Government Root Certification Authority
Certification Practice Statement
Version 1.5

Administrative Organization: National Development Council

Executive Organization: ChungHwa Telecom Co., Ltd.

July, 10, 2017

Contents

Summary

In compliance with the Certification Practice Statement bylaws of the Taiwan Digital Signature Act, the following is a description of key aspects of the Government Root Certificate Authority Certification Practice Statement (GRCA CPS):

1. **Competent Authority Approval Number: Jing-shang no._____.**
2. **Certificate Issuance:**
   (1) Types: Self-signed certificates, self-issued certificates and cross-certificates issued to certification authorities by the Government Root Certificate Authority (GRCA).
   (2) Assurance level: The five types of assurance level certificates defined by the Certificate Policy in accordance with the Government Public Key Infrastructure.
   (3) Scope of use:

   The self-signed certificate is used to establish the trust anchor of the GPKI. The self-issued certificate is the certificate issued during GRCA rekey or for CP requirements and used to establish a trust pathway between old and new keys or CP interoperable certificates. Cross-certificates are used to build mutual trust relationships between CAs and trust pathways needed for the interoperability of CAs.
3. **Major Liability Matters:**
   (1) The GRCA assumes no liability for any consequences arising from use of certificates by Cross-certified CAs and Trusted Parties outside the scope of the CPS.
   (2) Regarding liability of the GRCA to the Cross-certified CA for damages arising from the issue or use of certificates, the liability of the GRCA for damages shall be limited to that set down in the GPS

and related contracts.

(3) The GRCA assumes no liability for any damages arising from a force majeure or other events non-attributable to the GRCA.

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

4. Other Important Matters:

(1) The GRCA accepts certificate registration and revocation requests so no separate Registration Authority has been established.

(2) The Certification Authority must describe the assurance level of the requested certification when submitting the cross-certification request for GRCA issued certificates based on the scope of use of difference assurance levels.

(3) Private keys must be generated, kept and used by the requesting Certification Authority themselves.

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

(5) If a Certification Authority finds it necessary to revoke certificates, the GRCA should be promptly notified and CPS procedures should be followed. However, appropriate actions should first be taken to limit the impact on Certification Authorities and Trusted Parties and assumption of all liability arising from use of the certification prior

to the posting of the Certification Authority's certificate revocation status.

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

(7) The competent e-government authorities commissions a trusted third party to conduct external compliance audits of GRCA operations in accordance with the Government Procurement Act.

1. Introduction

The Government Root Certification Authority Certification Practice Statement (GRCA CPS) is stipulated to follow the Certificate Policy (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 self-signed certificates, self-issued certificates and cross certificates of cross-certified CAs.

1.1 Overview

According to the regulations of the GPKI CP, GRCA is the highest level 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 cross-certified CAs. This CPS only applies to the entities related to the community of GRCA, such as GRCA, Cross-certified CAs and Relying Parties and repository.

The GRCA and the Subject CAs issuing SSL certificates shall comply with the official version of the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates published by the CA/Browser Forum. For the requirements and relevant date in Section 1.2.1 of the Baseline Requirements, the GRCA is in compliance (see Appendix 1).

The National Development Council (NDC) is the administrative organization of GRCA. The establishment and any modification to the GRCA CPS may go into effect only after obtaining the permission of NDC and the Ministry of Economic Affairs (MOEA). The CPA does not authorize its use by CAs outside the GRCA. The CA

shall be solely responsible for any problems arising from the use of the CPS by other CA. 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 1.5. Its date of publication is May 20, 2014. The latest version of the CPS can be obtained from http://grca.nat.gov.tw/download/GRCA_CPS_v1.5.pdf.

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 further 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 management of 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. It is not necessary to set up a Registration Authority (RA) for the GRCA. The GRCA accepts and authenticates the applications from cross-certified CAs.

1.3.2 Repository

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

1.3.3 Subject Certification Authority

The CAs including principal CAs within and any CAs without Government PKI, that interoperate with GRCA through cross-certification are referred to as cross-certified 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 public key infrastructure, digital signature and certificate issuance technology and determine the duties and obligations of CA, RA and relying parties.

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding nature of the certificate subject 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

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

1.3.6 Applicability

1.3.6.1 Usage of Issued Certificates

The GRCA issues three kinds of certificates: self-signed certificates, self-issued certificates and cross-certificates.

Self-signed certificates are used to establish the trust anchor of GPKI. Self-issued certificates are used to help with the certificate path processing for old and new keys or CP. Cross-certificates are 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 cross-certified CA. The cross-certified CA will be more than one CA. The cross-certified CAs will include the Level 1 subordinate CAs within GPKI as well as the CAs from without. The public key of the cross-certified CA is 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 Certificate Use

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. The relying parties can then use the trusted public key to verify the signature of cross-certificates and CARLs that were signed by GRCA. Relying parties should careful select a trusted information environment such as secure computer operations system and trusted application system before its use to verify the signature of cross-certificates and CARLs issued by GRCA to ensure that the GRCA's self-signed certificate or public key will not be compromised or replaced. .

The GRCA's cross-certificate will describe which assurance level of the cross-certified CA and which levels the cross-certified CA can issue cross-certificates to other CAs. Then relying parties may use this information to determine whether or not they want to trust the certificates issued by a cross-certified CA. Furthermore, in the content of the GRCA's cross-certificate that is issued to a cross-certified 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 cross-certified 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 cross-certified 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 watch for any modifications of this CPS.

1.3.6.3 Certificates Are Not Permitted to Be Used for the Following

(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 be announced for implementation only after permission is obtained from the competent authority of the Digital Signature Act MOEA.

1.4.2 Contact Information

Direct all questions regarding this CPS and situations such as reporting lost keys to the GRCA, the postal and email addresses can be found at http://grca.nat.gov.tw.

1.4.3 Person Determining Certification Practice Statement Suitability for the Policy

In compliance with the bylaws of the Taiwan Digital Signature Act, this CPS must be reviewed by competent authority of the Electronic Signature Act before offering certificate issuance services to external parties.

2. General Provisions

2.1 Obligations

2.1.1 GRCA Obligations

(1) Ensuring that its own operations meet the provisions of the Assurance Level 4 of the CP

(2) Establishing the procedures that allow CAs to apply for cross-certification

(3) Identifying and authenticating CAs when they apply for cross-certification

(4) Issuing and publishing certificates

(5) Revoking certificates as needed

(6) Issuing and publishing Certification Authority Revocation Lists (CARLs)

(7) Identifying and authenticating the CA personnel

(8) Securely generating the CA private keys

(9) Ensuring safekeeping of the GRCA private keys,

(10) Key changeover and issuance of the GRCA self-signed certificate

(11) Processing application for issuing or revoking cross-certificates from cross-certified CAs.

