Rwanda National Public Key Infrastructure

Certification Policy (CP)

Version 1.0

November, 2018

Document Title : Certification Policy

Document type : Policy

Author **:** Government Certification Authority

Issue/Version No : 1.0

OID **:** 2 16 646 200001 3 1 1 3 1

Issue Date : November, 2018

CP Revision Control

Date	**Issue No.**	**Details of Changes**

Contents

1 INTRODUCTION

Government of Rwanda established 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 (hereafter referred as CP) 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.

A CP is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

This CP applies to certificates issued under the certification scheme for digital signatures.

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

1.2 Document Name and Identification

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

1.3 PKI Participants

1.3.1 Rwanda Certification Authorities

The Root Certification Authority 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

1.3.1.1 Rwanda Root CA (RootCA) obligations:

1) Operate and manage the Root CA system and its functions;
2) Issue and manage certificates for designated Accredited CAs;
3) Re-key of the Root CA and approved CA signing keys;
4) Establishment and maintenance of the CP and CPS for Root CA;

5) Provide technical expertise in the conduct of assessment of CAs when necessary;
6) Support international cooperation on certification service, including mutual recognition and cross-certification;
7) Notification of issuance, revocation, suspension or renewal of its certificates; and
8) Resolve disputes between concerned parties.

1.3.1.2 Government CA obligations:

Government certification authority (GovCA) is the government Accredited Certification Authority by the Root CA.

The GovCA is obliged to perform certain functions as follows:
1) Operate and manage the CA systems and its functions in accordance with the RootCA-CP;
2) Issue and manage certificates to user or juridical entities, used for general or specific purpose;
3) Publish certificates revocation information;
4) Handle revocation request regarding certificate issued by the CA; and
5) Notification of issuance, revocation, suspension or renewal of its certificates.

1.3.2 Registration Authority (RA)

GovCa may designate specific RAs to perform the Subscriber Identification and Authentication and certificate request and revocation functions defined in the GovCA CPS and related documents.
The RA is obliged to perform certain functions pursuant to an RA Agreement including the following:

1) Identify the user and register the user information;
2) Transmit the certificate request to the CA;
3) Validate certificates by the CA Directory Server and CRL; and
4) Request for revocation, suspension and restoration of certificates.
5) Other troubleshooting related to certificate management

1.4 Subscribers

A subscriber is an individual or juridical entity whose name appears as the subject 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.

1.5 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 as

detailed in GovCA CPS.

1.6 Other Participants

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

1.7 Certificate Usage

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

1.7.1 Appropriate Certificate Usage

1) The Root CA certificate can only be used for signing subordinate CA's and CRL's.
2) 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 CP.
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 or Certificate Revocation List checks.

1.7.2 Prohibited Certificate Usage

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 laws of the Republic of Rwanda

1.8 Policy Administration

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

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

1.8.1 Contact person

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

1.8.2 Determining CP Suitability for the Policy

The CP is one of the assessment requirements by the Root CA.
Attn: Director General
Rwanda Utilities Regulatory Authority
Controller of Certification Service Provider
P. o. Box 7289, Kigali-Rwanda
Tel No: (+250)252584562
E-mail: rootca@rura.rw

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

GovCA is responsible for the publication of this CP and is publicly accessible at CA website: https://www.govca.rw

GovCA shall post its CRL issued 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 the GovCA or other authorized parties.

2.2 Publication of Certification Information

The publicly accessible directory system shall be designed and implemented

2.3 Time or Frequency of Publication

A certificate shall be made available as soon as it is issued to a subscriber, suspended, renewed or revoked.
This CP 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 protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. The CPS shall detail 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).
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 Rules for Interpreting Various Name Forms

The naming convention used by GovCA is ISO/IEC 9595:1998 (X.500) Distinguished Name (DN).

3.1.4 Uniqueness of Names

Name uniqueness must be enforced by the CSP.

3.1.5 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 of Proof of Possession of Private Key

In all cases where the subject named in a certificate generates its own keys, that subject shall be required to prove possession of the private key that corresponds to the public key in the certificate request.

3.2.2 Authentication of Organization Identity

Requests for organization certificates shall include the organization name, address and documentation of the existence of the organization.
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:

2) Business Registration Number;
3) For a government agency:
- Official signed document/Power of attorney

4) For non-government entities:
- Business registration certificate/

- Power of attorney for a representative;
- Physical presence for foreigner applicant is option, the relying party is responsible for due diligence before offering service.

3.2.3 Authentication of Individual Identity

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

i. Physical presence of the applicant;
ii. Copy of National Identification (NID)/ Valid Passport;
iii. Phone number (mobile and/or landline);
iv. E-mail address; and
v. Consent to verify the information submitted attested by the applicant signature on the application form.
vi. The relying party is responsible for due diligence before commitment for foreigner applicants.

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 up on the agreement with relying parties

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Subscriber certificate re-key shall be possible if the key pair is still valid and request for re-key shall be authenticated by GovCA.

