the certificates issued by a Subject CA.

The Relying parties must read the GRCA CPS before they adopt the certification service of the GRCA. They should also obey the regulations and pay attention to the modification of this CPS whenever they need.

1.3.6.3 Prohibitions in using the Certificate

- (1) Crime
- (2) Control of military orders for nuclear, biological, chemical weapons
- (3) Operation of nuclear equipment
- (4) Control of aviation

1.4 Contact Details

1.4.1 Specific Administrative Organization

The GRCA is responsible for establishing this CPS. The CPS may go into effect only after obtaining the permission of RDEC and MOEA.

1.4.2 Contact Person

Direct all questions regarding this CPS to the GRCA, the address can be found at <http://grca.nat.gov.tw>.

1.4.3 Person Determining Certification Practice Statement Suitability for the Policy

The RDEC is responsible for determining the suitability of this CPS for the GPKI CP. Complying with the bylaws of the Taiwan Digital Signature Act, the GRCA CPS also passes the examination of MOEACA CPS. Then the GRCA can start its certification service.

2 General Provisions

2.1 Obligations

2.1.1 GRCA Obligations

The GRCA is responsible for:

- (1) Ensuring that its own operations meet the provisions of the Assurance Level 4 of the GPKI CP,
- (2) Establishing the procedures that allow potential Subject CAs to apply for cross-certification,
- (3) Identifying and authenticating potential Subject CAs when they apply for cross-certification,
- (4) Issuing and publishing certificates as needed,
- (5) Revoking certificates as needed,
- (6) Issuing and publishing Certification Authority Revocation Lists (CARLs),
- (7) Identifying and authenticating the GRCA personnel,
- (8) Securely generating the GRCA private keys,
- (9) Ensuring safekeeping of the GRCA private keys,
- (10) Implementing key rollover of the GRCA self-signed certificate as needed, and
- (11) Processing application for issuing or revoking cross-certificates from potential Subject CAs.

2.1.2 Subject CA Obligations

Subject CAs, that are subscribers of the GRCA, are responsible for:

- (1) Abiding by the provisions of this CPS and the Cross-Certification Agreement between the Subject CA and the GRCA and being fully aware that the Subject CA may be liable for damages otherwise,

- (2) Being fully aware of the different applicability of certificates issued by the GRCA according to different assurance levels of the GPKI CP and clearly stating the assurance level under which the Subject CA wishes its own cross-certificate to be issued when applying for cross-certification from the GRCA,
- (3) Submitting valid information for cross-certificate application to the GRCA in accordance with the procedure specified in Section 4.1 of this CPS,
- (4) Accepting or rejecting its own cross-certificate in accordance with Section 4.3 of this CPS after receiving notification of certificate issuance,
- (5) Being fully aware that accepting a cross-certificate issued by the GRCA implies the confirmation of the correctness of the content of the cross-certificate,
- (6) Securely generating its own private keys in accordance with Section 6 of this CPS,
- (7) Ensuring safekeeping and proper usage of its own private keys,
- (8) Being fully aware that the legal effect of digital signature generated with the private key corresponding to the public key in its own certificate and being fully aware that it should not use the corresponding private key to generate any digital signature unless the Subject CA confirms that it accepts the certificate, the certificate is still in the validity period, and the certificate is not revoked,
- (9) Immediately notifying the GRCA of any event (such as key compromise or loss) as specified in Section 4.4.1 of this CPS, applying for certificate revocation or suspension in accordance with Section 4.4 of this CPS, and being fully aware that the Subject CA is still liable before the revocation information of its own certificate is published by the GRCA, and
- (10) Implementing obligations or liability to other party otherwise in the event that the certification or repository services of the GRCA are unavailable, and being fully aware that the event that the certification or repository services of the GRCA are unavailable should not be used as an excuse of entering a plea against the other party.

2.1.3 Relying Party Obligations

Relying parties are responsible for:

- (1) Abiding by the provisions of this CPS when using certificates issued by the GRCA or when seeking information published on the repository of the GRCA,
- (2) Acquiring the self-signed certificate of the GRCA via trusted distribution channel as described in Section 6.1.4 of this CPS,
- (3) Ensuring the applicability of certificates issued by the GRCA by checking their assurance level approved by the GRCA,
- (4) Determining the applicability of certificates issued by the GRCA by checking their key usage approved by the GRCA,
- (5) Determining the validity of certificates issued by the GRCA by checking the appropriate CARLs published by the GRCA,
- (6) Verifying the digital signature of certificates and CARLs claimed to be issued by the GRCA,
- (7) Ensuring that the rely party's computer environment is secure, ensuring that the application system is trustworthy, and being fully aware that the relying party may be liable for damages otherwise,
- (8) Implementing obligations or liability to other party otherwise in the event that the certification or repository services of the GRCA are unavailable, being fully aware that the event that the certification or repository services of the GRCA are unavailable should not be used as an excuse of entering a plea against the other party, and
- (9) Being fully aware that using certificates issued by the GRCA implies that the relying party agrees the provisions related to relying party responsibilities set forth in this CPS and that applicability of certificates set forth in Section 1.3.6 of this CPS.

2.1.4 Repository Obligations

The repository of the GRCA is responsible for:

- (1) Regularly publishing the issued certificates, issued CARLs, and other related information in accordance with Section 2.6 of this CPS,
- (2) Publishing update information of the GPKI CP and this CPS,
- (3) Providing administrative access control mechanisms when needed to protect repository information as described in Section 2.6.3 of this CPS,
- (4) Ensuring the availability of the repository.

2.2 Liability

2.2.1 GRCA Liability

2.2.1.1 Warranties and Limitations on Warranties

The GRCA warrants and promises to operate in accordance with the provisions of the Assurance Level 4 of the GPKI CP and to implement practices to ensure that its certification and repository services, issuance and revocation of certificates, and issuance of CARLs are in accordance with this CPS.

2.2.1.2 Disclaimer of Warranties

The GRCA assumes no liability whatsoever in relation to the use of certificates issued by the GRCA or associated public-private key pairs for any use other than the uses set out in Section 1.3.6 of this CPS, and subscribers will indemnify the GRCA from any such liability.

2.2.1.3 Limitations of Liability

The liability of the GRCA to the Subject CA certified by the GRCA for damages caused by issuing certificates by the GRCA or by using certificates issued by the GRCA are subject to this CPS, or contracts or cross-certificate agreements that may be entered into by the certified

Subject CA and the GRCA.

2.2.1.4 Other Exclusions

The GRCA assumes no liability for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to a force majeure.

In the event that the GRCA needs to pause all or part of its certification or repository services due to system maintenance, transit, or expansion, the GRCA will announce that event on the repository of the GRCA and notify Subject CA's; the GRCA assumes no liability for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to that event.

In the event that a Subject CA or the governing entity of a Subject CA applies for certificate revocation as set forth in Section 4.4.1 of this CPS, the GRCA will accomplish the revocation procedure, which includes validating the application, revoking the certificate, issuing CARLs, and publishing CARLs no later than 10 working days upon receiving the certificate revocation application and if the application is valid; the Subject CA is still liable, before the revocation information of the certificate is published, for the use of the certificate or its corresponding private key as set forth in this CPS; and it is the responsibility of the Subject CA to take appropriate actions, before the revocation information of the certificate is published, to protect relying parties from damages.

