RISA

Rwanda Information Society Authority

Rwanda National Public Key Infrastructure

Certification Practice Statement

Version 1.0

October 2018

Document Title : Certification Practice Statement

Document type : Policy

Author : Government Certification Authority

Issue/Version No : 1.0

OID : 2 16 646 200001 3 1 1 3 2

Issue Date : October 2018

CPS Revision Control:

Date	Issue No.	Details of Changes

Notice

The services provided by GovCA shall, at any time, be in accordance with the applicable laws and regulations in Rwanda and shall be subject to the jurisdiction of courts in Rwanda, including but not limited to the ICT Law N°24/2016 OF 18/06/2016 governing information and communication technologies (Official Gazette n°26 of 27/06/2016) which is a revision of law nº18/2010 of 12/05/2010 relating to electronic message, electronic signature and electronic transaction.

Any person who uses the Digital certificate issued by GovCA in an improper manner or violate the provisions detailed under this GovCA Certification Policy shall render himself/herself liable for criminal action and be proceeded against as per the provisions of applicable criminal laws or any other relevant law that is relevant.

Definitions and acronyms

Definitions

Access Control: Process of granting access to information system resources only to authorized users, programs, processes, or other systems.

Accreditation: Formal declaration by a designated approving authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Applicant: The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.

Archive: Long-term, physically separate storage.

Audit: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Authenticate: To confirm the identity of an entity when that identity is presented.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Backup: Copy of files and programs made to facilitate recovery if necessary.

Binding: Process of associating two related elements of information.

Certificate: A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. As used in this CPS, the term certificate‖ refers to X.509 certificates that expressly reference the OID of this CPS in the certificate Policies extension.

Certification Authority (CA): An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.

CA Facility: The collection of equipment, personnel, procedures and structures that are used by a certification authority to perform certificate issuance and revocation.

Certification Authority Software/solution: Key management and cryptographic software used to manage certificates issued to subscribers.

Certificate Policy (CPS): A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practice Statement (CPS): A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CPS, or requirements specified in a contract for services).

Certificate-Related Information: Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.

Certificate Revocation List: A list maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date.

Client (application): A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.

Common Criteria: A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Compromise: Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Cross-Certificate: A certificate used to establish a trust relationship between two certification authorities.

Hardware Security Module: The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Data Integrity: Assurance that the data are unchanged from creation to reception.

Digital Signature: The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made..

Integrity: Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Intellectual Property: Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Key Escrow: A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.

Key Exchange: The process of exchanging public keys in order to establish secure communications.

Key Generation Material: Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

Key Pair: Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (2) even knowing the public key, it is computationally infeasible to discover the private key.

Non-Repudiation: Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.

Object Identifier (OID): A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.

Physically Isolated Network: A network that is not connected to entities or systems outside a physically controlled space.

Public Key: The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital certificate.

Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA): An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate): To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.

Relying Party: A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Renew (a certificate): The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository: A database containing information and data relating to certificates as specified in this CPS; may also be referred to as a directory.

Revoke a Certificate: To prematurely end the operational period of a certificate effective at a specific date and time.

Risk: An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Root CA: In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Server: A system entity that provides a service in response to requests from clients.

Signature Certificate: A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subscriber: A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device.

Trust List: Collection of Trusted Certificates used by relying parties to authenticate other certificates.

Acronyms and abbreviations

CA: Certification Authority

CP: Certificate Policy

CPS: Certification Practice Statement

CRL: Certificate Revocation List

CSP: Certification Service Provider

DN: Distinguished Name

HTTP: Hypertext Transfer Protocol

IETF: Internet Engineering Task Force

IETF: Internet Engineering Task Force

ISO: International Organization for Standardization

ISO: International Organization for Standardization

ITU: International Telecommunications Union

LDAP: Lightweight Directory Access Protocol

OCSP: Online Certificate Status Protocol

OID: Object Identifier

PKI: Public Key Infrastructure

PKIX: Public Key Infrastructure X.509 Working Group

RA: Registration Authority

ROOT CA: Root Certification Service Provider

RFC: Request for Comment

RRCSP : Rwanda Root Certification Service Provider

RSA: Rivest-Shamir-Adleman (encryption algorithm)

SHA: Secure Hash Algorithm

URL: Uniform Resource Locator

GovCA: Government Certification Authority

RISA: Rwanda Information Society Authority

Contents

1 INTRODUCTION

Government of Rwanda established the National Public Key Infrastructure (PKI) to enable a secure and safe online environment by using digital certificates. The PKI will guarantee confidentiality, integrity, authentication and non-repudiation in electronic transaction and communication. The accredited certification service provider shall be named as Government Certification Authority (GovCA).

1.1 Overview

This Certificate Policy statement (hereafter referred as CPS) applies to general purpose certificate, which can be used for all government and private transactions, as well as to specific purpose certificate, which can only be used for a specific transaction, issued by GovCA.

CPS is a statement of the practices which a certification authority employs in issuing certificates. It establishes practices concerning certificate lifecycle services in addition to issuance, such as certificate management (including publication and archiving), revocation, and renewal or re-keying.

This CPS is consistent with Request for Comments 3647 (RFC3647) and 7382 (RFC7382) of the Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement.

The Certificate Policy describes what needs to be done and the policies around this. The Certification Practice Statement (CPS) describes the manner in which the policy statements need to be executed. The Certification Practice Statement usually contains confidential information regarding procedures and policies that need to be executed.

1.2 Document name and identification

Document Title: Certification Practice Statement
Author: Government Certification Authority (GovCA)
Document Version: Version 1.0
Document Date: August 2018
OID: 2 16 646 200001 3 1 1 3 2

1.3 PKI participants

1.3.1 Certification authorities

1.3.1.1 Rwanda Root Certification Service Provider (Root CA)

The Rwanda Root Certification Service Provider is the primary trust point for the entire PKI architecture. Rwanda Utilities Regulatory Authority (RURA) is designated to operate a hierarchy of Rwanda Root Certification Service Provider (RROOTCA).

1.3.1.2 Government Certification Authority (GovCA)

GovCA is the accredited certification Authority and has the following obligations:

1. Operate and manage the CA system and its functions in accordance to CA policies, RROOT CA -CPS and all applicable regulations;
2. Issue and manage certificates to individual or legal person, used for general or specific purpose;
3. Publish issued certificates and revocation information;
4. Handle revocation request regarding certificate issued by the CSP; and
5. Notification of issuance, revocation, suspension or renewal of its certificates.

1.3.1.3 Registration authorities

GovCA may designate specific RAs to perform subscriber identification, authentication, certificate request and revocation functions defined in the CPS and related documents.

The RA is obliged to perform certain functions pursuant to an RA agreement including the following:

1. Identify the user (face-to-face) and register the user information;
2. Transmit the certificate request to the CSP;
3. Validate certificates from the CSP directory server and CRL; and
4. Request revocation and suspension and restoration of certificates.
5. Assist on other troubleshooting related to certificate management.