2.1.2 Cross-Certified CA Obligations

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

(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 cross-certified CA wishes its own cross-certificate to be issued when applying for cross-certification from the GRCA.

(3) Submitting valid information for cross-certificate applications to the GRCA in accordance with the procedure specified in Section 4.1 of this CPS.

(4) Deciding whether or not to accept 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 confirmation of the correctness of the content of the cross-certificate and use in accordance with the provisions of Section 1.3.6.

(6) Securely generating its own private keys in accordance with Section 6 of this CPS.

(7) Ensuring the safekeeping and proper usage of its own private keys.

(8) With regard to the digital signature used to sign the private key corresponding to the certificate's public key, the cross-certified CA must confirm that it accepts the certificate and check if the certificate is unrevoked and within the validity period.

(9) Immediately notify the GRCA of the reasons for certificate revocation (such as private key compromise or loss) as specified in Section 4.4.1 and request certificate revocation or suspension in accordance with Section 4.4. However, the CA is still liable before the revocation information of its own certificate is published by the GRCA.

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

2.1.3 Relying Party Obligations

(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) Obtaining the self-signed certificate of the GRCA by a reliable 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) Obtaining self-certificate from GRCA repository to establish a trust pathway between the GRCA and CA when certificate is issued after rekey.

(7) Verifying the digital signature of certificates and CARLs claimed to be issued by the GRCA.

(8) Ensuring that the relying 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.

(9) 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.

(10) 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

(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 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 Warranties and Limitations on Warranties

The GRCA warrants and promises to operate in accordance with the provisions of the Assurance Level 4 of the CP and to follow CPS regulations for the issuance and revocation of certificate, posting of CARLs and maintenance of repository operations.

The GRCA complies with the official version of the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates published by the CA/Browser Forum to issue and manage certificates.

2.2.2 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.

2.2.3 Limitations of Liability

The liability of the GRCA to the CA cross-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 cross-certified CA and the GRCA.

2.2.4 Other Exclusions

The GRCA assumes no liability for any losses arising out of or relating to a force majeure or other reason not attributable to the GRCA.

In the event that the GRCA needs to pause all or part of its certification services due to system maintenance, transit, or expansion, the GRCA will announce that event on the repository of the GRCA and notify cross-certified CAs. Trusted parties or cross-certified CAs may not use this event as a reason to request compensation from the GRCA.

In the event that a cross-certified CA or the competent authority of a CA applies for certificate revocation as set forth in Section 4.4.1 of this CPS, the GRCA shall complete the certificate revocation work within 10 working days upon receipt of the certificate revocation application, issue the CARL and post it in the repository. The cross-certified 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 cross-certified 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 NDC budgets the operating expenses the GRCA and the National Audit Office of the Control Yuan audits the budget annually. The GRCA currently has no insurance against the financial responsibility for indemnification. Other aspects of financial responsibility shall be in accordance with applicable law.

2.3.1 Indemnification by Cross-Certified 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 sections of this CPS shall remain in effect until the CPS is updated. The process for updating this CPS is described in chapter 8.

The GRCA complies with the official version of the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates published by the CA/Browser Forum. In the event of a conflict between Baseline Requirements and a law, regulation or government order (hereinafter 'Law') of Taiwan, the GRCA can modify any conflicting requirement to the minimum extent necessary

to make the requirement valid and legal. In such event, the GRCA will describe the detailed reference to the Law requiring a modification of these Requirements in this section and notify the CA/Browser Forum of the relevant information newly added to this CPS by sending a message to questions@cabforum.org.

Any modification to GRCA practice enabled under this section must be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified to make it possible to comply with both them and the Law simultaneously.

An appropriate change in practice, modification to the GRCA CPS and a notice to the CA/Browser Forum must be made within 90 days.

2.4.3 Dispute Resolution Procedures

Disputes between the GRCA and any cross-certified CA should be settled in the first instance by negotiation between the two parties. Disputes that cannot be 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 CP. In case that a lawsuit is unavoidable, the Taiwan Taipei District Court is the competent court.

2.5 Fees

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 determine the inquiry method or refund procedure for the related fees.

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) Its own self-signed certificates (until expiry of all certificates signed by the private key which correspond with the public key of the signed certificates).

(5) Its own self-issued certificates co-signed by the GRCA old and new keys (until expiry of certificates signed by the old GRCA key and all certificates signed by the private key which correspond with the public key of the signed certificates).

(6) Cross-certified CA certificates.

(7) Privacy protection policy.

(8) Software utility downloads.

(9) The latest audit report of the GRCA.

(10) 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.

2.6.3Access Control

For security purposes, the CA host of the GRCA will be always kept off-line, and therefore the certificates and CARLs issued by the GRCA may not be sent to the repository directly via computer network because there is not any direct or indirect network line between the CA host and the repository. When certificates and CARLs need to be published to the repository, authorized GRCA personnel use manual out-of-band transfer to store published certificates and CARLs onto portable media and then copy the files to the repository for publication.

The information published in the repository of the GRCA as set forth in Section 2.6.1 of this CPS is primarily provided for searches by cross-certified CAs and relying parties. Therefore, the information is open to public access. Access controls have been put in place to protect the repository security as well as maintain the accessibility and 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 restoring 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 compliance with the security practices and procedures detailed in this CPS.

2.7.2 Identity/Qualifications of Compliance Auditor

An auditing firm shall be retained that is familiar GPKI related regulations and GRCA / level 1 subordinate CA operations and conforms with Trust Service Principles and Criteria for Certification Authorities standards for the external compliance auditing of GPKI CA (including the GRCA and level 1 subordinate CA operations) outsourced in accordance with the Government Procurement Act to provide fair and objective auditing services. The GRCA shall perform ID checks of auditors during the auditing period.

2.7.3 Compliance Auditor's Relationship to Audited Party

An auditing firm shall be retained to perform audits of GRCA operations in conjunction with the external compliance auditing of GPKI CA performed by the NDC.

2.7.4 Topics Covered by Compliance Audit

(1) Operation of the GPS is in accordance with this CPS, and

(2) CPS conformance with GPKI CP.

2.7.5 Actions Taken as a Result of Deficiencies

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 note 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, revoke the cross-certificate issued by the GRCA, or take other accompanying actions.

2.7.6 Communication of Result

The results of the most recent external audit will be made public in electronic form and published in the repository of the GRCA except for information that may be used to attack GRCA systems.

2.8 Confidentiality

2.8.1 Types of Information to be Kept Confidential

Any information generated, received and kept by the GRCA which does not appear on issued certificates is considered confidential. Both present and former employees are responsible for keeping information strictly confidential. Confidential information includes:

(1) All private and secret keys used and handled during GRCA operations are to be kept confidential.

(2) Safekeeping information regarding secret shares of the GRCA private keys.

(3) 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.