2.3 Financial Responsibility

The RDEC of the Executive Yuan budgets the expense of operating the GRCA and the National Audit Office of the Control Yuan audits the budget. The GRCA currently has not bought any insurance against the financial responsibility for indemnification. Other aspects of financial responsibility shall be in accordance with applicable law.

2.3.1 Indemnification by Subject CAs and Relying Parties

Should be implemented in accordance with applicable law.

2.3.2 Administrative Processes

Should be implemented in accordance with applicable law.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

The laws of the Republic of China govern the practices described in this CPS and agreements entered into by the GRCA and other party for the sake of requirements set forth in this CPS.

2.4.2 Severability of Provisions, Survival, Merger, and Notice

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

2.4.3 Dispute Resolution Procedures

Disputes between the GRCA and any Subject CA should be settled in the first instance by negotiation between the two parties. A dispute not settled by negotiation should be resolved in accordance with the GRCA dispute resolution procedure (Please refer to <http://grca.nat.gov.tw>) by asking the REDC of the Executive Yuan for the interpretation of related provisions in this CPS or the GPKI CP. In case that a lawsuit is unavoidable, the Taiwan Taipei District Court is the competent court.

2.5 Fees

The GRCA is currently being funded centrally; however the GRCA reserves the right to charge a fee to each Entity in order to operate the GRCA. These fees will only be used to fund operation of the GRCA.

In the future, if the GRCA changes the fee policy or refund policy, the GRCA will update this CPS in accordance with applicable law and publish the new fee mechanism or the new refund procedure.

2.5.1 Certificate Issuance or Renewal Fees

Free of charge.

2.5.2 Certificate Access Fees

Free of charge.

2.5.3 Revocation or Status Information Access Fees

Free of charge.

2.5.4 Fees for Other Services such as Policy Information

Free of charge.

2.5.5 Refund Policy

No fee no refund.

2.6 Publication and Repository

2.6.1 Publication of CA Information

The GRCA will publish:

- (1) The GPKI CP and the Technique Specification for the Government Public Key Infrastructure,
- (2) This CPS,
- (3) The CARLs it issues,
- (4) The self-signed certificates (Be available at least until all the certificate signed by the corresponding private key of that self-signed certificate expires.),
- (5) The cross certificates it issues,
- (6) The privacy policy of the GRCA,
- (7) The software utilities related to the use of the GRCA certification service,
- (8) The latest audit report of the GRCA, and
- (9) The latest news about the GRCA.

2.6.2 Frequency of Publication

The GRCA issues a CARL every one day and publishes the CARL in the repository once it is issued.

2.6.3 Access Controls

For the sake of security, the CA host of the GRCA will be always kept off-line, and therefore the certificates and CARLs issued by the GRCA cannot be sent to the repository directly via a computer network because there exists no any direct or indirect network line between the CA host and the repository. To publish certificates and CARLs to the repository, authorized GRCA personnel have to utilize a manual out-of-band transfer via portable media such as a floppy diskette.

The information published in the repository of the GRCA as set forth in Section 2.6.1 of this CPS is essential to all Subject CAs and relying parties. Therefore, the public anonymous read access to its information is enabled. Only authorized GRCA personnel can update the information stored in the repository. Access controls are set by administrative function and

assigned roles/responsibilities. The GRCA will endeavor to maintain the availability of its repository.

2.6.4 Repositories

The GRCA operates the repository by itself. In the event that the repository services were suspended due to system damage or any other reason, the GRCA is responsible for resuming the repository services in two working days. The URL of the repository is:

<http://grca.nat.gov.tw>.

2.7 Compliance Audit

2.7.1 Frequency of Compliance Audit

The GRCA will arrange for annual GPKI external compliance audits and casual internal compliance audits to validate that the GRCA is operating in accordance with the security practices and procedures described in this CPS.

2.7.2 Identity/Qualifications of Compliance Auditor

The RDEC of the Executive Yuan will out-source, in accordance with the Government Procurement Law, GPKI external compliance audits from external auditors that meet the following criteria:

- (1) Understanding of provisions related to GPKI compliance audits
- (2) Knowledge of the operation of the GRCA and subordinate CAs
- (3) Independence from the organization being audited

The RDEC of the Executive will identify the external compliance auditor selected to audit the GRCA.

2.7.3 Compliance Auditor's Relationship to Audited Party

The GRCA external compliance auditor will be selected by the RDEC of the Executive

Yuan in the process of out-sourcing, in accordance with the Government Procurement Law, GPKI external compliance audits.

2.7.4 Topics Covered by Compliance Audit

The GRCA compliance audit will address:

- (1) The GRCA operates in accordance with this CPS; and
- (2) This CPS outlines, in sufficient detail, the technical, procedural, and personnel practices of the GRCA that meet the requirements of the GPKI CP.

2.7.5 Actions Taken as a Result of Deficiency

If deficiencies in the deployment or operation of the GRCA with respect to the GPKI CP, this CPS, or Cross-Certification Agreements are found in the audit, the course of actions include:

- (1) The compliance auditor shall note the discrepancy;
- (2) The compliance auditor shall notify the GRCA of the discrepancy;
- (3) The GRCA will promptly correct the discrepancy and then notify the compliance auditor for reexamination; and
- (4) Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the GRCA will decide to halt temporarily operation of the GRCA, to revoke a cross-certificate issued by the GRCA, or take other actions it deems appropriate.

2.7.6 Communication of Results

The conclusive results of the most recent audit will be made public in electronic form and published in the repository of the GRCA. Conclusive results is here defined to be information of all deficiencies which may affect a relying party's trust in a certificate issued by the GRCA but excluding detailed information which can be used to attack the GRCA system.

2.8 Confidentiality

2.8.1 Types of Information to be Kept Confidential

Any certificate application information held by the GRCA which is not appearing on issued certificates is considered confidential. Both present and former employees are responsible for strictly keeping the confidential information. For the GRCA:

- (1) All private and secret keys used and handled within the GRCA operations are to be kept confidential;
- (2) The safekeeping information of the secret shares of the GRCA private keys is to be kept confidential;
- (3) Any certificate application information held by the GRCA will not be released without the prior consent of the subscriber, unless required otherwise by law;
- (4) Audit trail records created or retained by the GRCA are to be kept confidential;
- (5) Audit reports generated during external or internal compliance audits shall not be made available as a whole, except as required by law; and
- (6) All classified GRCA operational documents and manuals are to be kept confidential.

2.8.2 Types of Information not Considered Confidential

- (1) Certificates, CRL's and revocation/suspension information published in the GRCA repository are not considered confidential.
- (2) Identification information or other information appearing on certificates is not considered confidential, unless statutes or special agreements so dictate.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

There is no certificate suspension information produced by the GRCA since the GRCA does not provide certificate suspension service. Certificate revocation information produced is

not considered confidential and will be made public in the GRCA repository as specified in Section 2.8.2 of this CPS.

2.8.4 Release to Law Enforcement Officials

In the event that juridical apparatuses, control apparatuses, or security apparatuses need confidential information specified in Section 2.8.1 of this CPS for the purpose of investigation or searching for evidences, the procedure is subject to applicable laws. However, the GRCA reserves the right to collect reasonable fees from the inquirer to cover the expense of providing such information.

2.8.5 Release as Part of Civil Discovery

In the event that juridical apparatuses, control apparatuses, or security apparatuses need to inquire into confidential information specified in Section 2.8.1 of this CPS for the purpose of investigation or searching for evidences, the procedure is subject to applicable laws. In this case, the GRCA will likewise collect reasonable fees from the inquirer to cover the expense of providing such information.