1.3.2 Subscribers

A subscriber is an individual or legal person whose name appears as the subject name field in a certificate. The subscriber asserts that he or she uses the keys and certificate in accordance with the certificate policy, including the following:

1. Accuracy of representations in certificate application;
2. Protection of the entity's private key;
3. Restrictions on private key and certificate use; and
4. Notification upon private key compromise or suspect of compromise.

1.3.3 **Relying parties**

A relying party is the entity that relies on the validity of the binding of the subscriber's name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A relying party may use the information in the certificate to determine the suitability of the certificate for a particular use, including the following:

1. Purpose for which a certificate is used;
2. Digital signature verification responsibilities;
3. Revocation and suspension checking responsibilities; and
4. Acknowledgement of applicable liability caps and warranties.

1.3.4 **Other participants**

CSPs and RAs operating under this CPS may require the services of other security, application and other service providers.

1.4 **Certificate usage**

By using the certificate, a subscriber agrees to use the certificate for its lawful and intended use only.

1.4.1 **Appropriate certificate uses**

Certificates issued by GovCA can only be used strictly as part of the framework of the limitations incorporated in the certificates.

Relying parties are required to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

1) The appropriateness of the use of the certificate for any given purpose and that the use is not prohibited by this CPS.
2) The certificate is being used in accordance with its key-usage field extensions.
3) The certificate is valid at the time of reliance by reference to Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) checks.

1.4.2 **Prohibited certificate uses**

All certificates issued under this policy cannot be used for purposes other than what is allowed in section 1.4.1 above and what is stipulated in the laws of the Republic of Rwanda.

1.5 Policy administration

1.5.1 Organization administering the document

The GovCA is responsible for all aspects of this CPS and can be contacted at:

C/o Rwanda Information Society Authority
Telecom House, 8 KG 7 Ave, Kigali
Kigali, Rwanda
Website: https://www.govca.rw

1.5.2 Contact person

Att. Chief Executive Officer
Telecom House, 8 KG 7 Ave, Kigali
Kigali, Rwanda
Phone: +250 0788313060 or 4045
Website: https://www.govca.rw
Email: pki@risa.rw

1.5.3 Person determining CPS suitability for the policy

The CPS is one of the assessment requirements by the Root CA.

1.5.4 CPS approval procedures

RISA management shall approve CPS procedures.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

GovCA is responsible for the publication of this CPS and is publicly accessible at CA website.

GovCA shall post its CRL in a directory that is publicly accessible through the Lightweight Directory Access Protocol (LDAP) or Hypertext Transport Protocol (HTTP). To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.
Published CRLs may be replicated in additional repositories for performance enhancement. Such repositories may be operated by GovCA or other authorized parties.

2.2 Publication of certification information

The publicly accessible directory system shall be designed and implemented so as to comply with the following requirements:

1) A general-purpose repository shall be made available 24/7;
2) A general-purpose repository shall have an aggregate uptime not less than 99.7% (or aggregate downtime not exceeding 0.3%) at any period in one (1) month;
3) Any downtime, whether scheduled or not, shall not exceed 30 minutes duration at any one time; and
4) A specific-purpose repository may be made available with specific hours of operation.

2.3 Time or frequency of publication

This CPS and any subsequent changes shall be made publicly available within three (3) days after its approval.

This CPS and any subsequent changes shall be made publicly available within three (3) calendar days after its approval.

2.4 Access controls on repositories

GovCa shall provide unrestricted access to its repository and shall implement logical and physical controls to prevent unauthorized write access to the repository. GovCA shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the internet. This CPS details what information in the repository shall be exempt from automatic availability and to whom, and under which conditions, the restricted information may be made available.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

GovCA shall only generate and sign certificates that contain a non-null subject Distinguished Name (DN). CA shall follow naming and identification rules that include types of names assigned to the subject such as X.500 distinguished names RFC-822.

GovCA must have a unique and readily identifiable Distinguished Name according to the X.500 standard. Details of naming conventions are found in their respective Certificate Profiles.

3.1.2 Need for names to be meaningful

Names used in the certificates must identify the subscriber in a meaningful way to which they are assigned. A name is meaningful only if the names that appear in the certificates can be understood and used by relying parties.

3.1.3 Anonymity or pseudonymity of subscribers

GovCA shall not issue anonymous certificates. Pseudonymous certificates may be issued under this CPS to support internal operations.

3.1.4 Rules for interpreting various name forms

The naming convention used by GovCA is ISO/IEC 9595:1998 (X.500) Distinguished Name (DN) and RFC822 for e-mails.

3.1.5 Uniqueness of names

Name uniqueness must be enforced under this CPS. Distinguished names must be unique for all end entities of GovCA. The Subject Unique Identifiers field, as defined in the Internet X.509 Public Key Infrastructure Certificate and CRL Profile, used to differentiate subscribers with identical names, will not be supported.

GovCA reserves the right to make decisions regarding entity names in all assigned certificates. A party requesting a certificate may be required to demonstrate its right to use a particular name.

3.1.6 Recognition, authentication and role of trademarks

The use of trademarks in names shall not be allowed, unless the subject has legal rights to use that name.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Subscribers must prove possession of the private key corresponding to the Public Key being registered with the GovCA. Such a relationship can be proved by, for example, a digital Signature in Certificate Signing Request (CSR).

3.2.2 Authentication of Organization identity

Requests of Digital Certificates for Organization shall include the organization's name and registered trading address and documentation of the existence of the organization. The legal existence, legal name, legal form and provided address of Organization must be verified and any methods used is highlighted in the CPS.

GovCA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

Juridical applicant's information shall be verified with prior submission of the following:

1) For a government agency:
- Official signed document/power of attorney;
- Copy of National Identification (NID)/ Passport

2) For non-government entities:
- Business registration certificate
- Power of attorney for a representative;

3.2.3 Authentication of individual identity

A request by an individual seeking to be a subscriber in his or her own capacity ("Prospective Subscriber") must be presented by the individual or by another individual authorized to act on behalf of the prospective subscriber.

For Subscribers or authorized representative, GovCA and its RAs shall ensure that the identity information is verified by prior compliance with the following:

1) Physical presence of the applicant;
2) Copy of National Identification (NID)/passport;
3) Phone number (mobile and/or landline);
4) E-mail address; and
5) Consent to verify the information submitted attested by the applicant signature on the application form.
6) The relying party is responsible for due diligence before commitment for foreigner applicant.

3.2.4 Non-verified subscriber information

Any information that is not verified shall not be included in certificates.

Any additional information to be verified may be added upon the agreement with relying parties.

3.2.5 Validation of authority

Before issuing digital certificates that assert organizational authority, GovCA shall validate the individual's authority to act in the name of the organization. For pseudonymous certificates that identify subjects by their organizational roles, GovCA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role

3.2.6 Criteria for interoperation

Root CA shall determine the interoperability criteria for CSPs.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

A request for re-key may be presented by the entity in whose name the keys have been issued or by another individual authorized to act on behalf of the entity. All requests for re-key must be authenticated by GovCA.

An entity requesting re-key may authenticate the request using its valid Digital Signature key pair. Where one of the keys has expired, the request for re-key must be authenticated in the same manner as initial registration.