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 Certificate Revocation List in all repositories of such list;
3) Requests for revocation shall be received and acted upon any time
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 CP or through its accredited RA and fulfilling the application requirements as enumerated in Section 3 of this CP.

4.1.1 Submission of a Certificate Application

An individual applicant or authorized organization representative can submit a Certificate Application Form directly to GovCA.

4.1.2 Enrolment Process and Responsibilities

The applicant shall be responsible for providing accurate information in the Certificate Application Form.

4.2 Certificate Application Processing

The information in Certificate Application Form must be verified as accurate before a 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 CP.

4.2.2 Approval or Rejection of Certificate Application

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

4.2.3 Time to Process Certificate Application

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

The GovCA and its RA 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 GovCA or its RA

GovCA or its RAs operating under this CP 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, the GovCA or its RAs shall convey to the subscriber its responsibilities

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 CP and the CPS of the GovCA.

4.4.2 Publication of the Certificate by the GovCA

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 at all times. 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 CP.
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.

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

A subscriber requests for certificate renewal directly to the GovCA or through the RA.

4.6.3 Processing Certificate Renewal Requests

The GovCA or its RA shall process requests for renewal by verifying that the subscriber information has not changed. The 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 CP. GovCA and its RAs operating under this CP may inform the subscriber of the issuance of renewed certificate as specified in Section 4.3.2 of this CP.

4.6.5 Conduct Constituting Acceptance of a Renewed 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 CP and the CPS of the GovCA.

4.6.6 Publication of Renewed Certificate

No stipulation.

4.7 Certificate Re-key

4.7.1 Circumstance for 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 for Re-Key

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

4.7.3 Processing Certificate Re-Key Requests

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

4.7.4 Notification of Certificate with New Keys to Subscriber

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

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

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

4.8 Certificate Modification

4.8.1 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

4.8.2 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 CP shall be followed to verify the information of the subscriber.

4.8.3 Processing Certificate Modification Requests

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

4.8.4 Publication of the Modified Certificate by the GovCA

No stipulation.

4.8.5 Notification of new certification issuance to subscriber

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

4.9 Certificate Revocation and Suspension

Any request for certificate revocation or suspension must be authenticated. GovCA shall publish its CRL as specified in Section 2 of this CP.

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 will revoke the end-entity's certificate if:

i. The GovCA determines that its policy requirement is no longer being met by the subscriber.

ii. An authenticated request to GovCA or its RA is received from an individual subscriber or an authorized representative of a juridical entity subscriber.

iii. An authorized employee determines that an emergency has occurred that may impact the integrity of the certificates issued by the GovCA. Under this circumstance, the official performing the duty shall authorize the immediate revocation of the certificate.

4.9.2 Who Can Request Revocation

A request for certificate revocation may be done by the 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 GovCA or its RAs shall 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.

4.9.5 Time within which GovCA must process the revocation request

A revocation request shall be processed without any delay.

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 CP.

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 Circumstances for Suspension

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.

4.9.11 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.

4.9.12 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 CP.

4.9.13 Limits on Suspension Period

A suspension shall be temporary and limited with a maximum time of six (6) months.
A suspended certificate may be terminated before the maximum suspension time under the following conditions:

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

4.10 Certificate Status Services

Both OCSP and CRL are to be made available by GovCA.

5 MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

5.1 Physical Security Controls

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

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

5.1.1 Site Location and Construction

The location and construction of the facility housing the GovCA equipment, as well as sites housing remote workstations used to administer the GovCA systems shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the equipment and records of GovCA.

5.1.2 Physical Access

The GovCA equipment including remote workstations used to administer the GovCA systems shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment.

At a minimum, the physical access security shall:

i. Ensure that no unauthorized access to the hardware is permitted;
ii. Be manually or electronically monitored for unauthorized intrusion at all times;
iii. Ensure that an access log is maintained and inspected periodically;
iv. Require two-person physical access control; and
v. Ensure that all removable media and paper copy containing sensitive plain-text information is stored in secure containers.

5.1.3 Power and Air Conditioning

GovCA environment shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. 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

The GovCA equipment shall be installed such that it is not in danger of exposure to water.

Water exposures from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

The GovCA shall implement reasonable precautions to prevent and extinguish the fire.

5.1.6 Media Storage

All media storage shall be protected from accidental damage (e.g. water, fire, electromagnetic) and unauthorized physical access.

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

Full system backups sufficient to recover from system failure shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy of CA system shall be stored at an off-site location separate from the GovCA's equipment. The backup shall be stored at a site with physical and procedural controls commensurate to the operational controls of the CA.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one who performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible for their roles otherwise the integrity of the CA or RA is weakened. The functions performed in these roles form the basis of trust for all uses of the national certification scheme for digital signatures. Approaches shall be taken to increase the likelihood that these roles can be successfully carried out. The first shall ensure that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

PKI Manager	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

Two or more persons are required for GovCA for the following tasks:
1) CA key generation
2) CA signing key activation
3) CA private key backup

5.2.3 Identification and Authentication for Each Role

All individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Roles Requiring Separation of Duties

Role separation may be enforced either by the CA equipment, or procedurally, or by both means.