2.8.6 Disclosure Upon Owner's Request

A Subject CA has the right to inquire certificate application information as specified in item (3) of Section 2.8.1 of this CPS. However, the GRCA reserves the right to collect reasonable fees from the inquirer to cover the expense of providing such information.

2.8.7 Other Information Release Circumstances

According to applicable laws.

2.8.8 Privacy Protection

The GRCA will protect certificate application information in accordance with “the Privacy Protection Act of Person Data in Computer Processing” of the Republic of China.

2.9 Intellectual Property Rights

The GRCA retains all intellectual property rights in and to its own key pairs and their secret shares. A Subject CA retains all intellectual property rights to its own key pairs. However, the GRCA retains all intellectual property rights in and to certificates issued by the GRCA even though the certificates contain public keys of Subject CAs.

The GRCA retains all intellectual property rights to the subject names of its self-signed or self-issued certificates.

The GRCA will ensure the correctness of the names of Subject CAs to the best of its capability. However, the GRCA shall not be responsible for the dispute resolution of the ownership of the names of Subject CAs. In the event that the registration mark dispute occurs in the name of a Subject CA, the Subject CA should resolve the dispute in accordance with applicable laws and notify the GRCA of the result of the dispute resolution in order to protect its own rights.

The RDEC of the Executive Yuan and Chunghwa Telecom Co., Ltd. co-retain all intellectual property rights in and to all documents written for running certificate management service of the GRCA.

The RDEC of the Executive Yuan and Chunghwa Telecom Co., Ltd. co-retain all intellectual property rights in and to this CPS. This CPS can be downloaded from the GRCA repository for free, and can be, to the extent permitted by the Copyright Act, reproduced or distributed for free provided that the copy is intact. Those who reproduce or distribute this CPS should not charge a fee for this CPS itself and should not restrict the access to this CPS. In no event will the RDEC of the Executive Yuan or Chunghwa Telecom Co., Ltd. be liable for any

GRCA CPS

losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any improper usage or distribution of this CPS.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

The subject name of the certificate issued by Government Root Certification Authority conforms to the Distinguished Name of X.500. The self-signed certificate of Government Root Certification Authority and cross-certification certificates among certification authorities use the same type of Distinguished Name.

3.1.2 Need for Names to be Meaningful

The organization names applying for cross-certification should comply with the naming rule of related laws. Meanwhile, names should be able to represent and identify the certification authority.

3.1.3 Rules for Interpreting Various Name Forms

According to the certificate profile in the technical specification of Government Public Key Infrastructure, rules for interpreting various name forms should comply with the Name attribute definition of ITU-T X.520.

3.1.4 Uniqueness of Names

Government Root Certification Authority examines the uniqueness of organization names applying for cross-certification. If a duplicate name is found then the applying certification authority is required to change the name.

In favor of international interoperabilities, the self-signed certificate of Government Root Certification Authority uses the following name form:

C=TW , O=Government Root Certification Authority

Moreover, in the self-signed certificate of Government Root Certification Authority the issuer name is identical to the subject name.

3.1.5 Name Claim Dispute Resolution Procedure

The resolution of name claim dispute is the responsibility of Research Development and Evaluation Commission.

3.1.6 Recognition, Authentication, and Role of Trademarks

Not applicable.

3.1.7 Method to Prove Possession of Private Key

Government Root Certification Authority examines whether the private key of the certification authority in question and the public key in the announcing certificate work in pairs. Using the public key in the PKCS#10 certification request file generated by the certification authority in question to verify the signature in the same file, Government Root Certification Authority can insure that the applying certification authority owns the corresponding private key.

3.1.8 Authentication of Organization Identity

The application form for cross-certification submitted by certification authorities should include organization name, locality and representative information that are sufficient to identify the organization. Government Root Certification Authority examines the existence of the organization, meanwhile verifies the official document, representative identity and the representative's authority of representing the organization. The organization representative is required to apply the certificate in person. For certification authorities outside of Government Public Key Infrastructure, the above authentication process of organization identity applies.

3.1.9 Authentication of Individual Identity

The governmental organization should assign a representative (the person who is authorized to apply for cross-certification) with official documents to apply for the certificate of certification authority. The authentication process is as follows:

- (1) Formal document check: The representative should show his/her identification card or passport while applying for certificates so that Government Root Certification Authority may authenticate the representative's identity. The identification number, name and registered permanent residence are compared with the application information submitted by the certification authority.
- (2) Submit the representative's authorization document.
- (3) The representative must prove his/her identity in person.

3.1.10 Authentication of Hardware Device or Server Software

Not applicable.

3.2 Routine Key Change and Certificate Renewal

3.2.1 Routine Certificates Renewal

Routine key change is the issuance of a new certificate that has the same feature and guaranteed grade as the old certificate. In addition to owning another newly generated public key (paired with a new private key) and a new serial number, the new certificate might be assigned a different valid period.

The private key of Government Root Certification Authority itself is 4,096 bits long, valid for 10 years, yet its public key certificate has a validity period of 30 years. Government Root Certification Authority will change the key pair and issue a new self-signed certificate if:

- (1) Current key pair is expired.

- (2) The security of current key pair is dubious. For instance, the private key is suspected or sure to be compromised.

Cross-certification organizations processing the key changes should apply for new certificates from Government Root Certification Authority. The Government Root Certification Authority identifies and authenticates the organization applying for cross-certification according to the rules described in section 3.1.

3.2.2 Certificate Renewal

Government Root Certification Authority disallows the renewal of its self-signed certificate and the subordinate cross-certification certificates.

3.3 Rekey after Revocation

After the certificate revocation for certification authorities, the identification and authentication process of the new certificate application follows the rules described in section 3.1 to initialize a registration.

3.4 Revocation Request

The authentication process of certificate revocation requests for cross-certification organizations is the same as the process described in section 3.1.8 and 3.1.9.

4 Operations Requirement

4.1 Certificate Application

(1) Initial Process

1. Initial application

Cross-certification request form shall be accompanied by the Certification Practice Statement and Certification request file in PKCS#10 format shall be post mailed via formal official document. If the Certification Authority adopts Certificate Policy other than GPKI-CP, then its complying Certificate Policy shall also be included.

2. Identification and authentication

Identification and authentication of the applicants shall be performed in accordance with procedures defined in section 3.1.8.

3. Verification

It shall be confirmed that there is no technological incompatibility between applicant Agency and GRCA. If GPKI-CP is not adopted, the policy mapping shall be examined. It shall be verified that CPS of applicant Agency complies with its adopting CP. Certification request file in PKCS#10 shall be verified to ensure that the actual cross-certification can be carried out.

(2) Examination

The Task Force Committee for the Promotion of Electronic Authentication shall be convened in which the submitted documents together with the GRCA verifying summary shall be evaluated. Based on the evaluation, this Committee shall make a determination regarding whether or not to enter into next stage, to demand additional supporting documents, or to reject the request.

(3) Arrangement

An arrangement meeting shall be convened which the applicant agency shall be

notified to attend. It shall proceed as follows:

1. Identification and authentication

Before the commencement of the meeting, the delegate of the applicant agency shall be identified and authenticated in accordance with section 3.1.9.