3.3.2 Identification and authentication for re-key after revocation

After a certificate has been revoked other than during a renewal or update action, the subscriber is required to go through the initial registration process described in Section 3.2 above to obtain a new certificate with new keys.

3.4 Identification and authentication for revocation request

Revocation requests must be authenticated and comply with the following requirements:

1) Confirmation that the person making the revocation request is the subscriber or the request is done by the authorized representative of the subscriber with authority to make the revocation request;
2) Immediately upon revocation, publish a signed notice of the revocation or a CRL in all repositories of such list;
3) Requests for revocation shall be received and acted upon any time; and
4) Record and keep, in trustworthy manner, the date and time of all transactions in relation to the revocation request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

An application for a certificate shall be made directly with GovCA under this CPS or through its accredited RA and fulfilling the application requirements as enumerated in section 3 of this CPS.

4.1.1 Who can apply for a certificate application

An individual applicant or authorized organization representative shall submit a certificate application form directly to GovCA or through its accredited RA.

4.1.2 Enrolment process and responsibilities

All communication during the certificate application process, including delivery of public keys to be included in certificates, shall be authenticated and protected from modification. The applicant shall be responsible for providing accurate information on their certificate applications.

4.2 Certificate application processing

It is the responsibility of GovCA to verify that the information in certificate applications is accurate before the certificate is issued.

4.2.1 Performing identification and authentication functions

The identification and authentication of an applicant for a certificate must meet the requirements specified in section 3 of this CPS.

4.2.2 Approval or rejection of certificate applications

The approval or rejection of certificate application is at the discretion of GovCA under this CPS.

4.2.3 Time to process certificate applications

The certificate application must be processed and a certificate issued within thirty (30) days after the successful identity verification.

4.3 Certificate issuance

4.3.1 Actions during certificate issuance

GovCA and its RAs shall verify the identity and authority (for juridical application) of a prospective subscriber before issuance of a certificate. A certificate shall be checked to ensure that all fields and extension fields are properly populated.

4.3.2 Notification to subscriber by the CSP of Issuance of certificate

GovCA or its RAs operating under this CPS may choose to inform the subscriber of the creation of their certificate and make the certificate available to the subscriber without reasonable delay.

4.4 Certificate acceptance

Before a subscriber can make effective use of its private key, GovCA or its RAs shall convey to the subscriber its responsibilities as defined in section 9.6.3 of this CPS.

4.4.1 Conduct constituting certificate acceptance

Failure to object to the certificate or its contents within thirty (30) days, after notification of the issuance of the certificate, constitutes acceptance of the certificate. A subscriber agrees to the terms and conditions contained in this CPS and the CP of GovCA.

4.4.2 Publication of the certificate by the CSP

No stipulation.

4.4.3 Notification of certificate issuance by the CSP to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private Key and certificate usage

Subscribers shall protect their private keys from access by other parties. By using the certificate, a subscriber agrees to use the certificate for its lawful and intended use only.

4.5.2 Relying party public key and certificate usage

Relying parties are required to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

a) The appropriateness of the use of the certificate for any given purpose and that the use is not prohibited by this CPS.
b) That the certificate is being used in accordance with its key-usage field extensions.
c) That the certificate is valid at the time of reliance by reference to Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) Checks.
d) That the subscriber has a basic understanding of the use and purpose of certificates.

4.6 Certificate renewal

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key.

4.6.1 Circumstance for certificate renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised and the subscriber name and attributes are unchanged.

4.6.2 Who may request renewal

Renewal of a certificate must always be requested by the subscriber directly to the GovCA or through the RA.

4.6.3 Processing certificate renewal requests

GovCA or its RA shall process requests for renewal by verifying that the subscriber information has not changed. GovCA or its RAs shall estimate the validity time left of the keys considering the validity time of the new certificate.

4.6.4 Notification of new certificate issuance to subscriber

The notification of a renewed certificate to a subscriber follows the same routine as when a new certificate is issued as specified in Section 4.3.2 of this CPS. GovCA shall inform the subscriber of the renewal of his or her certificate and the contents of the certificate

4.6.5 Conduct constituting acceptance of a renewal certificate

Failure to object to the certificate or its contents within thirty (30) days, after notification of the renewal of the certificate, constitutes acceptance of the renewed certificate. A subscriber agrees to the terms and conditions contained in this CPS and the CP of GovCA.

4.6.6 Publication of the renewal certificate by the CSP

No stipulation.

4.6.7 Notification of certificate issuance by the CSP to other entities

See section 4.4.3

4.7 Certificate re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtains new keys and re-establishes its identity. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

4.7.1 Circumstance for certificate re-key

A certificate re-key may be done if it is deemed necessary due to one of the following reasons:

1) Migration of hardware;
2) The keys have low cryptographic strength;
3) The keys have high exposure; or
4) Enforced by a standard or application.

There is no limitation of re-key request in a year.

4.7.2 Who may request certification of a new public key

A request for re-keying may be done by a subscriber or the authorized representative of a juridical entity directly to GovCA or its RA. Section 3.3.1 of this CPS shall be followed to verify the information of the subscriber.

4.7.3 Processing certificate re-keying requests

All re-key requests shall be authenticated and authorized by the GovCA or its RAs

4.7.4 Notification of new certificate issuance to subscriber

GovCA or its RAs operating under this CPS may inform the subscriber of the issuance of re-keyed certificates as specified in section 4.3.2 of this CPS.

4.7.5 Conduct constituting acceptance of a re-keyed certificate by the CSP

Failure to object to the certificate or its contents within thirty (30) days, constitutes acceptance of re-keyed certificate.

4.7.6 Publication of the re-keyed certificate by the CSP

No stipulation.

4.7.7 Notification of certificate issuance by the CSP to other entities

See section 4.4.3

4.8 Certificate modification

4.1.1 Circumstance for certificate modification

Certificate modification is performed when change occurs in any of the information of an existing certificate except NID and Names. After modification, the original certificate may or may not be revoked.

4.8.1 Who may request certificate modification

A request for certificate modification may be done by a subscriber or the authorized representative of a juridical entity directly with the GovCA or its RAs. Sections 3.2.1 to 3.2.5 of this CPS shall be followed to verify the information of the subscriber.

4.8.2 Processing certificate modification requests

Proof of all information changes must be provided to GovCA or its RAs before the modified certificate is issued.

4.8.3 Notification of new certificate issuance to subscriber

GovCA shall notify affected subscribers of certificate renewal or modification by any appropriate and secure means.

4.8.4 Conduct constituting acceptance of modified certificate

Failure to object to the certificate or its contents within thirty (30) days, after notification of the certificate modification, constitutes acceptance of the modified certificate. A subscriber agrees to the terms and conditions contained in this CPS and the CP of GovCA.

4.9 Certificate revocation and suspension

Any request for certificate revocation or suspension must be authenticated. GovCA shall publish its CRL for any update done on the digital certificates as specified in section 2 of this CPS.