(5) Audit records or discoveries generated by related personnel during audits shall not be made available as a whole, except as required by law.

(6) GRCA operational documents that are assigned confidential.

2.8.2 Types of Non-Confidential Information

(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 when stipulated otherwise.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

The GRCA does not provide certificate suspension service. Certificate revocation information shall be made available in the GRCA repository.

2.8.4 Release to Law Enforcement Officials

In the event that juridical, control or security apparatuses need access to the types of confidential information specified in Section 2.8.1 of this CPS for the purpose of investigation or evidence collection, 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, control or security apparatuses need access to confidential information specified in Section 2.8.1 of this CPS for the purpose of investigation or evidence collection, 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 cross-certified CA has the right to inquire into 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 Computer-Processed Personal Data Protection Act 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 cross-certified 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 cross-certified CAs.

The GRCA retains all intellectual property rights to the certificates and CARLs issued by the GRCA.

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

The GRCA will ensure the correctness of the names of cross-certified 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 cross-certified CAs. In the event that the registration mark dispute occurs in the name of a cross-certified CA, the cross-certified 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 NDC 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 NDC or Chunghwa Telecom Co., Ltd. be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any improper usage or distribution of this CPS.

3. Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

The subject name of the certificate issued by GRCA conforms to the Distinguished Name (DN) of X.500. Only this DN format is used for self-signed certificates and self-issue certificates of GRCA and cross-certification certificates among certification authorities.

3.1.2 Need for Names to be Meaningful

The organization names applying for cross-certification should comply with relevant naming rules in related laws and 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 GPKI, rules for interpreting various name forms should comply with the Name attribute definition of ITU-T X.520.

3.1.4 Uniqueness of Names

The GRCA Authority examines the uniqueness of the CA names applying to become subordinate CA and cross-certification CA. If a duplicate name is found then the applying certification authority is asked to change the name.

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

C=TW, O=Government Root Certification Authority

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

C=TW,

O=Executive Yuan,

CN=Government Root Certification Authority - Gn

Where n = 3.4…

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 NDC is in charge of handling name claim disputes.

3.1.6 Recognition, Authentication, and Role of Trademarks

Not applicable

3.1.7 Method to Prove Possession of Private Key

The GRCA examines whether the private key of the CA and the public key listed on the certificate work in pairs. With the PKCS#10 certification request file generated by the CA, the GRCA can use the public key used by the CA to prove that the CA owns the corresponding private key.

3.1.8 Authentication of Organization Identity

Cross-certification applications submitted by CA shall include information such as the organization name, location and representative which is adequate to identify the organization. The application information shall be combined with the documentation and sent in electronic or paper form to the NDC. After the NDC verifies the legality and adequacy, the documentation shall be passed to the GRCA for cross-certificate issuance.

If the documentation and cross-certificate application is submitted by a CA operator which is a government agency that is not a part of the ROC government, the

NDC shall verify the existence of the CA and confirm that documentation, representative identity and representative have the right to represent the organization for certification application. The representative shall appear in person for certificate application processing.

3.1.9 Authentication of Individual Identity

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

(1) Formal document check:

The representative should present his/her identification card or passport while applying for certificates in order to GRCA may authenticate the representative's identity. The ID number, name and registered permanent residence are cross-checked 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 features and guarantee 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 validity period.

The private key of GRCA itself is 4,096 bits long. The validity of self-issued certificate is limited to 10 years. The validity of public key certificates is 30 years. The GRCA will change the key and issue a new self-signed certificate under the following two circumstances:

(1) The current key has expired.

(2) The security of current key is dubious. For instance, the private key is suspect or has been compromised.

The cross-certified CA should apply for new certificates from GRCA when processing key changes. The GRCA identifies and authenticates the CA applying for cross-certification as stipulated in section 3.1.

3.2.2 Certificate Renewal

The GRCA does not permit the renewal of self-signed certificates, self-issued certificates and subordinate CA cross-certifications.

3.3 Rekey after Revocation

The identification and authentication process of the new certificate application after CA certificate revocation follows the rules described in section 3.1 when making a new initial registration.

3.4 Revocation Request

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

3.5 Certificate Suspension and Resumption

Not applicable

4. Operations Requirements

4.1 Certificate Application

1. Initiation

(1) Initiation application

The cross-certification request form together with the CPS and certification request file in PKCS#10 format shall be post mailed via formal official document. If the CA adopts a certificate policy other than GPKI-CP, then the complying certificate policy shall also be included.

(2) Identification and authentication

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

(3) Verification

- Check if there is any technical incompatibilities between the CA issuing the cross-certification and GRCA.
- If the CP followed by the requesting CA is a non-GPKI CP, the corresponding relationship between this CP and the GRCA CP should be examined.
- Check if the CPS of the CA follows the cited CP.
- Check if the PKCS#10 certificate request file submitted with the initialization request can complete the actual cross certification work.

2. Examination

Approval of government agency CA application is decided directly by the GRCA. If the application is approved, the NDC will notify the GRCA about the certificate issuance procedure.

A meeting of the GECSC shall be convened when non-governmental CA apply for cross-certification to review the related documentation and information submitted by the CA in the application and the GRCA examination results to determine the appropriateness of CA and GRCA cross-certification. The determination of the GECSC shall decide whether the application goes to the next stage, supplemental information is required or the application is rejected.

3. Arrangement

The following steps shall be followed when a meeting is convened:

(1) Identification and authentication

Prior to the commencement of the meeting, the identity of the representative of the CA applying for cross-certification shall be checked and authenticated in accordance with section 3.1.9.

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

(3) After determining whether the cross-certification application from the cross-certified CA can proceed, a Cross-Certification Agreement is signed with the cross-certified CA. No Cross-Certification Agreement needs to be signed if it is a government agency.

(4) Proceed with certificate issuance process.

4.2 Certificate Issuance

The GRCA shall determine whether or not to issue the requested certificate(s) based on the examination results

If the certificate application is approved, the GRCA shall perform the work related to certificate issuance. Once the certificate is issues, official notification and the issued certified shall be sent together to the applicant CA.

If the certificate application is rejected, the applicant CA shall be sent an official notification stating the reason why the application was rejected.

One Self-Signed Certificate issued by GRCA shall be sent to the relying party in accordance with Section 6.1.4.

4.3 Certificate Acceptance

After receiving the official notice of application approval, the applicant CA (now Subscriber) must check the content of attached certificate(s) for correctness. If the content is error-free, the Subscriber must sign the certificate acceptance and confirmation documents and return them in official document format to complete the acceptance procedure.

After receiving the acceptance and confirmation document, the GRCA shall publish the corresponding issued certificate(s) in the repository.