2. The terms and conditions to be followed shall be negotiated with the applicant agency.

3. If the cross-certification is deemed feasible, than it is ratified by signing the Cross-Certification Agreement.

4. Proceed to certificate issuance process.

4.2 Certificate Issuance

Based upon the ratification result of the cross-certification, GRCA shall determine whether or not to issue the requested certificate(s). GRCA will carry out certificate issuance process. When the issuance is done, the applicant agency shall be notified by formal official document with its issued certificate(s) included. If the request of certificate is rejected, the applicant agency shall be notified by formal official document, with explanation as to why the request was rejected.

A Self-Signed Certificate shall be signed by GRCA and shall delivered to the relying parties in accordance with Section 6.1.4.

4.3 Certificate Acceptance

Upon receiving the formal official document for granting the application request, the applicant agency (now Subscriber) shall check the correctness of the content of included certificate(s). If the content is correct, the Subscriber shall sign and send back (in the formal official document) the acceptance document to complete the acceptance procedure. Upon receiving the acceptance document, GRCA shall publish the corresponding issued certificate(s)

in the depository. If the Subscriber fails to send back the signed acceptance document, it is deemed a refusal of acceptance. In this case, GRCA shall revoke the corresponding certificate(s) without further announcement.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances under which a Certificate may be revoked

The Agency must request for the revocation of its certificate(s), should (but not limited to) any of the following situations occurs:

- (1) The corresponding private key of the Agency is suspected or confirmed to be compromised.
- (2) The certificate(s) is no longer needed, which may have been due to the termination of the Agency service or termination of the cross-certification between GRCA.

In addition, GRCA shall revoke the certificate(s) of the Agency without prior approval from the Agency, should any of the following situations occurs:

- (1) Incorrectness of any part of the certificates content
- (2) Confirmed case of un-authorized use, forge, or compromise of the Agency's private key.
- (3) In case of confirmed un-authorized use, forgery, or compromise of the GRCA's private key, all of the cross-certificates signed by GRCA shall be revoked.
- (4) The certificate(s) of Agency is not issued in accordance to this Certification Practice Statement.
- (5) The Agency does not operate in accordance with its CPS or Cross-Certification Agreement, or applicable laws or regulation.
- (6) The revocation is requested by the supervising organization of the Agency or is required by laws or regulation.
- (7) GRCA terminates its services.

If the main information in the certificate needs to be updated, GRCA shall review and determine if the certificate should be revoked.

4.4.2 Who can Request Revocation of a Certificate Issued by GRCA

- (1) Interoperating Agency which requests revocation of its Cross-certificate.
- (2) Supervising organization of the Agency

4.4.3 Procedure for Revocation

(1) Initial Process

1. Initial request

Request shall be brought out via formal official document, with revocation request form filled-in and included.

2. Identification and authentication

Identification and authentication of the Agency shall be carried out in accordance to section 3.1.8.

3. Request review

Handed-in documents shall be reviewed to determine the feasibility of the revocation.

4. Determination

Determine whether to enter next stage, to ask for additional supporting documents, or to notify the Agency via formal official document of the denial of its revocation request. In the case of the denial, explanation shall be enclosed.

(2) Certificate revocation

If the revocation request appears to be valid, GRCA shall revoke the certificate, insert the certificate in CARL, and post the CARL in the GRCA repository. The Agency and its supervising organization shall be notified of the revocation through formal

official document. The certificate status information posted at the depository shall include revoked certificates until its expiration date.

4.4.4 Revocation Request Grace Period

Should any of the situations described in Section 4.4.1 occurs, the Agency shall request for revocation within 10 working days and if possible, before GRCA publishes the updated CARL.

4.4.5 Circumstances under which a Certificate may be Suspended

Suspension shall not be provided by GRCA.

4.4.6 Who can Request the Suspension of a Certificate

Not applicable.

4.4.7 Procedure for suspension request

Not applicable.

4.4.8 Suspension Request Grace Period

Not applicable.

4.4.9 CARL Issuance Frequency

CARLs shall be issued once each day. The updated CARL shall be published in the depository.

4.4.10 CARL Checking Requirements

Before checking CARL published in the depository, the Relying Party should verify the digital signature to confirm the correctness of the CARL. Refer to section 2.6.3 for the conditions necessary for the relying parties to check information that is published in depository.

4.4.11 On-line Revocation / Status Checking

On-line Revocation / Status checking is not provided.

4.4.12 On-line Revocation / Status Checking Availability

Not applicable.

4.4.13 Other Forms of Revocation Advertisements Available

No other forms of revocation advertisements are provided.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

Not applicable.

4.4.15 Special Requirements Related to Key Compromise

In the event of an Agency CA private key compromise, GRCA shall note in the published CARL that the reason code for revocation of corresponding key is Key Compromise.

4.5 Security Audit Procedures

Audit log files shall be generated for all events relating to the security of the GRCA. The security audit logs shall be automatically generated by the system, or manually recorded by a logbook, paper form, or other physical mechanism. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with *Retention period for archive*, Section 4.6.2.

4.5.1 Types of Events Recorded

(1) Security Audit

1. Any changes to the Audit parameters, e.g., audit frequency, type of event audited
2. Any attempt to delete or modify the Audit logs

(2) Identification and Authentication

1. Successful and unsuccessful attempts to assume a role
2. Change in the value of maximum authentication attempts
3. Maximum number of unsuccessful authentication attempts during user login
4. An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
5. An Administrator changes the type of authenticator, e.g., from password to biometrics

(3) Key Generation

Whenever GRCA generates a key.

(4) Private Key Load and Storage

The loading of Component private keys

(5) Trusted Public Key Entry, Deletion and Storage

All changes to the trusted public keys, including additions and deletions

(6) Private Key Export

The export of private keys (keys used for a single session or message are excluded)

(7) Certificate Registration

All certificate requests and processes

(8) Certificate Revocation

All certificate revocation requests and the processes

(9) Certificate Status Change Approval

The approval or rejection of a certificate status change request

(10) GRCA Configuration

Any security-relevant changes to the configuration of the GRCA

(11) Account Administration

1. Roles and users are added or deleted
2. The access control privileges of a user account or a role are modified

(12) Certificate Profile Management

All changes to the certificate profile

(13) Certificate Revocation List Profile Management

All changes to the certificate revocation list profile

(14) Miscellaneous

1. Installation of the Operating System
2. Installation of the GRCA
3. Installing hardware cryptographic modules
4. Removing hardware cryptographic modules
5. Destruction of cryptographic modules
6. System Startup
7. Logon Attempts to GRCA Apps
8. Receipt of Hardware / Software
9. Attempts to set passwords
10. Attempts to modify passwords
11. Backing up GRCA internal database
12. Restoring GRCA internal database
13. File manipulation (e.g., creation, renaming, moving)
14. Posting of any material to a repository
15. Access to FBCA or Agency CA internal database
16. All certificate compromise notification requests
17. Loading tokens with certificates
18. Rekey of GRCA or Agency CA

(15) Configuration changes to the GRCA server involving:

1. Hardware
2. Software
3. Operating System
4. Patches
5. Security Profiles

(16) Physical Access/Site Security

1. Personnel Access to room housing GRCA
2. Access to the FBCA or Agency CA server
3. Known or suspected violations of physical security(

(17) Anomalies

1. Software Error conditions
2. Software check integrity failures
3. Receipt of improper messages
4. Misrouted messages
5. Network attacks (suspected or confirmed)
6. Equipment failure
7. Electrical power outages
8. Uninterruptible Power Supply (UPS) failure
9. Obvious and significant network service or access failures
10. Violations of Certificate Policy
11. Violations of Certification Practice Statement
12. Resetting Operating System clock

4.5.2 Frequency of Processing Data

GRCA shall review audit logs once every month to keep track all significant events.