4.9.1 Circumstances for revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid.

GovCA shall revoke the end-entity's certificate if:

1. Identifying information or affiliation components of any names in the certificate become invalid;
2. The Subject can be shown to have violated the stipulations of its agreement with GovCA;
3. The private key is suspected of compromise; or
4. The Subject or other authorized party (as defined in the applicable CPS) asks for the subscriber's certificate to be revoked.
5. Key Lost;
6. Subscriber is not in a position to use certificate (death – copy of death certificate made available GovCA)

Whenever any of the above circumstances occur, GovCA shall revoke the associated certificate and place it on the CRL. Once revoked, a certificate shall remain on the CRL at least until the certificate expiration date.

4.9.2 Who can request revocation

A request for certificate revocation may be done by GovCA itself, a subscriber or the authorized representative of a juridical entity directly to GovCA or its RAs.

4.9.3 Procedure for revocation request

The request for revocation is done directly to GovCA or its RAs, and these verify the identity and authority (for juridical entity) of a subscriber making the request for revocation.

4.9.4 Revocation request grace period

All revocations shall be performed without any delay after verification and confirmation of the revocation request. There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

4.9.5 Time within which CSP must process the revocation request

A revocation request shall be processed without delay. GovCA shall make best efforts to process revocation request so that it is posted in the next CRL unless a revocation request is received and approved within two hours of next CRL generation.

4.9.6 Revocation checking requirement for relying parties

Relying parties should validate any presented certificate against available CRL or through OCSP.

4.9.7 CRL issuance frequency (if applicable)

GovCA shall publish its CRL at least once every twenty-four (24) hours. The publication and frequency of CRL issuance shall be in conformance with Section 2 of this CPS.

4.9.8 Maximum latency for CRLs (if applicable)

The publication of CRL shall be done without any delay.

4.9.9 On-line revocation/status checking availability

GovCA may provide on-line validation service. If on-line validation is available, it is expected to perform revocation checks using the OCSP server provided.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

The subscriber shall be notified of the revocation of his certificate.

4.9.12 Special requirements re key compromise

In case the private key issued by GovCA get compromised or suspected compromised, the affected certificates shall be revoked.

4.9.13 Circumstances for suspension

The suspension involves the loss of validity. Suspension of a certificate is temporary and proceed with a reactivation or a permanent revocation.

The circumstances under which a certificate issued by GovCA may be suspended are the following:

i. An authenticated request for certificate suspension is received by GovCA or its RAs from an individual subscriber or an authorized representative of a juridical entity subscriber; and
ii. The GovCA has reasonable grounds to believe that the certificate is unreliable, regardless of whether the subscriber consents to the suspension or not; but GovCA shall complete its investigation into the reliability of the certificate and decide within a reasonable time whether to reinstate or to revoke the certificate.

4.9.14 **Who can request suspension**
GovCA or its RAs shall suspend a certificate after receiving a valid request from an individual subscriber or an authorized representative of a juridical entity subscriber.

4.9.15 **Procedure for suspension request**
Suspension of certificates shall follow the same procedures and routines for revocation as provided in section 4.9.3 of this CPS.

A request to suspend a certificate shall identify the certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated (e.g., digitally or manually signed).

4.9.16 **Limits on suspension period**
A suspension shall be temporary and limited with a maximum time (6 months).

A suspended certificate may be terminated before the maximum suspension time under the following conditions:

i. The purpose of the certificate is no longer applicable and the holder is no longer entitled to the use of the certificate; or
ii. The holder requests for immediate termination.

4.10 **Certificate status services**
Both OCSP and CRL are to be made available by GovCA.

4.10.1 **Operational characteristics**
The certificate status validation service shall be always available.

4.10.2 **Service availability**
Both OCSP and CRL shall be always made available by the GovCA.

4.10.3 **Optional features**
No optional features are available.

4.11 **End of subscription**
The term of the contractual relationship is given by the period of validity as indicated in the certificate.

4.12 **Key escrow and recovery**
GovCA does not support key escrow and recovery.

4.13 **Key escrow and recovery policy and practices**
No stipulation

4.14 **Session key encapsulation and recovery policy and practices**
No stipulation

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

GovCA equipment, including cryptographic modules, shall be protected from unauthorized access.

All physical security control requirements specified below shall apply to GovCA and any remote workstations used to administer the CA system, except where specifically noted.

5.1.1 Site Location and Construction

GovCA shall perform its CA operations from a secure data center equipped with logical and physical controls that make the CA operations inaccessible to untrusted users. The site location and construction, when combined with other physical security protection mechanisms such as guards, door locks, and intrusion sensors, shall provide robust protection against unauthorized access to CA equipment and records.

5.1.2 Physical access

GovCA shall protect its equipment from unauthorized access and shall implement physical controls to reduce the risk of equipment tampering. The security mechanisms shall be commensurate with the level of threat in the equipment environment. At a minimum, the physical security access to GovCA hardware and systems shall:

i. Ensure that unauthorized access is not permitted;
ii. Be manually or electronically monitored for unauthorized intrusion at all times;
iii. Ensure that an access log is maintained and inspected periodically; and
iv. Require two-person physical access control.

5.1.3 Power and air conditioning

GovCA shall maintain a backup power supply and sufficient environmental controls to protect th e CA systems and allow the CA to automatically, finish pending operations and record the state of the equipment before a lack of power or air conditioning causes a shutdown. In addition, directories (containing issued certificates and CRLs) shall be provided with Uninterrupted Power sufficient for a minimum of one (1) hour operation in the absence of commercial power.

5.1.4 Water exposures

GovCA shall protect its CA equipment from water exposure. Water exposures from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire prevention and protection

GovCA shall implement reasonable precautions to prevent and extinguish the fire. Each room where a system is installed shall have dry chemical fire extinguisher so that even in case of emergency the system is not affected

5.1.6 Media storage

GovCA shall protect all media from accidental damage (e.g. water, fire, electromagnetic) and unauthorized physical access. GovCA shall duplicate and store its audit and archive information in a backup location that is separate from its primary operations facility.

5.1.7 Waste disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned or otherwise rendered unrecoverable.

5.1.8 Off-site backup

GovCA shall perform weekly system backups sufficient to recover from system failure and shall store the backups, including at least one full backup copy, at an offsite location that has procedural and physical controls that are commensurate with its operational location.

5.2 Procedural controls

5.2.1 Trusted roles

GovCA personnel operating the key management operations administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted role.

GovCA shall distribute the functions and duties performed by persons in trusted roles in a way that prevents one person from circumventing security measures or subverting the security and trustworthiness of the PKI. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of GovCA and RA operations. The following six trusted roles are defined by this CPS, although GovCA or RA may define additional roles:

PKI Manager/Coordinator	GovCA operationalization, system integrations and excellent services delivery
System Developer	Having overall responsibility of system development and integration
Security Officer	Having overall responsibility for administering the implementation of the security policies and practices.
System Administrator	Having authority to install, configure and maintain systems, but with controlled access to security-related information.