If the Subscriber fails to send back the signed acceptance document within 30 calendar days, it shall be deemed as refusal of acceptance. In this case, the GRCA shall revoke the corresponding certificates(s) without further announcement.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances under which a Certificate may be Revoked

The cross-certified CA must submit a certificate revocation application under (but not restricted to) the following circumstances:

(1) The corresponding private key of the Agency is suspect or known to be compromised.

(2) The certificate(s) is no longer needed, which may have been due to the termination of CA service or termination of the cross-certification between GRCA.

In addition, the GRCA may revoke certificates under the following

circumstances provided permission has been received in advance from the cross-certified CA:

(1) The information listed on the certificate is verified to be incorrect.

(2) Verified cases of unauthorized, forged or comprised private keys used for cross-certified CA signing.

(3) For verified cases of unauthorized, forged, or compromised GRCA private keys, all cross-certified CA certificates signed by GRCA shall be revoked.

(4) It is confirmed that cross-certified CA certificates were not issued in accordance to the CPS.

(5) The cross-certified CA has not acted in conformance with the CPS, Cross-Certification Agreement or applicable laws / regulations.

(6) The revocation is requested by the competent authorities of the cross-certified CA or is required by law.

(7) GRCA or cross-certified CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate.

(8) GRCA's or cross-certified CA's right to issue certificates under these statements expires or is revoked or terminated, unless the GRCA has made arrangements to continue maintaining the CRL/OCSP Repository.

(9) Revocation is required by the GRCA's Certificate Policy and/or Certification Practice Statement.

(10) The technical content or format of the certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

If the entity information on the certificate needs to be changed, the GRCA shall determine whether or not to approve certificate revocation application.

4.4.2 Who Can Request Revocation of a Certificate Issued by GRCA

(1) Cross-certified CAs which requests revocation of its cross-certificate.

(2) Competent authority or responsible agency of the cross-certified CA.

4.4.3 Procedure for Revocation

1. Initiation

(1) Initiation request

Request shall be submitted via formal official document with the revocation request form attached.

(2) Identification and authentication

Identification and authentication of the Agency carrying out the cross certification shall be done in accordance with section 3.1.8.

(3) Request review

The submitted documents shall be reviewed to determine the appropriateness of the revocation request.

(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 repository shall include revoked certificates until

its expiration date.

4.4.4 Revocation Request Grace Period

The GRCA shall begin investigation of a Certificate Problem Report within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint; and
4. Relevant legislation.

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

GRCA shall complete the related certificate revocation work no later than 7 working days following receipt of the certificate revocation request.

4.4.5 Circumstances under which a Certificate may be Suspended

No certificate suspension services are provided at this time.

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 Procedure for Resumption of Use

Not applicable

4.4.10 CARL Issuance Frequency

CARLs shall be issued once each day, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field. The updated CARL shall be published in the repository.

4.4.11 CARL Checking Requirements

Before checking CARL published in the repository, 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 repository.

4.4.12 On-line Status Checking Service

On-line Revocation / Status Checking services are not provided.

4.4.13 On-line Status Checking Requirements

Not applicable

4.4.14 Other Forms of Revocation Announcement

Other forms of revocation announcements are not provided.

4.4.15 Checking Requirements for Other Forms of Revocation Announcements

Not applicable

4.4.16 Special Requirements in the Event of 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 in a logbook, paper form, or some 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

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

(2) Identification and Authentication

- Successful and unsuccessful attempts to assume a role
- Change in the value of maximum authentication attempts
- Maximum number of unsuccessful authentication attempts during user login
- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
- The Administrator changes the type of authenticator ranging from password to biometrics

(3) Key Generation

- Whenever GRCA generates a key

(4) Private Key Load and Storage

- Loading of component private keys

(5) Trusted Public Key Entry, Deletion and Storage

- Changes to the trusted public keys, including additions, deletions and storage

(6) Private Key Export

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

(7) Certificate Registration

- Certificate registration request processes

(8) Certificate Revocation

- Certificate revocation request processes

(9) Certificate Status Change Approval

- Approval or rejection of a certificate status change request

(10) GRCA Configuration

- Security-relevant changes to the configuration of the GRCA

(11) Account Administration

- Addition and deletions of roles and users
- The access control privileges of a user account or a role are modified

(12) Certificate Profile Management

- Changes to the certificate profile

(13) CARL Profile Management

- Changes to the CARL profile

(14) Other

- Installation of the operating system
- Installation of the GRCA system
- Installation of hardware cryptographic modules
- Removal of hardware cryptographic modules
- Destruction of cryptographic modules
- System activation
- Logon attempts to GRCA Apps
- Receipt of hardware / software
- Attempts to set passwords
- Attempts to modify passwords
- Backing up the GRCA's internal database
- Restoring the GRCA's internal database
- File manipulation (e.g., creation, renaming, moving)
- Posting of any information to a repository.
- Access to the GRCA internal database
- All certificate compromise complaints
- Certificate loading symbols
- Rekey of GRCA or cross-certified CA

(15) Configuration changes to the GRCA server involving:

- Hardware
- Software
- Operation systems
- Patches
- Security profiles

(16) Physical Access/Site Security

- Personnel access to GRCA server room
- Access to GRCA servers
- Known or suspected violations of physical security regulations

(17) Abnormality

- Software errors
- Software check integrity failures
- Receipt of improper messages
- Misrouted messages
- Network attacks (suspected or confirmed)
- Equipment failure
- Insufficient power supply
- Uninterruptible power supply (UPS) failure
- Obvious and significant network service or access failures
- Violations of Certificate Policy
- Violations of Certification Practice Statement
- Resetting operating system clock

4.5.2 Frequency of Record File Processing

GRCA shall review audit logs once a month to keep track all significant events. 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 for two months as well as being retained in accordance with sections 4.5.4, 4.5.5, 4.5.6 and 4.6 in the log retention management

system rules.

Audit personnel are responsible for the removal of the expired audit logs. Other personnel may not perform this work.

4.5.4 Protection of Security Audit Logs

(1) Current and archived audit logs 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. The audit system may not reveal private keys.

(3) Manual audit logs shall be moved to a safe, secure storage location.

4.5.5 Audit Log Backup Procedures

Electronic audit logs shall be backed up once per month.

(1) GRCA shall periodically back up the event logs: The audit system shall automatically archive the audit trail data on a daily, weekly and monthly basis.

(2) GRCA shall store event logs in a safe location.

4.5.6 Security Audit System

An audit system is built in the GRCA system. Audit processes shall be activated upon GRCA system startup and end only at GRCA system shutdown.

If the audit system is not operating normally and the integrity of the system or confidentiality of the information protected by the system is at risk, the GRCA shall temporarily stop issuing certificates until the problem is remedied.

4.5.7 Notification to Event-Causing Subject

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

that caused the recorded event.

4.5.8 Vulnerability Assessments

(1) Vulnerability assessment of the operation systems.

(2) Vulnerability assessment of the physical facilities.