Such reviews involve verifying that the log has not been tampered with, inspecting all log entries, and investigating any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

4.5.3 Retention Period for Security Audit Data

Audit logs shall be retained onsite for two months as well as being retained in accordance with sections 4.5.4、4.5.5、4.5.6 and 4.6. The removal of the expired audit logs of the GRCA system shall be performed by no other parties than the auditors.

4.5.4 Protection of Security Audit Data

- (1) Current and archived audit data shall be protected by digital signing and encryption technologies and shall be stored in CD-R or other non-modifiable storage media.
- (2) Private keys used to sign event log shall not be used for any other purpose. Use of Private keys of audit system for any other purpose is strictly prohibited. Audit system shall not reveal private keys.
- (3) Manual audit logs shall be moved to a safe, secure storage location.

4.5.5 Security Audit Data Backup Procedures

Electronic audit logs and audit summaries shall be backed up monthly. A copy of the audit log shall be sent off-site in accordance with the CPS on a monthly basis.

- (1) GRCA shall periodically back up the event logs: audit system shall automatically archive the audit trail data daily, weekly and monthly.
- (2) GRCA shall store audit logs in a safe location.

4.5.6 Security Audit Collection System (Internal vs. External)

Audit processes shall be invoked at GRCA system startup, and cease only at GRCA

system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the GRCA shall temporarily stop issuing certificates until the problem is remedied.

4.5.7 Notification to Event-Causing Subject

When an event was audited, the audit system does not need to provide notice to the individual, organization, device, or application that caused the event.

4.5.8 Vulnerability Assessments

- (1) Vulnerability Assessment on the operation systems.
- (2) Vulnerability Assessment on the physical facilities.
- (3) Vulnerability Assessment on the certification authority systems.
- (4) Vulnerability Assessment on the network

4.6 Records Archival

4.6.1 Types of Events Archived

- (1) GRCA accreditation record
- (2) Certification Practice Statement
- (3) Cross-certification agreement
- (4) System and equipment configuration
- (5) Modifications and updates to system or configuration
- (6) Certificate requests
- (7) Revocation requests
- (8) Documentation of receipt and acceptance of certificates
- (9) All certificates issued or published
- (10) Record of FBCA or Agency CA Re-key

- (11) All CARLs and CRLs issued and/or published
- (12) All Audit Logs
- (13) Other data or applications to verify archive contents
- (14) Documentation required by compliance auditors
- (15) Subscriber identity Authentication data as per Section 3.1.8 and 3.1.9

4.6.2 Retention Period for Archive

The retention period for archive data in GRCA is 20 years. Applications required to process the archive data shall also be maintained for 20 years.

4.6.3 Protection of Archive

- (1) It is not permitted to write to, modify, or delete the archive
- (2) GRCA may move archived records to another storage medium and shall provide proper protection with level of assurance not lower than the original one.
- (3) Archive media shall be stored in a safe, secure storage facility.

4.6.4 Archive Backup Procedures

The backup of archive data shall be stored in off-site backup center, currently located in Taoyuan country. (Refer to section 5.1.8)

4.6.5 Requirements for Time-Stamping of Records

Electronic archive data (such as certificates, Certification Authority Revocation Lists and audit data, etc.) shall be time-stamped and protected by proper digital signatures so that the integrity of the time-stamps can be verified. However the time-stamps on these archive data are not electronic time-stamps provided by trusted third-party. Rather, they are obtained from the clock of computer operation system. The system clocks of all the computers of GRCA shall be

periodically adjusted to ensure the precision and reliability. The paper archive documentation shall also be dated, and even time-stamped if necessary. The time and date on the paper documentation shall not be altered unless the modification is acknowledged and signed by the auditors.

4.6.6 Archive Collection System (Internal or External)

GRCA does not have an archive collection system.

4.6.7 Procedures to Obtain and Verify Archive Information

Archive information may be obtained upon the receipt of formal authorization of request in-writing. The auditors are in charge of verifying the archive information. In the case of paper documentation, the authenticity of the dates and signatures shall be verified, whereas the digital signature of the electronic archive information will be verified.

4.7 Key Changeover

The GRCA's signing key shall be changed no later than 3 months prior to the expiration date of its self-signed certificate. A new self-signed GRCA certificate shall be issued at the same time. New self-signed certificate shall be delivered to the relying parties in accordance with section 6.1.4.

Cross-certified organizations shall change their signing keys no later than 2 months prior to the expiration date of their certificates and shall request (in accordance with section 4.1) new certificates from GRCA after key changeover is done.

4.8 Compromise and Disaster Recovery

4.8.1 Computing Resources, Software, and/or Data are Corrupted

GRCA shall define recovery procedures used if GRCA computing resources, software, and/or data are corrupted. Recovery drill will be practiced every year. If GRCA equipment is

damaged or rendered inoperative, but the GRCA signature keys are not destroyed, GRCA operation shall be reestablished as quickly as possible, giving priority to the operation of GRCA repository.

4.8.2 GRCA Signature Keys are Revoked

GRCA shall define recovery procedures used if the GRCA signature keys are revoked. Recovery drill will be practiced every year.

4.8.3 GRCA Signature Keys are Compromised

GRCA shall define recovery procedures used if the GRCA signature keys are compromised. Recovery drill will be practiced every year.

4.8.4 Secure Facility after a Natural or Other Type of Disaster

GRCA shall practice the disaster recovery drill of the secure facility every year.

4.9 CA Termination

In the event of termination of the GRCA operation, it will follow the procedure defined by 電子簽章法. To minimize the impact on the subordinate CA's and the subscribers in the event of termination, GRCA will:

- (1) Notify the cross-certificating organizations and publish the announcement in the depository 3 month before the proposed termination date.
- (2) Revoke any un-revoked or not expired certificates upon termination, and safe-keep and consign record archive following the regulation defined in 電子簽章法.

5 Non-Technical Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The GRCA facility is located in the housing of Chunghwa Telecom Data Communication Branch. The construction of the facility housing is consistent with facilities used to house high value, sensitive information. Combined with other physical security protection mechanisms including guards, video monitoring and intrusion sensors it provides robust protection against unauthorized access to the GRCA equipments.

5.1.2 Physical Access

The physical access control of the GRCA meets the level 4 assurances defined in the GPKI CP. There are four guarding levels in the GRCA facility housing. The first and second levels are 24 hours entry guards and building guards. The third level using IC card technology performs the building story access control. The forth level is a fingerprint access control system that uses a 3D sampling technology and is capable of detecting the tint, penetration and live state.

The physical access control system of the GRCA is able to protect the facilities from unauthorized access. The computer rack is able to prevent any unauthorized access to any hardware, software, or hardware secure module in the GRCA.

Any portable storage device brought to the facility housing shall be checked without computer software virus and any other software that may damage the GRCA system.

Under certain circumstances, unauthorized persons may need to be in the facilities housing. This access can only be performed when an authorized person is presented and all actions taken by the unauthorized person shall be recorded. The authorized person needs to perform the following checks after the unauthorized persons is left the facilities housing

- (1) Check the operation of system equipment
- (2) Lock the computer rack
- (3) Check the operation guarding system

5.1.3 Electrical Power and Air Conditioning

In addition to commercial power, the power system of the GRCA has backup capability (sufficient to support 6 continue day operation) and is provided with Uninterrupted Power System. The switch between commercial power system and backup power system is automatic and the power shall be sufficient for a minimum of six hours operation to backup the process data.