System Operator	Responsible for operating trustworthy system on a day-to-day basis. A System Operator is authorized to perform system backup and recovery.
System Auditor	Having authority to view archives and audit logs of system.
Database Administrator	Having privileged access to the database and can create users, databases and manipulate tables. The DBA has access during installation. During normal operations, the DBA is not allowed to log into the system.
PKI promotion officer	Having overall responsibility of promoting usage of PKI service and awareness.
Infrastructure office	Having overall responsibility of maintaining PKI infrastructure and facilities
Registration Officer	Responsible for approving Certificate generation, revocation, suspension, renewal and re-key for end entity.

Some roles may be combined or expanded. The roles required are further identified, with the following subsections providing a detailed description of some of the responsibilities for each role.

5.2.2 Number of persons required per task

GovCA shall require at least two or more people for the following tasks:

1) CA key generation
2) CA signing key activation
3) CA private key backup

All roles are recommended to have multiple persons in order to support continuity of operations.

5.2.3 Identification and authentication for each role

GovCA personnel shall identify and authenticate themselves before being permitted to access to the systems necessary to perform their trusted roles.

5.2.4 Roles requiring separation of duties

Role separation may be enforced either by the CA equipment, or procedurally, or by both means. Individuals may assume more than one role, except:

i. Individuals who assume an officer role may not assume an administrator or audit administrator role;
ii. Individuals who assume an audit administrator shall not assume any other role on the CA; and
iii. Under no circumstances shall any of the roles perform their own compliance audit

function.

No individual shall be assigned more than one identity.

5.3 Personnel controls

5.3.1 Qualifications, experience and clearance requirements

GovCA shall identify at least one individual or a group of individuals responsible and accountable for the operation of the CA and compliance with CP and CPS. GovCA personnel filling trusted roles shall be selected on the basis of loyalty, trustworthiness and integrity. All trusted roles are required to be held by national citizens and in accordance with the following requirements:

i. At least one (1) of the technical personnel shall be a full-time certified information security professional, who shall oversee the operations/management of the CA and whose certification is issued by the national government or internationally-recognized bodies such as, but not limited to ISO, ISACA, SANS and (ISC)2;

ii. Each technical personnel shall have any of the following educational qualifications:

    Degree or Diploma in computer engineering, computer science or information and communications technology and any other related fields;

iii. At least a half of the personnel shall have work experience of at least five (5) years in the field of information security or operation and management of information and communications technology;

iv. Not an undischarged bankrupt person in the country or elsewhere, or has made arrangement with his creditors;

v. Has not been convicted, whether in the country or elsewhere, of an offense, or fraudulent or dishonest act;

5.3.2 Background check procedures

GovCA personnel fulfilling a trusted role shall, at a minimum, prior to acting in the role, undergo a background investigation procedure covering the following areas:

i. Employment
ii. Education
iii. Place of residence
iv. Criminal background
v. References

The period of investigation must cover at least the last five (5) years for each area, excepting the residence check which must cover at least the last three (3) years. Regardless of the date of award, the highest educational degree shall be verified.

5.3.3 Training requirements

All personnel performing duties with respect to the operation of the CA or RA shall receive comprehensive training in all operational duties they are expected to perform, including good knowledge on the following:

i. PKI policies, regulations and related laws.
ii. Basic Public Key Infrastructure (PKI) knowledge;
iii. All PKI software versions in use by GovCA;
iv. Authentication and verification policies and procedures;
v. CA/RA security principles and mechanisms;
vi. Disaster recovery and business continuity procedures,
vii. Common threats to the validation process, including phishing and other social engineerig tactics.
viii. GovCA’s Certification Practice Statement; and
ix. Regulation governing certification authorities

Documentation shall be maintained identifying all personnel who received training and the level of training completed. Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.

5.3.4 Retraining frequency and requirements

Individuals acting in trusted roles shall be aware of changes to the GovCA's or RA's operations. For any significant change to the CA operations, GovCA shall provide a documented training, in accordance with an executed training plan, to all trusted roles. Examples of such changes are software or hardware upgrade, changes in automated security systems and relocation of equipment.

5.3.5 Job rotation frequency and sequence

Job rotation frequency and sequencing procedures shall be provided for continuity and integrity of GovCA’s services.

5.3.6 Sanctions for unauthorized actions

GovCA employees failing to comply with this CPS, whether through negligence or malicious intent, shall be subject to administrative or disciplinary actions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review.

5.3.7 **Independent contractor requirements**

GovCA allowing independent contractors to be assigned to perform trusted roles shall require that they agree to the obligations under this section 5 (Facility, Management, and operation Controls) and the sanctions stated above in section 5.3.6.

5.3.8 **Documentation Supplied to Personnel**

GovCA shall provide personnel in trusted roles with the documentation necessary to perform thei r duties.

5.4 **Audit logging procedures**

Audit log files shall be generated for all events relating to the security of the CA or RA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form or other physical mechanism shall be used.

All security audit logs, both electronic and non-electronic, shall be retained, indexed, stored, preserved and reproduced so as to be accurate, complete, legible and made available during compliance audits.

5.4.1 **Types of events recorded**

GovCA systems shall require identification and authentication at system logon. Important system actions shall be logged to establish the accountability of the operators who initiate such actions.

A message from any source received by the CA requesting an action related to the operational state of the CA is an auditable event. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

i. The type of event;
ii. The date and time the event occurred;
iii. A success or failure indicator, where appropriate; and
iv. The identity of the entity and/or operator (of the CA or RA) that caused the event.

The following are auditable events:

8. Authentication to systems
9. Physical access
10. Key generation
11. Certificate lifecycle
12. Transaction logs
13. System logs
14. Application logs

All essential event auditing capabilities of the CA's operating system and applications required by this CPS shall be enabled. As a result, the events identified above shall be automatically recorded. Where events cannot be automatically recorded, GovCA shall implement manual procedures to satisfy this requirement. All event records shall be made available to auditors as proof of GovCA's practices.

5.4.2 Frequency of processing log

Audit logs shall be reviewed daily. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the log.

Examples of irregularities include discontinuities in the logs and loss of audit data. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention period for audit log

Audit logs shall be retained in a trustworthy manner on-site until reviewed, as well as being retained for a period of ten (10) years from the date of issuance of the certificate.

5.4.4 Protection of audit log

GovCA shall configure its systems and establish operational procedures to ensure that:

1) Only authorized people have read access to logs;
2) Only authorized people may archive audit logs, and
3) Audit logs are not modified.

Procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

The off-site storage location for audit logs shall be a safe and secure location that is separate from the location where the data was generated.

5.4.5 Audit log backup procedures

On at least a monthly basis, GovCA shall make backups of audit logs and audit log summaries and send a copy of the audit log off-site.

5.4.6 Audit collection system (internal vs. external)

The audit log collection system may or may not be external to the CA system. Automated audit collection processes shall be invoked at system or application startup and cease only at system or application shutdown.

5.4.7 Notification to event-causing subject

This CPS imposes no requirement to provide notice that an event was audited to the individual, organization, device or application that caused the event.

5.4.8 **Vulnerability assessments**
Once a year, GovCA shall assess the vulnerability of its systems and components. A routine risk assessment of the CA system shall be performed regularly.

5.5 **Records archival**

GovCA or its RA shall comply with their respective records retention policies.