(3) Vulnerability assessment of the certification authority systems.

(4) Vulnerability assessment of the network

4.6 Records Archival

4.6.1 Types of Events Archived

(1) GRCA accreditation information (assumed use)

(2) Certification Practice Statement

(3) Cross-certification agreement

(4) System and equipment configuration

(5) Modifications and updates to systems or configurations

(6) Certificate requests

(7) Revocation requests

(8) Receipt of certification verification documents

(9) Issued or published certificates

(10) GRCA re-key record

(11) All issued and/or published CARLs.

(12) All audit logs

(13) Other explanatory data or applications used to verify or substantiate archive contents

(14) Documentation requested by compliance auditors

(15) Organization and individual identification data as per sections 3.1.8 and 3.1.9

4.6.2 Retention Period for Archive

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

Written documents shall be destroyed in a safe manner at the end of the archive retention period. Electronic data files shall be backed up in other storage media and suitable protection provided or be destroyed in a safe manner.

4.6.3 Protection of Archive

(1) Amendment, revision or deletion of the archives is not permitted.

(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 the archive data shall be stored in off-site backup center, currently located in Taichung. (Refer to section 5.1.8)

4.6.5 Requirements for Time-Stamping of Records

Electronic archive data (such as certificates, CARLs and audit data) including date and time related data shall be protected by proper digital signatures so that the date and time information on the inspection logs can be verified. However the date and time information in the electronic archive data are not electronic time-stamps provided by trusted third-party. Rather, it is the date and time from the computer operation system. The date and time information of all the computers of GRCA is regularly calibrated to ensure the precision and reliability.

The paper archive documentation shall be dated, and even time-stamped if necessary. The time and date on the paper documentation may not be changed unless

the change is acknowledged and signed by the auditors.

4.6.6 Archive Collection System

GRCA does not have an archive collection system

4.6.7 Procedures to Obtain and Verify Archive Information

Archive information may be obtained after formal written authorization is received.

Auditors are responsible for archive information verification. For paper documentation, date and signature authenticity is verified and digital signature is verified for electronic archive information.

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 and two self-issued certificates shall be issued at the same time. New self-signed certificate shall be transmitted to the relying parties in accordance with section 6.1.4.

Cross-certified CAs shall change their signing keys no later than 2 months prior to the expiration date of their certificates. After the key changeover for is made, cross-certified CAs may submit a request for new certificates from GRCA in accordance with section 4.1.

4.8 Compromise and Disaster Recovery

4.8.1 Incident and Compromise Handling Procedures

GRCA shall according to which type of Incident and Compromise to do the recovery procedures. Backup copies of essential data are made routinely.

4.8.2 Restoration Procedure for Damaged or Corrupted Computing Resources, Software or Data

GRCA shall define the recovery procedures that are used in the event that GRCA computing resources, software, and/or date are corrupted. Recovery drills are held each year.

In the event that GRCA computer equipment is damaged or rendered inoperative, but GRCA signature keys are not destroyed, priority shall be given to restoring GRCA repository operations and the reestablishment of certificate issuance and management capabilities.

4.8.3 Restoration of Revoked GRCA Signature Keys

GRCA shall set up recovery procedures for use in the event that the GRCA signature keys are revoked. Recovery drills are held each year.

4.8.4 Restoration of Compromised GRCA Signature Keys

GRCA shall set up recovery procedures for use in the event that GRCA signature keys are compromised. Recovery drills are held each year.

4.8.5 Recovery of GRCA Security Facilities Following a Disaster

Disaster recovery drills for security facilities are held by GRCA every year.

4.9 Termination of GRCA Services

In the event of termination of the GRCA operation, the related provisions of the Electronic Signatures Act shall apply.

In order to minimize the impact on cross-certified CAs and subscribers in the event of termination, the GRCA shall:

(1) Notify cross-certified CAs (does not apply if notification is not possible) and publish the announcement in the repository three months before the

scheduled service termination date.

(2) Revoke any unrevoked or unexpired certificates upon service termination, and retain and consign archives in accordance with the Electronic Signatures Act.

5. Non-Technical Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The GRCA facility, located at the Chunghwa Telecom Data Communication Branch, complies with facility standards for the housing of high value, sensitive information. Equipped with other physical security protection systems including access control, security guards, video monitoring and intrusion sensors, the facility offers robust protection against unauthorized access to related GRCA equipment.

5.1.2 Physical Access

Physical access control of the GRCA meets assurance level 4 defined in the GPKI CP. There are four access control levels in the GRCA facility housing. On the first and second levels, there is year-round entrance and building security in place. On the third level, access is controlled to this floor using a card access control system. On the forth level, a fingerprint recognition control system is used to control facility personnel access. The fingerprint scanner uses 3D sampling technology which is capable of detecting whether the fingerprint is from a live object by fingerprint depth and color.

The physical access control system of the GRCA is able to protect the facilities from unauthorized access. There is also a monitoring system in place to control cabinet access which prevents unauthorized access to any hardware, software, or hardware secure module in the GRCA.

Portable storage devices that are brought into the facility housing are checked for computers viruses or other types of software that could damage the GRCA system.

Non-GRCA personnel who need to enter the facility need to sign the entry log and be accompanied by GRCA personnel.

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

(1) Check operation of the system equipment

(2) Check that the computer rack is locked.

(3) Check that the security access system is working

5.1.3 Electrical Power and Air Conditioning

In addition to municipal power, the power system at the GRCA facility is equipped with a generator (with enough fuel for six days of continuous operation) and an uninterrupted power system (UPS). The system is capable of automatically switching between the municipal power and backup power systems and at least six hours of power can be supplied for repository backup work.

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

5.1.4 Flood Prevention and Protection

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

Audit records, archives, and backups is kept in storage media for one year at the

GRCA facility. After one year, the data shall be moved off-site for storage at a separate location.

5.1.7 Waste Disposal

When sensitive information and documents of the GRCA as described in section 2.8.1 are no longer in use, all paper, magnetic tapes, hard disks, floppy disks, magneto-optical disks and other forms of memory shall be destroyed in accordance with the standard procedures announced by government authorities.

5.1.8 Off-site Backup

The off-site backup location is in Taichung, 30 km away from the GRCA facility. One backup of all information including system programs and data shall be made at least once per week. Backups of modified data shall be done on the same day of the modification. The backup site has equivalent security controls to the GRCA.

5.2 Procedural Controls

In order to protect the security of system procedures, the GRCA uses procedural controls to specify the trusted roles of related system tasks, the number of persons required for each task, and how each role is identified and authenticated.

5.2.1 Trusted Roles

In order to properly distinguish the duties of each system task and to prevent undetected malicious use of the system, the trusted role authorized to perform each system access item is clearly defined.