The GRCA facilities housing has an automatic temperature and a humidity control system to provide a proper environment for the operation of the GRCA.

5.1.4 Flood Prevention and Protection

The GRCA facilities housing is placed in a building without any flooding damage history. The building has water gate and water pump protection and the story used for the GRCA equipment is higher than third story.

5.1.5 Fire Prevention and Protection

The GRCA facilities housing has an automatic fire prevention and protection system and every entry provides a switch that allows person in emergency situation manually enable the fire prevention and protection system.

5.1.6 Media Storage

The data of audit, archive, and backup shall be stored in the facilities housing at least one year. After one year, the data shall be moved to the off-site backup location that is separated

from the GRCA system.

5.1.7 Waste Disposal

When the secret information and documents of the GRCA described in section 2.8.1 become useless all paper shall be processed by a paper cutting machine; tapes, hard disks, disks, MO and other types of memory shall be formatted to erase all information and then physically destroyed.

5.1.8 Off-site Backup

The off-site backup location is in Taoyuan, 30 km away from the GRCA facilities housing. The information including system programs and data shall be duplicated at least once per week. Modified data shall be duplicated within 24 hours. The backup site has physical and procedural controls commensurate to that of the operational GRCA.

5.2 Procedural Controls

In order to protect the security of the GRCA operations, the GRCA uses procedural controls to define the roles of operators, the number of persons required per task, and the identification and the authentication for each role.

5.2.1 Trusted Roles

In order to properly separate the duty of each operation and to prevent the damage caused by internal operations, the execution of every operation performed in the GRCA is clearly defined according to operator roles. There are five trusted roles defined in the GRCA including administrator, officer, auditor, operator, and controller. Each role is administrated according to section 5.3 to prevent the damage caused by internal operators. Every trusted role can be assigned to one individual or a group and one of that group should be assigned as chief role.

The job for each role is assigned as the followings.

- (1) Administrator: authorized to install, configure, and maintain the GRCA; establish and maintain user accounts; configure profiles and audit parameters; and generate as well as backup component keys.
- (2) Officer: authorized to request or approve certificates or certificate revocations.
- (3) Auditor: authorized to review, maintain, and archive audit logs; perform or oversee internal compliance audits to ensure that the GRCA is operating in accordance with its CPS
- (4) Operator: authorized to execute the routine operation of the GRCA equipment and operations such as system backups and recovery or changing recording media; Update software except the GRCA system programs; maintain the networks and Web servers including building an anti_virus system capable of detecting and reporting the network security events.
- (5) Controller: authorized to execute the physical controls of the GRCA facilities. (system access controls, air condition, flood, and fire prevention...)

5.2.2 Roles Assignments

The trusted roles as defined in section 5.2.1 must comply with the following roles

- (1) Individual may assume only one of the Administrator, Officer, and Auditor roles, but the individual may assume the operator role.
- (2) The controller may not assume other roles.
- (3) No individual may execute the self-audit function

5.2.3 Number of Persons Required Per Task

According to the security requirements, the number of each trusted role is assigned as the following:

GRCA CPS

- (1) Administrator: at least 3 qualified individuals
- (2) Officer: at least 3 qualified individuals
- (3) Auditor: at least 2 qualified individuals
- (4) Operator: at least 2 qualified individuals
- (5) Controller: at least 2 qualified individuals

The number of each assignment is given as the following:

| Assignments | Administrator | Office | Auditor | Operator | Controller |
|---|---------------|--------|---------|----------|------------|
| Installation, configuration, and maintenance of the GRCA; | 2 | | | | 1 |
| Establishing and maintaining the GRCA user accounts | 2 | | | | 1 |
| Configuring audit parameters | 2 | | | | 1 |
| Generating and backing up the GRCA keys | 2 | | 1 | | 2 |
| Issuing certificates | | 2 | | | 1 |
| Revoking certificates | | 2 | | | 1 |
| Publishing CRL | | 1 | | | 1 |
| Reviewing, maintaining, and archiving audit logs | | | 1 | | 1 |
| Daily routine operation | | | | 1 | 1 |
| System backing up and recovery | | | | 1 | 1 |
| Changing recording media | | | | 1 | 1 |
| Software and hardware update except the GRCA system | | | | 1 | 1 |
| Maintaining Network and Web server | | | | 1 | 1 |
| Configuring physical controls | | | | | 2 |

5.2.4 Identification and Authentication for Each Role

The GRCA utilizes system account management functions and IC cards to identify and authenticate administrator, office, auditor, operator, and controller.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

(1) The evaluation items of security requirements

1. Personality
2. Experiences
3. Academic and professional qualifications
4. Personal Identification
5. Trustworthiness

(2) The management of trusted roles

All GRCA operators shall be identified and authenticated before being permitted to perform any action. All operators shall receive comprehensive training and sign a document to accept the responsibility of performing duties. All operators shall be evaluated every year, and if individual cannot pass the evaluation, he/she should be replaced by a qualified individual.

(3) The shift of GRCA operators

The hiring or the changes of employee contract, especially personal quit or contract terminated the personal shall obey the role of keeping the confidential information of the GRCA.

(4) The responsibility of keeping confidential information

All GRCA operators shall sign a contract to keep the information about the GRCA as confidential and the confidential information cannot be revealed through copy, publish, or other methods.

5.3.2 Background Check Procedures

The GRCA shall check the requirements and necessary documents to identify the trusted

roles defined in Section 5.2.1.

5.3.3 Training Requirements

| Trusted Roles | Training Requirements |
|---------------|--|
| Administrator | <ol style="list-style-type: none">1. GRCA authorization2. Installation, configuration, and maintenance of the GRCA3. Establishing and maintaining the procedure of cross certification4. Establish the procedure of configuring audit parameters5. The procedure of generation and backup component keys6. The procedure of disaster recovery and daily maintenance |
| Officer | <ol style="list-style-type: none">1. GRCA authorization2. The operations of both GRCA software and hardware3. The procedure of issuing certifications4. The procedure of revoking of certifications5. The procedure of disaster recovery and daily maintenance |
| Auditor | <ol style="list-style-type: none">1. GRCA authorization2. The operations of both GRCA software and hardware3. The procedure of generation and backup component keys4. Reviewing, maintaining, and archiving audit logs5. The procedure of disaster recovery and daily maintenance |
| Operator | <ol style="list-style-type: none">1. GRCA authorization2. The routine operations3. The procedure of changing recording media4. The procedure of disaster recovery and daily maintenance5. The maintenance of Web Services |
| Controller | <ol style="list-style-type: none">1. The procedure of configuring the physical controls2. The procedure of disaster recovery and daily maintenance |

5.3.4 Retraining Frequency and Requirements

All operators shall aware of the changes of the GRCA software or hardware upgrade, routine procedure, CP, or CPS. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented to insure that all operators understand the changes.

5.3.5 Job Rotation Frequency and Sequence

- (1) There is at least one year needed before an administrator can be shifted to be an operator or an auditor.

- (2) There is at least one year needed before an officer can be shifted to be an administrator or an auditor.
- (3) There is at least one year needed before an auditor can be shifted to be an administrator or an officer.
- (4) After a properly training and two years experiences, an operator can have the qualification to be an operator, an administrator, or an auditor.