5.5.1 **Types of records archived**
GovCA shall make and keep in a trustworthy manner the records relating to the following:

1) Activities of issuance, renewal, suspension and revocation of certificates, including the process of identification of any person requesting a certificate from GovCA;
2) The process of generating subscribers' (where applicable) or GovCA's own key pairs; and
3) Such related activity of GovCA as may be determined later on by the Root CA.

5.5.2 **Retention period for archive**
The minimum retention periods for archived data shall be ten (10) years.

5.5.3 **Protection of archive**
No unauthorized user shall be permitted to access, write or delete the archived records. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally authorized representative(s).

5.5.4 **Archive backup procedures**
GovCA shall store its archived records at a secure of-site location in a manner that prevents unauthorized modification, substitution, or destruction. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined. GovCA shall maintain any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

5.5.5 **Requirements for time-stamping of records**
GovCA archive records shall be automatically time-stamped as they are created.

5.5.6 **Archive collection system (internal or external)**
No stipulation.

5.5.7 **Procedures to obtain and verify archive information**
GovCA may archive data manually or automatically. If automatic archival is implemented, GovCA shall synchronize its archived data on a daily basis.

GovCA may allow subscribers to obtain a copy of their archived information. Otherwise, GovCA shall restrict access to archive data to authorized personnel in accordance with GovCA's internal security policy and shall not release any archived information except as allowed by law.

GovCA shall maintain, and provide upon receipt of a proper request by such authorized person, t he procedures it follows to create, verify, package, transmit, and store archived information.

5.6 Key changeover

To minimize risk from compromise of GovCA's private signing key, that key may be changed; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, public key will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that cover certificates signed with that key, then the old key must be retained and protected.

Key changeover procedures will establish key rollover certificates where a certificate containing the old public key will be signed by the new private key, and a certificate containing the new public key will be signed by the old private key.

GovCA operating under this CPS either must establish key rollover certificates as described above or must obtain a new CA certificate for the new public key from the issuers of their current certificates.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

GovCA shall develop and implement procedures to be followed in the event of a serious security incident or system compromise. Required documentation includes, but is not limited to, an Incident Response Plan, a Disaster Recovery or Business Continuity Plan (DR/BCP), and related resources. GovCA shall review, test, and update its Incident Response Plan and DR/BCP, and supporting procedures, at least annually.

GovCA shall provide notice to the Root CA for any of the following incidents:
1) Compromise of CA's signing key;
2) Penetration of CA's system and network;
3) Unavailability of infrastructure; and
4) Fraudulent registration and generation of certificates, certificate suspension and revocation information.

If any incident above happens, GovCA shall report it to the Root CA within the next working day.

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

GovCA shall make regular back-up copies of its private keys and store them in a secure off- site location. GovCA shall also make regular system back-ups on at least a weekly basis.

When computing resources, software, and/or data are corrupted, GovCA shall respond as follows:

1) Before returning to operation, ensure that the system's integrity has been restored;
2) If the CA signature keys are not destroyed, CA operation shall be re-established, giving priority to the ability to generate certificate status information within the CRL issuance schedule;
3) If the CA signature keys are destroyed, CA operation shall be re-established as quickly as possible, giving priority to the generation of a new CA key pair.

5.7.3 Entity private key compromise procedures

1) If GovCA suspects that its private key is compromised or lost (such that compromise is possible even though not certain):

   i. The Root CA and its entire member entities shall be notified so that entities may issue CRLs revoking any cross-certificates issued to the compromised CSP;
   ii. A new key pair shall be generated by the CA; and
   iii. New certificates shall also be issued to subscribers.

2) If the CSP distributes its key in a self-signed certificate, the new self-signed certificate shall be distributed as specified in Section 6.1.4 of this CPS.
3) The CSP governing body shall also investigate and report to the Root CA what caused the compromise or loss, and measures that shall be taken to prevent a reoccurrence.

5.7.4 Business continuity capabilities after a disaster

GovCA directory system shall be deployed so as to provide 24 hour, 365 days per year availability.

GovCA shall operate a hot backup site to ensure continuity of operations in the event of a physical disaster or failure of the primary site. GovCA operations shall be designed to restore full service within six (6) hours of primary system failure.

5.7.5 CA or RA termination

In the event that GovCA terminates its operation, it shall provide notice to the Root CA 60 days prior to termination.

6 TECHNICAL SECURITY CONTROLS

GovCA private keys shall be protected within a hardware security module (HSM) meeting at least Level 2 of the Federal Information Processing Standard 140 (FIPS 140). Access to the HSM within the CA environment shall be restricted by the use of smartcard or biometric device. The HSM is always stored in a physically secure environment and subject to security controls throughout its lifecycle.

6.1 Key pair generation and installation

6.1.1 Key pair generation

GovCA key pair generation shall be performed by trained and trusted individuals using secure systems and processes. All the activities performed in each key generation are recorded, dated and agreed by all individuals involved. The records shall be kept for audit and tracking purposes for a length of time deemed appropriate by GovCA.

Subscriber key pair generation shall be performed (i) by the subscriber or (ii) by authorized member of GovCA team via a secured CA web portal after the physical identification performed by GovCA or RA. The key pair delivery follows the requirements specified in the following section.

6.1.2 Private Key delivery to subscriber

If a subscriber generates his/her own key pairs, then there is no need to deliver private keys and this section does not apply.

If GovCA or RA generates keys on behalf of the subscriber, then the private key must be delivered securely to the subscriber. Private keys may be delivered electronically or on a hardware cryptographic module.

In all cases, the following requirements shall be met:

1. Anyone who generates a private signing key for a subscriber shall not retain any copy of the key after delivery of the private key to the subscriber.
2. The private key must be protected from activation, compromise or modification during the delivery process.
3. The subscriber shall acknowledge receipt of the private key.

GovCA or RA shall maintain a record of the subscriber acknowledgement of receipt of the private key.

6.1.3 Public key delivery to certificate issuer

Subscribers shall provide their public key to GovCA for certification through a PKCS#10 Certificate Signing Request via GovCA web portal using credentials that bind the subscriber's verified identity to the Public Key. The certificate request process shall ensure that the applicant possesses the private key associated with the public key presented for certification.

6.1.4 CA Public Key Delivery to Relying Parties

When GovCA updates its signature key pair, it shall distribute the new public key in a secure fashion and in a manner that precludes substitution attacks. GovCA Certificates may also be downloaded from the GovCA Web site at http://www.govca.rw/.

6.1.5 Key Sizes

Key pairs shall be of sufficient size to prevent cryptanalytic attacks on encrypted communications during the period of expected utilization of such key pairs. The current GovCA standard for minimum key pair is 2048 bits for RSA. Subscribers use a minimum of 2048 bits RSA keys.

GovCA that generate certificates and CRLs under this CPS shall use SHA-224, SHA-256, SHA-384 or SHA-512 hash algorithm when generating digital signatures.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Keys may be used for the purposes and in the manner described in Section 7.1 of this CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

GovCA shall implement a combination of physical, logical, and procedural controls to ensure the security of GovCA private keys. Subscribers are required to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

For both the generation and maintenance of private keys, GovCA shall use the HSM that meet at least level 2 of FIPS 140.