The five trusted roles at the GRCA are administrator, officer, auditor, operator, and controller. Each trusted role is administrated according to section 5.3 to prevent possible internal intrusion. Each trusted role may be performed by multiple persons but one person shall be assigned the chief role. The work performed by each role is as follows.

(1) The administrator is responsible for:

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

(2) The officer is responsible for:

- Certificate issuance.
- Certificate revocation.

(3) The auditor is responsible for:

- Checking, maintenance and archiving of audit records.
- Perform or supervise internal audits to ensure the GRCA is operating in accordance with CPS regulations.

(4) The operator is responsible for:

- Daily operation and maintenance of system equipment.
- System backup and recovery.
- Storage media updating.
- Hardware and software updates outside of the GRCA system.
- Network and web server maintenance: Set up system for security, virus protection system and network security event detection and reporting.

(5) The controller is responsible for:

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

5.2.2 Roles Assignments

The five trusted roles defined in section 5.2.1 must follow the rules below:

(1) A person may only assume one of the Administrator, Officer, and Auditor roles, but the person may also assume the Operator role.

(2) The Controller may not concurrently assume any of the other four roles.

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

5.2.3 Number of Persons Required Per Task

In accordance with security requirements, the number of people assigned to serve in each trusted role is as follows:

(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 people assigned to perform each task is as follows:

Assignments	Administrator	Officer	Auditor	Operator	Controller
Installation, configuration, and maintenance of the GRCA certificate management system	2				1
Establishment and maintenance of GRCA certificate management system user accounts	2				1
Configuring audit parameters	2				1
Generation and backup of GRCA keys	2		1		1
Issuing certificates		2			1
Revoking certificates		2			1
Publishing CARL in repository	1				1
Review, maintenance and archiving of audit logs			1		1
Daily routine operation				1	1
System backup and recovery				1	1
Updating storage media				1	1
Software and hardware updates outside of GRCA				1	1

Assignments	Administrator	Officer	Auditor	Operator	Controller
system					
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, password and group management functions and IC cards to identify and authenticate administrator, office, auditor, operator, and controller roles as well as central access control system authorization setting function to identify and authenticate physical security controllers.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

(1) Personnel selection and security clearance items

- Personality
- Experience
- Academic and professional qualifications
- Verification of personal identification
- Trustworthiness

(2) Management of personnel evaluation

All GRCA personnel shall have their qualifications checked before employment to verify their qualifications and work abilities. After formal employment, personnel shall receive appropriate training and sign a document accepting responsibility to perform certain duties. All personnel shall have their qualifications rechecked each year. If personnel do not pass the qualification check, a qualified individual shall be

assigned to serve in this position.

(3) Appointment, dismissal and transfer

If there are changes to the employment, temporary worker hiring conditions especially personnel severance or termination of temporary worker contracts, personnel are still required to uphold their duty of confidentiality.

(4) Duty of confidentiality agreement

All GRCA personnel shall sign an agreement to fulfill the duty of confidentiality and sign a non-disclosure agreement stating that confidential information may not be disclosed orally, by photocopy, by loan, by delivery, article or other methods.

5.3.2 Background Check Procedures

The GRCA shall check the related documents that verify the identity and certify the qualifications of the personnel performing the trusted roles defined in Section 5.2.1 prior to employment.

5.3.3 Training Requirements

Trusted Roles	Training Requirements
Administrator	1. GRCA security clearance system. 2. Installation, configuration, and maintenance of the GRCA operation procedures. 3. Establishment and maintenance cross-certified CA account operation procedures. 4. Set up audit parameter configuration operation procedures. 5. GRCA key generation and backup operation procedures. 6. Disaster recovery and continuous operation procedure.
Officer	1. GRCA security clearance system. 2. GRCA software and hardware use and operation procedures 3. Certification issuance operation procedure. 4. Certification revocation operation procedure. 5. Disaster recovery and continuous operation procedure.
Auditor	1. GRCA security clearance system. 2. GRCA software and hardware use and operation procedures 3. GRCA key generation and backup operation procedures. 4. Audit log check, upkeep and archiving procedures. 5. Disaster recovery and continuous operation procedure.

Operator	1. GRCA security clearance system. 2. Daily operation and maintenance procedures for system equipment. 3. Upgrading of storage media procedure. 4. Disaster recovery and continuous operation procedure. 5. Network and web service maintenance procedure.
Controller	1. Physical access authorization setting procedure. 2. Disaster recovery and continuous operation procedure.

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

(1) A full year of service at the original position is needed before an administrator can be reassigned to the position of operator or auditor.

(2) A full year of service at the original position is needed before an officer can be reassigned to the position of administrator or an auditor.

(3) A full year of service at the original position is needed before an auditor can be can be reassigned to the position of administrator or an officer.

(4) Only personnel with a full two years of experience as an operator as well as the requisite training and clearance may be reassigned to the position of operator, administrator, or 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. In the event of serious cases that resulted in damages, appropriate legal action shall be taken.

5.3.7 Contract Personnel Requirements

Contract personnel hired by the GRCA must possess sufficient knowledge and skills, follow the code of conduct and perform work in accordance with the CPS.

5.3.8 Documentation Supplied to Personnel

The GRCA shall make available to related personnel relevant documentation pertaining to the GPKI CP, the CPS, system operation manuals and the Electronic Signature Act.

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 by means of a random number generator mechanism which complies with the requirements of FIPS140. Once generated, the private keys from hardware security module are all stored within the module and not output except for key backup recovery and security module replacement.

GRCA key generation is witnessed by those related personnel who also sign the (GRCA) Public Key Initiation Witness document (public key corresponding to the generated key is listed too). This public key is distributed via the trusted channels.

Cross-certified CAs must generate key pairs in accordance with CP regulations.

When issuing certificates to Cross-certified CAs, the 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 CAs cross-certified with GRCA has to generate the private key on its own. Therefore, GRCA does not need to send private keys to the cross-certified CAs.

6.1.3 Public Key Delivery to GRCA

Cross-certified CAs shall hand in a PKCS#10 certificate request when submitting a request with GRCA.

6.1.4 GRCA Public Key Delivery to Relying Parties

GRCA self-signed certificates contain its public key. There are several secure distribution channels.

(1) After approval of the issue of a cross certificate to a CA, the GRCA shall 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). This CA distributes this token securely to the CA users or a relying party.

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

(3) For large issues of CD-ROMs with GRCA self-signed public key certificates, users who have obtained these CD-ROMs via secure channels will also receive the self-signed certificate from the GRCA.

(4) During GRCA activation, a public key shall be announced concurrently and related personnel shall sign GRCA public key witness document and pass it to the media for announcement. Relying parties 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 uses 4096-bit RSA keys and SHA-2 hash function to issue certificates.

Cross-certified CAs have to follow CP regulations when selecting a proper key size. The GRCA will check if the CA has selected the proper key size before issuing the cross certificate.