5.3.6 Sanctions for Unauthorized Actions

The GRCA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving GRCA or its repository not authorized in this CP, the GRCA CPS, or other procedures published by the GRCA Operational Authority.

5.3.7 Contracting Personnel Requirements

No contractor personnel should be employed. All trusted roles should be working on the basis of full-time employee.

5.3.8 Documentation Supplied to Personnel

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

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

According to section, 6.2.1, GRCA generates key pairs using RSA algorithm within the hardware security module via True Random Number Generator; private keys are generated within the hardware security module and they are not distributed at all.

GRCA Key generation is witnessed by those related personnel who also sign the (GRCA) Public Key Initiation Witness document; this document records the public key pairs generated. This public key is distributed via the trusted channels.

A CA which is cross-certified with GRCA must generate key pairs according to its Certificate Policy.

While issuing cross certificates to its cross-certified CAs, GRCA checks the public key in each certificate request file to ensure that each CA's public key is unique.

6.1.2 Private Key Delivery to Cross-certified CAs

Any CA cross-certified with GRCA has to generate the private key by itself. Therefore, GRCA does not need to deliver private keys to any cross-certified CA.

6.1.3 Public Key Delivery to GRCA

A cross-certified CA will send its PKCS#10 certificate request when it requests for cross certification with GRCA.

6.1.4 GRCA Public Key Delivery to Relying Parties

GRCA self-signed certificate contains its public key. There are several secure distribution channels as follows.

- (1) After GRCA has issued a cross certificate to a CA, it will deliver this cross certificate along with the GRCA self-signed certificate or public key to this CA. This CA stores GRCA self-signed certificate or public key into the token (such as IC card, etc). This CA distributes such token securely to the certificate users or relying party.
- (2) GRCA self-signed certificate is stored in the build-in reliable software issued by trusted third party. Certificate users obtain this software via the secure channel (for example, purchase software installation CD-ROM from reliable distributors). After the installation, GRCA self-signed certificate is obtained by the certificate users simultaneously.
- (3) GRCA self-signed public key certificate stores in CD-ROMs with large volume of circulation; certificate users obtain these CD-ROMs via secure channels, at the same time, they will obtain the GRCA self-signed certificate.
- (4) While GRCA is activated, its public key will be announced; at the same time, related personnel will sign GRCA public key witness document and deliver it to the media for announcement. Relying party can compare the GRCA public key announced by the media with the one contained in the GRCA self-signed public key certificate downloaded from Internet.

6.1.5 Key Sizes

GRCA adapts 4096-bit RSA public keys pairs and SHA-1 hash function to issue certificates. A cross-certified CA has to follow its certificate policy to choose a proper key size. GRCA will exam whether this CA has chosen an appropriate key size before it issues a cross certificate to this CA.

6.1.6 Public Key Parameters Generation

The public key parameter of the RSA algorithm is Null.

6.1.7 Parameter Quality Checking

GRCA adapts ANSI X9.31 algorithm to generate the prime numbers used in the RSA algorithms. This method can guarantee such generated prime numbers are strong prime.

A cross-certified CA has to proceed key parameters quality checking depending on the algorithm it chooses.

6.1.8 Hardware/Software Key Generation

GRCA adapts hardware cryptographic modules to generate random numbers, public keys and symmetric keys.

A Cross-certified CA has to follow the stipulations from its certificate policy to choose appropriate software and/or hardware to generate keys. Before issuing a cross certificate, GRCA will examine whether the software and hardware chosen by this CA is appropriate.

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

The private key corresponding to the GRCA self-signed certificate can only be used for issuing certificates and ARL. GRCA self-signed certificate does not contain the *KeyUsage* extension field.

Cross certificates issued by GRCA set two key usage bits: cRLSign and CertSign , in the *KeyUsage* extension field.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

According to the certificate policy, GRCA uses hardware secure modules with the assurance level 3.

A Cross certified CA has to follow the stipulations from its certificate policy to choose an

appropriate cryptographic module. Before issuing a cross certificate, GRCA will check whether the assurance level of the cryptographic module chosen from this CA is appropriate.

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

GRCA private key multi-person control adapts the m-out-of-n LaGrange Polynomial Interpolation. It is a perfect secret sharing method which can be used for private key splitting and recovering. Adapting such method can guarantee the highest assurance level for GRCA private key multi-person control; therefore it can be used for the private key activation method (also refer to section 6.2.7).

If GRCA is about to issue a private key which is used for CA's digital signature generation with assurance level 3 or 4 to a CA, it has to follow its certificate policy to adapt multi-person procedure. Before issuing a cross certificate, GRCA examines whether this CA has adapted an appropriate Multi-Person control.

6.2.3 Private Key Escrow

The GRCA private key used for digital signature generation cannot be escrowed. GRCA is not responsible for managing any private key used for signature from any cross-certified CA.

6.2.4 Private Key Backup

According to section 6.2.2, GRCA adapts the private key multi-person control to backup the private key. It also uses highly secure IC cards to store secret sharing.

A cross-certified CA has to follow stipulations from its certificate policy to choose an appropriate private key backup method. Before issuing a cross certificate, GRCA has to examine whether the private key backup method chosen by this CA is appropriate.

GRCA is not responsible for managing private key backups for any cross-certified CA.

6.2.5 Private Key Archival

The GRCA private key for digital signature cannot be archived. GRCA does not archive any CA's private key used for digital signature.

6.2.6 Private Key Entry into Cryptographic Module

Only when GRCA is backing up keys, it can import private keys into cryptographic modules.

If a cross-certified CA needs to import a private key into cryptographic modules, then it has to follow its certificate policy to choose an appropriate private key importing method. Before issuing a cross certificate, GRCA examines whether the private key import method chosen by this CA is appropriate.

6.2.7 Method of Activating Private Key

GRCA RSA private key activation is controlled via m-out-of-n controlling IC cards; controlling IC cards with different usages are managed by managers and issuers separately.

A cross-certified CA has to follow the stipulations from its certificate policy to choose an appropriate private key activation method. Before issuing a cross certificate, GRCA examines whether the private key activation method chosen by this CA is appropriate.

6.2.8 Method of Deactivating Private Key

As GRCA adapts offline operating mode, normally GRCA key pairs will be at deactivation state in order to avoid any illegal use of its private key.

Once completing the certificate issuing and relative management operations, GRCA adapts m-out-of-n method to suspend its private key.

A cross-certified CA has to follow the stipulations from its certificate policies to choose an appropriate private key suspension method. Before issuing a cross certificate, GRCA

examines whether this CA has chosen an appropriate private key suspension method.

6.2.9 Method of Destroying Private Key

In order to prevent GRCA old private key from being stolen, which will influence the correctness of issued certificates, GRCA private key will be destroyed once it reached its complete life cycle. Therefore, after the completion of GRCA key renewal and new certificate issuing processes, GRCA will implement the Zeroization process in the memory in order to destroy the old private key stored in the hardware cryptographic module. At the same time, old private key splits are destroyed physically.

A cross-certified CA has to follow the stipulations from its certificate policy to choose an appropriate private key destroying method. Before issuing a cross certificate, GRCA examines whether the private key destroying method chosen by this CA is appropriate.

6.3 Other Aspects of Key Pair Management for Cross-certified CAs

Cross-certified CAs have to manage their own key pairs; GRCA is not responsible for private keys of any cross-certified CA.