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

GovCA private keys shall be accessed through multi-person control as specified in section 5.2.2 of this CPS.

6.2.3 Private Key Escrow

Private keys shall not be escrowed.

6.2.4 Private Key Backup

GovCA's private keys are stored in encrypted state and access is only by multi-person control as specified in section 6.2.2 of this CPS. The private keys are backed up under further encryption and maintained on-site and off-site in a secure storage.

Subscribers may choose to back up their private keys by backing them up on their hard drive or the encrypted file containing their keys.

6.2.5 Private Key Archival

Private keys used for encryption shall not be archived.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

If a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport.

6.2.7 Private Key Storage on Cryptographic Module

Private keys held in a cryptographic module are stored in an encrypted form and password-protected.

6.2.8 Method of Activating Private Key

GovCA signing activation requires multi-party control as specified in section 5.2.2 of this CPS. All GovCA PKI participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

GovCA shall activate its private keys in accordance with the specifications of the cryptographic module manufacturer. Subscribers are solely responsible for protecting their private keys. At a minimum, subscribers must authenticate themselves to the cryptographic module before activating their private keys. Entry of activation data shall be protected from disclosure.

6.2.9 Method of Deactivating Private Key

A cryptographic module that had been activated shall not be available to unauthorized access. After use, a cryptographic module shall be deactivated following procedures that meet the process described by the cryptographic module vendor.

6.2.10 Method of Destroying Private Key

A private key shall be destroyed when no longer needed or when the certificate to which it corresponds is already expired or is revoked. A private key shall be destroyed in a way that prevents its loss, theft, modification, unauthorized disclosure or unauthorized use. Such destruction shall be documented, and will be done following the procedures that meet the process described by the cryptographic module vendor.

6.2.11 Cryptographic Module Rating

See section 6.2.1 of this CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum validity period for the certificate of GovCA shall be ten (10) years while the certificate of a Root CA shall be for twenty (20) years. GovCA shall not issue a certificate that extends beyond the expiration date of its own certificate and public key. A subscriber's certificate shall have a maximum validity period of one (1) year renewable.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Two-factor authentication shall be used to protect access to a private key. GovCA is also required to use strong passwords to further prevent unauthorized access to the CA system.

6.4.2 Activation Data Protection

Data used to unlock a private key shall be protected from disclosure. Activation data shall be memorized, biometric in nature or recorded and secured at the level of assurance associated with the activation of the cryptographic module.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

GovCA performs all CA and RA functions using trustworthy systems. These activities shall follow the rules and guidelines issued by GovCA for the information security requirements.

6.5.1 Specific Computer Security Technical Requirements

GovCA shall have a formal Information Security Policy that documents the policies, standards and guidelines relating to information security. The computer security functions listed below are required. These functions may be provided by the operating system or through a combination of operating system, software and physical safeguards.

a. Require authenticated logins
b. Provide discretionary access control
c. Provide a security audit capability
d. Restrict access control to CA services and PKI roles
e. Enforce separation of duties for PKI roles
f. Require identification and authentication of PKI roles and associated identities
g. Archive audit data

e. Require self-test security related services
f. Require recovery mechanisms for keys and the CA system

6.5.2 Computer Security Rating
No stipulation.

6.6 Life Cycle Technical Controls
6.6.1 System Development Controls
No Stipulation.

6.6.2 Security Management Controls
No Stipulation.

6.6.3 Life Cycle Security Controls
No Stipulation.

6.7 Network Security Controls
All access to CA equipment via network shall be protected by network firewall and filtering router. Networking equipment shall turn off unused network ports and services.

6.8 Time Stamping
Certificates, CRLs, and other revocation database entries shall contain time and date information. All logs will contain synchronized time.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

Certificates issued under this policy shall conform to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

7.1.1 Version Number(s)

GovCA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

GovCA shall use standard certificate extensions that comply with RFC [3280/5280].

7.1.3 Algorithm Object Identifiers

Certificates issued under this CPS shall use the Object Identifier (OID).

7.1.4 Name Forms

The subject and issuer fields of the base certificate shall be populated with a non-empty X.500 Distinguished Name as specified in section 3.1.1 above. Distinguished names shall be composed of standard attribute types, such as those identified in RFC [3280/5280].

7.1.5 Name Constraints

GovCA may assert name constraints in the name constraints field when appropriate.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CPS shall use the OID number that points to the correct CSP as well as Certificate Policy.

7.1.7 Usage of Policy Constraints Extension

GovCA may assert policy constraints in GovCA certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CPS may contain policy qualifiers identified in RFC [3280/5280].

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

GovCA operating under this CPS shall issue X.509 version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

GovCA operating under this CPS shall use RFC [3280/5280] CRL and CRL entry extension.

7.3 OCSP profile

OCSP requests and responses under this CPS shall be in accordance with RFC 2560.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No Stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

At least once a year, GovCA shall be subject to audit in respect with its accreditation by ROOT CA.

8.2 Identity/qualifications of assessor

The audit requirement shall be performed by a qualified independent assessment team comprising, but not limited to, the following:

i. Certified Public Accountants; and
ii. Certified Information Security practitioners.

The following conditions should also be fulfilled:

i. Expertise: The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with Public Key infrastructures, certification systems, and Internet security issues.
ii. Reputation: The firm must have a reputation for conducting its auditing business competently and correctly.

8.3 Assessor's relationship to assessed entity

Any member of the assessment team and the firm(s) or company(ies) the member affiliated with shall have no conflict of interest with the CSP being assessed and shall not be a software or hardware vendor that is or has been providing services or supplying equipment to the CSP within the last two (2) years.

8.4 Topics covered by assessment

The audit must conform to industry standards, cover GovCA's compliance with its business practices disclosure, and evaluate the integrity of GovCA's PKI operations. The audit must verify that GovCA is compliant with this CPS.

8.5 Actions taken as a result of deficiency

If an audit reports a material noncompliance with applicable law, this CPS, then

(1) The auditor shall document the discrepancy,
(2) The auditor shall promptly notify GovCA and the ROOT CA, and
(3) GovCA and the ROOT CA shall develop a plan to cure the noncompliance.

GovCA shall submit the plan to the ROOT CA for approval and to any third party that GovCA is legally obligated to satisfy. The ROOT CA may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected certificates.

8.6 Communication of results

A copy of the assessment report shall be submitted to controller within four (4) weeks after completion of an assessment.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

GovCA or RA, operating under this CPS shall be allowed to charge fees for the issuance of certificates.

9.2 Certificate issuance or renewal fees

No stipulation.

9.3 Certificate access fees

GovCA is required to publish certificates and the CRL. Thus, no additional fees for access to this information shall be made by GovCA.

9.3.1 Revocation or status information access fees

GovCA is required to publish certificates and the CRL. Thus, no additional fees for access to this information shall be made by GovCA.

9.3.2 Fees for other services

No stipulation.

9.3.3 Refund policy

No stipulation.