6.1.6 Public Key Parameters Generation

The public key parameter of the RSA algorithm is Null.

6.1.7 Key Parameter Quality Checking

The GRCA adapts ANSI X9.31 algorithm or the FIPS 186-3 standard to generate the prime numbers used in the RSA algorithms. This method can guarantee

that the generated prime numbers are strong prime.

Cross-certified CAs have to perform quality checking of key parameters using the algorithm it has selected.

6.1.8 Key Generation by Hardware/Software

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

Cross-certified CAs has to follow CP regulations to select the appropriate software and/or hardware to generate keys. Before issuing a cross certificate, GRCA will check whether the CA has selected suitable software and hardware.

6.1.9 Key Usage Purposes

The private key corresponding to the GRCA self-signed certificate can only be used for issuing certificates and CARLs. Self-signed certificate newly issued from this version does not contain the KeyUsage extension field.

The certificates issued by the GRCA to cross-certified CAs have set two key usage bits: keyCertSign and cRLSign in the extension fields.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

According to CP regulations, the GRCA uses hardware secure modules with an FIPS140-2 assurance level 3 to generate random numbers and key pairs.

Cross-certified CAs need to follow CP regulations when selecting appropriate cryptographic module. Before issuing a cross certificate, GRCA will check whether the CA has selected a cryptographic module that has the right security level.

6.2.2 Private Key Splitting 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 backup and recovery. Adapting such method can guarantee the highest assurance level for GRCA private key multi-person control; therefore it can be used as a private key activation method (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, the multi-person control procedure must be followed in accordance with CP regulations. Before the cross certificate is issued, the GRCA checks whether the multi-person procedure used by CA is appropriate.

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 by cross-certified CAs.

6.2.4 Private Key Backup

According to section 6.2.2, GRCA adopts key splitting multi-person control method to back up the private key. Highly secure IC cards are used as storage media for secret sharing.

Cross-certified CAs must follow CP regulations when selecting an appropriate private key backup method. Before the cross certificate is issued, GRCA must check whether the private key backup method selected by this CA is appropriate.

GRCA is not responsible for the safekeeping of private key backups for cross-certified CAs.

6.2.5 Private Key Archiving

RCA private keys used for digital signatures cannot be archived. The GRCA does not archive the private keys used for digital signature on the behalf of Cross-certified CAs.

6.2.6 Private Key Importation into Cryptographic Module

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

Cross-certified CAs must follow CP regulations when selecting an appropriate private key importation method for importing private keys into the cryptographic module. Before the cross certificate is issued, GRCA must check whether the private key importation method selected by this CA is appropriate.

6.2.7 Methods for Activating Private Keys

GRCA RSA private key activation is controlled via m-out-of-n control IC cards. Control IC card sets with different usages are managed by managers and officers.

Cross-certified CAs must follow CP regulations when selecting an appropriate private key activation method. Before the cross certificate is issued, GRCA checks whether the private key activation method selected by the CA is appropriate.

6.2.8 Methods for Deactivating Private Keys

As GRCA adopts offline operation mode, normal GRCA key pairs are kept in a deactivated state in prevent illegal use of private keys.

Each time certificate issuance and related management work is completed, GRCA deactivates the private key using the m-out-of-n method.

Cross-certified CAs must follow CP regulations when selecting an appropriate when selecting an appropriate key deactivation method. Before the cross certificate is issued, GRCA checks whether the private key deactivation method selected by the CA

is appropriate.

6.2.9 Methods for Destroying Private Keys

In order to prevent the theft of old GRCA private keys which could compromise the authenticity of certificates, GRCA private key must be destroyed once it expires. When the GRCA completes the key renewal and obtains the new GRCA certificate, the GRCA shall implement stored in the cryptographic module to make sure the old private key stored in the hardware cryptographic module is destroyed. At the same time, old private key splits are destroyed physically.

Cross-certified CAs must follow CP regulations when selecting an appropriate when selecting an appropriate private key destruction method. Before the cross certificate is issued, the GRCA checks whether the private key destruction method selected by the CA is appropriate.

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

Cross-certified CAs are responsible for the management of their own key pairs. The GRCA is not responsible for the private keys of any Cross-certified CAs.

6.3.1 Public Key Archival

The GRCA shall archive the certificates and also follow the archiving system security controls in section 4.6. No further public key archiving is done because certificate archiving can substitute for public key archiving.

6.3.2 Usage Periods for the Public and Private Keys

6.3.2.1 Usage Periods for GRCA Public Keys and Private Keys

The RSA key sizes for GRCA public and private keys are 4096 bits. The usage period for public keys is limited to 30 years and private key usage period is limited to 10 years.

6.3.2.2 Usage Periods for Cross-certified CA Public and Private Keys

RSA 2048 bits: The usage periods for public key certificates and private keys is limited to 20 years but the usage periods for private keys used to issue certificates is limited to 10 years.

The usage period of the 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 personal identification number (abbreviated as PIN) of the IC card is input directly using the keyboard built into the hardware cryptographic module.

Cross-certified CAs must follow CP regulations when selecting an appropriate data activation method. Before issuing a cross certificate, the GRCA checks whether this data activation method chosen by the CA is appropriate.

6.4.2 Data Activation Protection

GRCA activation data is protected by the m-out-of-n control IC cards; IC card PINs are kept by the custodians and may not be stored in any media. If there are more than three failed logins, the IC card is locked. The new custodian must create a new PINs after IC card handover.

Cross-certified CAs must follow CP regulations when selecting an appropriate data activation protection method. Before the cross certificate is issued, the GRCA checks whether this data activation data protection method is appropriate.

6.4.3 Other Data Activation Rules

Not stipulated

6.5 Computer Hardware and Software Security Controls

6.5.1 Specific Technical Requirements for Computer Security

The GRCA and related auxiliary systems provides the following security control functions by means of the operating system, or jointly through the operating system, software and physical protection measures for ID login authentication. The security control functions are as follows:

(1) Self-discretionary access control

(2) Security audit capability

(3) Control restrictions to certificate services and trust roles access

(4) Identify and authenticate trusted role and identities.

(5) Ensure security of communication and databases through encryption technology

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

(7) Offer procedure integrity and security control protections.

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

GRCA system development follows the quality control standards of competent authorities in order to control quality. These standards are posted in the GRCA website repository.

GRCA hardware and software was designed for dedicated use and may only utilize components with relevant security authorization. No unrelated devices, network connection and software components are installed or operated in conjunction with GRCA hardware and software. The GRCA checks for malicious code during each use.

6.6.2 Security Management Controls

The first time any GRCA is installed, a check is made to determine if the correct unmodified version has been provided by the vendor. After installation, the GRCA checks the software integrity during initial use and then conducts routine software integrity checks each month.

GRCA records and controls system configurations, modifications and function upgrade while also testing for unauthorized modifications of system software and configurations.