6.3.1 Public Key Archival

GRCA will proceed the certificates archival, and also follow regulations from section 4.6 to perform the security control for archival systems. There is no other procedure for public key archival, as certificates archival can replace the public key archival.

6.3.2 Usage Periods for the Public and Private Keys

6.3.2.1 Usage Periods for GRCA Public Key and Private Key

RSA Key sizes for both GRCA public key and private key are 4096 bits. Public key certificates usage period is at most 30 years; private key usage period is at most 10 years.

6.3.2.2 Usage Periods for Cross-certified CA's Public Key and Private Key

(1) RSA 2048 bits: public key certificates usage periods are at most 20 years; private keys usage periods are at most 10 years.

(2) RSA 1024 bits: public key certificates usage periods are at most 10 years; private keys usage periods are at most 5 years.

The usage period of the cross certificates issued to cross-certified CAs, plus the GRCA private key (used for digital signature) usage period, cannot exceed the life usage period of GRCA self-signed certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

GRCA activation data is generated by hardware cryptographic module then stored in the m-out-of-n controlled IC cards. The activation data within the IC cards will be accessed directly by the built-in card readers in hardware cryptographic module; the IC cards person identification number (abbreviated as PIN) will be input directly from the built-in keyboard in the hardware cryptographic module.

A cross-certified CA has to follow the stipulations from its certificate policy to choose an appropriate data activation method. Before issuing a cross certificate, GRCA examines whether this data activation method chosen by this CA is appropriate.

6.4.2 Activation Data Protection

GRCA activation data is protected by the m-out-of-n control IC cards; IC card PINs are kept safe by the managers. It does not allow keeping PIN records on any media. If the number of failed login exceeds 3 times, this IC card is locked. When IC card is handed over, the new manager has to reset a new PIN.

A cross-certified CA has to follow the stipulations from its certificate policy to choose an appropriate activation data protection method. Before issuing a cross certificate, GRCA examines whether this method of activation data protection method is appropriate.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Through the operating systems, or combining operating system software and physical entity protection measures, GRCA and related auxiliary systems provide the following security control functions:

- (1) To login with authentication
- (2) To provide self-discretionary access control
- (3) To provide security audit capability
- (4) To restrict access control from certificate services and trust roles
- (5) To process trust role and trust identity authentication
- (6) To ensure the security of communication and database by adapting cryptographic technology
- (7) To process the secure and reliable channel for trust role and relative identity authentication.
- (8) To process procedure integrity and security control protection.

6.5.2 Computer Security Rating

GRCA adapts computer systems with security levels equivalent to ITSEC (Information Technology Security Evaluation Criteria) E2.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

GRCA system development follows the ISO 9001 to control the quality.

GRCA hardware and software have to be specialized and only use components with security authorization. GRCA will not install any hardware network connection and software components which are unrelated to GRCA operations. Whenever being initiated, GRCA will check if there is any malicious code.

6.6.2 Security Management Controls

When any GRCA software being installed for the first time, it will be ensured this software provider provides the correct software and the software version is not revised. After the system installation, GRCA will check the software integrity when it is initiated. On the other hand, software integrity will be performed routinely every month.

GRCA will record and control every system configuration, modification and functional update; at the same time, GRCA will detect any unauthorized modification of system software and configuration.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

Neither GRCA server nor interior repository connects to exterior network. Exterior repository connects to Internet to provide the uninterrupted certificates and ARL requesting services (unless necessary maintenance and backups).

Information stored in the GRCA interior repository (including certificates and ARLs) is

protected by the digital signature engine; it is transmitted manually from interior repository to exterior repository.

GRCA exterior repository can prevent denial of services and intrusion attacks through the updates for system patch files, system vulnerability scanning, intrusion detection system, firewall systems and Filtering Router.

6.8 Engineering Controls

Follow the stipulations from section 6.1 and 6.2.

7 Certificate and CARL Profiles

7.1 Certificate Profile

The certificate profile field of the certificate issued by GRCA shall comply with GPKI technical profile.

7.1.1 Version Numbers

The GRCA shall issue X.509 v3 certificates.

7.1.2 Certificate Extensions

The certificate extensions field of the certificate issued by GRCA shall comply with GPKI technical profile.

7.1.3 Algorithm Object Identifiers

The certificate issued by GRCA shall use the following algorithm OIDs for signatures:

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

(OID : 1.2.840.113549.1.1.5)

The certificate issued by GRCA shall use the following algorithm OIDs for identifying the algorithm for which the subject key was generated:

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

(OID:1.2.840.113549.1.1.1)

7.1.4 Name Forms

The subject and issuer fields of the certificate shall be complied with X.500 Distinguished Name and its attribute type shall be complied with RFC2459.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

The certificate policy object identifier field of the certificate shall use the OID of GPKI CP.

7.1.7 Usage of Policy Constraints Extension

The cross-certificate issued by GRCA shall use this field if it is necessary.

7.1.8 Policy Qualifiers Syntax and Semantics

The certificate issued by GRCA shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The GRCA shall not set the critical certificate policy extension field.

7.2 CARL Profile

7.2.1 Version Numbers

The GRCA shall issue X.509 v2 CARLs.

7.2.2 CARL Entry Extensions

The CARL issued by GRCA shall comply with GPKI technical profile.

8 Maintenance

8.1 Change Procedure

The need for changes to this CPS should be periodically evaluated every year to sustain its assurance. The changes can be made in an annex to the CPS or by materially rewriting the CPS. If GRCA CP or its OID has been changed, this CPS should be changed in accordance with the changed GRCA CP or its changed OID.

8.1.1 Items that can Change without Notification

Only editorial change and typographical correction may be made to this CPS without notification.

8.1.2 Changes with Notification

8.1.2.1 Change Items

- (1) Changes to items which will significantly impact the CAs, which are directly cross-certified with GRCA, and relying party using this CPS should be posted in the repository of GRCA for 30 days before the changes are made to this CPS materially.
- (2) Otherwise, they should be posted for 15 days.

8.1.2.2 Notification Mechanism

Changes to all items in this CPS should be posted in the repository of GRCA. If the items are subject to 8.1.2.1(a), a formal documented notification to the CAs that are directly cross-certified with GRCA is required.

8.1.2.3 Comment Period

- (1) If the items are subject to 8.1.2.1(1), the comment period will be 15 days once their

changes have been posted.

- (2) If the items are subject to 8.1.2.1(2), the comment period will be 7 days once their changes have been posted.

8.1.2.4 Mechanism to Handle Comments

Any comments on the proposed changes should be received in the form posted in the repository of GRCA before the deadline of comment period. All received comments will be reviewed and evaluated to decide the precise form and effective date of the changes.

8.1.2.5 Period for Final Change Notice

The changes to this CPS and their notification should be made in accordance with 8.1.2.2 and 8.1.2.3. According to 8.1.2.1, the changes should be posted at least for 15 days until the changed CPS goes into effect.

8.2 Publication and Notification Procedure

The revised CPS should be posted in the repository of GRCA within 7 days, and it will be in effect once it's posted, unless other specifications by PMA.

8.3 CPS Approval Procedures

After this CPS is approved by the authority concerned of MOEA, it should be posted by GRCA. If the CP has been revised and posted, this CPS should be revised in accordance with the revised CP, and submitted to the authority concerned of MOEA for approval.

Unless there is other stipulation, if the revised content of this CPS contradicts to the original one, it will be a standard. If the changes of the CPS is achieved by appending document, and the content of such document contradicts to the previous CPS, then this appended document will be a standard.