9.4 Financial responsibility

9.4.1 Insurance coverage

GovCA operating under this CPS shall be insured against liabilities for damages.

9.4.2 Other assets

No stipulation.

9.4.3 Insurance or warranty coverage for end-entities

No stipulation

9.5 Confidentiality of business information

Information about the GovCA or RA not requiring protection or confidentiality shall be made publicly available for transparency purposes. The mode of access to such information shall be determined by each respective organization.

9.5.1 Scope of confidential information

No stipulation.

9.5.2 Information not within the scope of confidential information

No stipulation.

9.5.3 Responsibility to protect confidential information
No stipulation.

9.6 Privacy of personal information
GovCA or RA shall keep all subscriber-specific information confidential except as required by law or pursuant to an order of court.

9.6.1 Privacy plan
GovCA or RA shall have a privacy plan to always protect personally identifying information from unauthorized disclosure.

9.6.2 Information treated as private
GovCA or RA shall protect all personally identifying information of subscribers from unauthorized disclosure. A record of an individual transaction may be released upon request of the subscriber involved in the transaction. Any record from the archive maintained by GovCA operating under this CPS shall not be released except as required by law or a court order.

9.6.3 Information not deemed private
Information included in Section 7 of this CPS is not subject to protection outlined in Section 9.4.2 above.

9.6.4 Responsibility to protect private information
Confidential information must be stored securely and may be released only in accordance with the requirements of RA.

9.6.5 Notice and consent to use private information
Personal information provided during the application and identity verification process is considered private information provided that the information is not included in a certificate. GovCA or RA shall only use private data after obtaining the subject's express written consent or as required by applicable law or regulation.

9.6.6 Disclosure pursuant to judicial or administrative process
GovCA shall not disclose any private information to any third party unless authorized by this CPS, required by law or through a court order. Any request for release of information shall be processed according to an established procedure.

9.6.7 Other information disclosure circumstances
No stipulation.

9.7 Intellectual property rights

The intellectual property rights held by other individual, organization or entities shall always be upheld by GovCA or RA.

9.8 Representations and warranties

9.8.1 CA representations and warranties

GovCA will operate its certification and repository services, issue and revoke certificates and issue CRLs in accordance with the requirements of this CPS. Identification and authentication procedures shall be implemented as specified in section 3 of this CPS.

9.8.2 RA representations and warranties

No stipulation.

9.8.3 Subscriber representations and warranties

Subscribers of GovCA operating under this CPS shall agree to the following:

i. Accurately represent themselves in all communications with the PKI authorities.
ii. Protect their private keys at all times, in accordance with this CPS.
iii. Promptly notify the appropriate CSP/RA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through procedures consistent with GovCA's CPS.
iv. Abide by all the terms, conditions and restrictions on the use of their private keys and certificates.

9.8.4 Relying party representations and warranties

No stipulation.

9.8.5 Representations and warranties of other participants

No stipulation.

9.9 Disclaimers of warranties

GovCA or its RA assumes no liability except as stated in the relevant contracts pertaining to certificate issuance and management.

9.10 Limitations of liability

GovCA or its RA shall not be liable for any damages to subscribers, relying parties or any other parties arising out of or related to the misuse of, or reliance on certificates issued by GovCA that has been:

i. Revoked;
ii. Expired;
iii. Used for unauthorized purposes;
iv. Tampered with;
v. Compromised; or
vi. Subject to misrepresentation, misleading acts or omissions.

9.11 Indemnities

Subscribers and relying parties shall agree to indemnify and hold GovCA or its RA harmless from any claims, actions or demands that are caused by the use or publication of a certificate and that arises from:

i. Any false or misleading statement of fact by the subscriber;

ii. Any failure by the subscriber to disclose a material fact, if such omission was made negligibly or with the intent to deceive;

iii. Any failure on the part of the subscriber to protect its private key and/or token if applicable or to take the precautions necessary to prevent the compromise, disclosure, loss, modification or unauthorized use of the subscriber's private key; or

iv. Any failure on the part of the subscriber to promptly notify GovCA or RA of the compromise, disclosure, loss, modification or unauthorized use of the subscriber's private key once the subscriber has actual or constructive notice of such event.

9.12 Term and termination

9.12.1 Term

This CPS becomes effective upon approval by the ROOT CA and its publication in the GovCA Repository of documents in its website.

9.12.2 Termination

This CPS shall remain in force until it is amended or replaced by a new version.

9.12.3 Effect of termination and survival

The requirements of this CPS shall remain in effect through the end of the archive period for the last certificate issued.

9.12.4 Individual notices and communications with participants

GovCA shall establish appropriate procedures for communications with RA through memorandum of understanding as applicable.

9.13 Amendments

9.13.1 Procedure for amendment

GovCA shall review this CPS at least once a year. Corrections, updates or suggested changes to this CPS shall be communicated to every RA. Such communication must include a description of the change, a change justification and contact information of the person requesting the change.

9.13.2 Notification mechanism and period

Proposed changes to this CPS shall be distributed electronically to RAs and other bodies/entities. The notification shall contain the final date for receipt of comments and the proposed effective date of change.

9.13.3 Circumstances under which OID must be changed

No stipulation.

9.14 Dispute resolution provisions

Any dispute arising with respect to this CPS or pertaining to the use and issuance of certificates, issued under this CPS, shall be resolved amicably by GovCA, through alternative dispute resolution between parties, subject to implementing guidelines to be issued.

9.15 Governing law

The laws of Rwanda and more particularly the law N°24/2016 OF 18/06/2016 GOVERNING INFORMATION AND COMMUNICATION TECHNOLOGIES (Official Gazette n°26 of 27/06/2016) which is a revision of law nº18/2010 of 12/05/2010 relating to electronic message, electronic signature and electronic transaction, regulation governing certification service provider and the guidelines issued and clarifications made from time to time by the controller shall govern the construction, validity, enforceability and performance of actions per this CPS.

9.16 Compliance with applicable law

GovCA or RA is required to comply with any applicable laws.

9.17 Miscellaneous provisions

9.17.1 Entire agreement

No stipulation.

9.17.2 Assignment

No stipulation.

9.17.3 Severability

If any section of this CPS is determined to be incorrect or invalid, the other sections of this CPS that are not affected shall remain in effect until the CPS is updated. The process for updating this CPS is described in Section 9.12 above.

9.17.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.17.5 Force Majeure

GovCA or its RA accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as, but not limited to the following:

i. Acts of God;
ii. Acts of War;
iii. Acts of Terrorism;
iv. Epidemics;
v. Power or telecommunication services failure;
vi. Earthquake;
vii. Fire; or
viii. Any other natural or man-made disasters.

9.18 Security Check

Self-inspections shall periodically be conducted to ensure effective security management when carrying out the certification management practice.

9.19 Validity of Certification Practice Statement

The established and revised certification practice statement shall become effective 15 days after the date of its reporting/publishing.

9.20 Other provisions

No stipulation.

Done at Kigali, on 04/10/2018

(Sé)

Innocent B. MUHIZI

Chief Executive Officer

Rwanda Information Society Authority