6.6.3 Life Cycle Security Ratings

At least one key compromise risk evaluation shall be conducted each year

6.7 Network Security Controls

GRCA servers and its internal repository are not connected to exterior networks. The external repository is connected to the Internet to permit uninterrupted provision of certificates and CARL search services (unless necessary maintenance and backups).

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

The GRCA external repository prevents denial of services and intrusion attacks with system patch file updates, system vulnerability scanning, intrusion detection

system, firewall systems and filtering routers.

6.8 Cryptographic Module Security Controls

Follow the provisions in sections 6.1 and 6.2.

7. Profile

7.1 Certificate Profile

The profile of GRCA issued certificates shall comply with related GPKI technical specifications.

7.1.1 Version Number

The GRCA issues X.509 v3 certificates.

7.1.2 Certificate Extension Fields

The certificate extensions field of GRCA issued certificates shall comply with GPKI technical specification regulations.

7.1.3 Algorithm Object Identifiers

Any of the following algorithm OIDs may be used for signatures used on GRCA issued certificates:

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

(OID：1.2.840.113549.1.1.11)

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

(OID：1.2.840.113549.1.1.12)

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

(OID：1.2.840.113549.1.1.13)

The following OIDs must be used with the subject key algorithm for GRCA issued certificates.

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 comply with X.500 Distinguished Name and its attribute type shall comply with RFC5280.

7.1.5 Name Constraints

Name constraints are not used.

7.1.6 Certificate Policy Object Identifier

GRCA self-sign certificate SHOULD NOT contain the certificatePolicies extension. The certificate policy object identifier field of the Self-Issued Certificate and Subordinate CA Certificate issued by GRCA will use the OIDs defined in the GPKI CP. Additionally, the Self-Issued Certificate and Subordinate CA Certificate issued by GRCA will also use the OID “2.23.140.1.2.2” defined by the CA/Browser Forum.

7.1.7 Use of Policy Constraints Extension

Cross-certificate issued by GRCA may use policy constraint expansion fields when necessary.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by GRCA shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

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

7.2 CARL Profile

7.2.1 Version Numbers

GRCA issues X.509 v2 CARLs.

7.2.2 CARL Entry Extensions

GRCA issued CARLs shall comply with GPKI technical specification regulations.

8. CPS Maintenance

8.1 Change Procedure

A periodic evaluation of the CPS shall be conducted each year to determine if any changes are required to maintain assurance. Revisions can be made to the CPS by document attachment or direct revision of the CPS content. If there are revisions made to the CP or changes to the OID, accompanying revisions should be made to CPS.

In addition, GRCA will annually review the official version of the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates published by the CA/Browser Forum (http://www.cabforum.org) and evaluate whether the CPS needs to be revised. In the event of contradiction between the CPS and the forum, provisions announced by the CA/Browser Forum shall take precedence and the GRCA shall update the CPS that describes in detail how the GRCA implements the latest version of Baseline Requirements.

8.1.1 Changes Allowed without Notification

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

8.1.2 Changes Requiring Notification

8.1.2.1 Change Items

Evaluation of the level of impact of the change on Cross-certified CAs and Trusted Parties:

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

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

8.1.2.2 Notification Mechanism

Changes to all items in this CPS shall be posted in the GRCA repository. If the

items are subject to 8.1.2.1(a), formal documented notification will be made to the Cross-certified CAs.

8.1.2.3 Comment Period

The comment period for changes are:

(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 Comment Response Mechanism

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. The changes should be posted for at least 15 calendar days in accordance with 8.1.2.1 until the CPS change goes into effect.

8.2 Publication and Notification Procedure

The revised CPS is posted within 7 calendar days to the GRCA repository and shall take effect on the date of announcement unless specified otherwise.

8.3 CPS Review Procedures

The CPS is announced by the GRCA once it is approved by the competent MOEA authorities of the Electronic Signature Act. CPS shall be revised to reflect any posted revisions of the CP and the revised CPS shall then be submitted to the competent MOEA authorities of the Electronic Signature Act for approval.

Unless stipulated otherwise, the revised CPS shall take precedence in the event of any conflicts between the content of the revised CPS and original CPS. If the revisions to the CPS are in the form of attached document, the content of the attached documents shall take precedence in the event of any conflicts between the content of the attached document and original CPS.

Appendix.1 BRs-Section 1.2.1 Revisions

Ver.	Ballot	Description	Adopted	Effective*	Implementation
1.0.0	62	Version 1.0 of the Baseline Requirements Adopted	22-Nov-11	01-Jul-12	—
1.0.1	71	Revised Auditor Qualifications	08-May-12	01-Jan-13	Compliant
1.0.2	75	Non-critical Name Constraints allowed as exception to RFC 5280	08-Jun-12	08-Jun-12	Compliant
1.0.3	78	Revised Domain/IP Address Validation, High Risk Requests, and Data Sources	22-Jun-12	22-Jun-12	Compliant
1.0.4	80	OCSP responses for non-issued certificates	02-Aug-12	01-Feb-13 01-Aug-13	Completed
--	83	Network and Certificate System Security Requirements adopted	03-Aug-13	01-Jan-13	Compliant
1.0.5	88	User-assigned country code of XX allowed	12-Sep-12	12-Sep-12	Compliant
1.1.0	--	Published as Version 1.1 with no changes from 1.0.5	14-Sep-12	14-Sep-12	—
1.1.1	93	Reasons for Revocation and Public Key Parameter checking	07-Nov-12	07-Nov-12	Compliant
1.1.2	96	Wildcard certificates and new gTLDs	20-Feb-13	20-Feb-13 01-Sep-13	Compliant
1.1.3	97	Prevention of Unknown Certificate Contents	21-Feb-13	21-Feb-13	Compliant
1.1.4	99	Add DSA Keys (BR v.1.1.4)	3-May-2013	3-May-2013	Compliant
1.1.5	102	Revision to subject domainComponent language in section 9.2.3	31-May-2013	31-May-2013	Compliant
1.1.6	105	Technical Constraints for Subordinate Certificate Authorities	29-July-2013	29-July-2013	Compliant
1.1.7	112	Replace Definition of “Internal Server Name” with “Internal Name”	3-April-2014	3-April-2014	Compliant
1.1.8	120	Affiliate Authority to Verify Domain	5-June-2014	5-June-2014	Compliant
1.1.9	129	Clarification of PSL mentioned in Section 11.1.3	4-Aug-2014	4-Aug-2014	Compliant
1.2.0	125	CAA Records	14-Oct-2014	15-Apr-2015	Compliant
1.2.1	118	SHA-1 Sunset	16-Oct-2014	16-Jan-2015 1-Jan-2016 1-Jan-2017	Compliant

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

* Effective Date and Additionally Relevant Compliance Date(s)