5.3 Personnel Security Controls

5.3.1 Background, Qualifications, Experience and Security Clearance Requirements

GovCA shall identify at least one individual or group responsible and accountable for the operation of the accredited CA. All persons 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 educational qualifications of Degree or Diploma in computer engineering, computer science or information and communications technology and any other related field;

iii. At least half of personnel shall have five (5) years' experience in the field of information security or operation and management of information and communications technology;
iv. Not an undischarged bankrupt person in the nation or elsewhere, or has made arrangement with his creditors;
v. Has not been convicted, whether in the nation or elsewhere, of an offense, the conviction for which involved a finding that he acted fraudulently or dishonestly;

5.3.2 Background Check Procedures

Personnel acting in trusted roles shall, at a minimum, undergo a background investigation procedure covering the following areas:

i. Employment
ii. Education
iii. Place of residence
iv. Law Enforcement
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 of PKI Policies, regulation and related laws.

In addition, personnel performing duties with respect to the operation of the CA shall receive comprehensive training or demonstrate competence in the following areas:

i. PKI policies, regulations and related laws.
ii. Basic Public Key Infrastructure (PKI) knowledge;
iii. CA/RA security principles and mechanisms;
iv. All PKI software versions in use by the CA systems; and
v. Disaster recovery and business continuity procedures
vi. Common threats to the validation process, including phishing and other social engineerig tactics.

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 responsible for PKI roles shall be aware of changes in the CA operation. Any significant

change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are software or hardware upgrade, changes in automated security systems and relocation of equipment.

Documentation shall be maintained identifying all personnel who received retraining and the level of retraining completed.

5.3.5 Job Rotation Frequency and Sequence

Any job rotation frequency and sequencing procedures shall provide for continuity and integrity of the CA's services.

5.3.6 Sanctions for unauthorized actions

GovCA employees failing to comply with this CP, 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 their 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

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:

i. System Access
ii. Physical Access
iii. Key generation
iv. Certificate Lifecycle
v. Transaction Logs
vi. System Logs Application Logs

All essential events auditing capabilities of the CA's operating system and applications required by this CP shall be enabled. As a result, the events identified above shall be automatically recorded. Where events cannot be automatically recorded, the CA shall implement manual procedures to satisfy this requirement.

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 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

The CA's system configuration and procedures must be implemented together to ensure that:

1) Only personnel assigned to trusted roles have access to the logs;
2) Only authorized people may archive audit logs; and,
3) Audit logs are not modified.

Procedures must be developed and 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 separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site on a monthly basis.

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 CP 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, the GovCA shall assess the vulnerability of its CA system or its components. A routine 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 ;

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

5.5.2 Period for Archive

The minimum retention periods for archive data shall be ten (10) years.

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to or delete the archive. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally authorized representative(s). Archive media shall be stored in a safe, secure storage facility separate from the GovCA itself.

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.

5.5.4 Archive Backup Procedures

If GovCA operating under this CP chooses to back up its archive records, GovCA shall store its archived records at a secure of-site location in a manner that prevents unauthorized modification, substitution, or destruction. 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.

5.6 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 CP 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 provide notice to the Root CA of any incident falling within the following requirements:

i. Compromise of CA's signing key;
ii. Penetration of CA's system and network;
iii. Unavailability of infrastructure; and
iv. 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

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

- Before returning to operation, ensure that the system's integrity has been restored
- 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.
- 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 CA Private Key Compromise Procedures

i. If the CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- 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 CA;
- A new key pair shall be generated by the CA; and
- New certificates shall be issued to subscribers also.

ii. If the CA 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 CP.

iii. The CA governing body shall also investigate and report to the Root CA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

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

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

5.8 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 are 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 is 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

CA key pair generation must create a verifiable audit trail that the security requirements procedures were followed. Subscriber key pair generation may be performed by the subscriber, CA or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 of this CP must also be met.

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

When key pairs are generated by the subscriber, the public key and the subscriber's identity must be delivered securely to GovCA or its RA for certificate issuance.

6.1.4 CA Public Key Delivery to Relying Parties

When GovCA updates its signature key pair, GovCA shall publish or distribute the new public key in a secure fashion.

6.1.5 Key Sizes

GovCA that generate certificates and CRLs under this CP shall use signature keys of at least 2048 bits for RSA.

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

6.1.6 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 CP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

GovCA is required to take all appropriate and adequate steps in accordance with the requirements of this CP to protect and prevent the loss, damage, disclosure, modification or unauthorized use of their private keys.

6.2.1 Cryptographic Module Standards and Controls

The HSM used by GovCA is required to meet at least level 2 of FIPS 140 in both the generation and maintenance of private keys.

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 CP.

6.2.3 Private Key Escrow

Private keys shall not be escrowed.

6.2.4 Private Key Backup

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

Subscribers may choose to back up their private keys by backing up 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 CP.

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.

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.

6.2.11 Cryptographic Module Rating

See section 6.2.1 of this CP.

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

GovCA shall not issue a certificate that extends beyond the expiration date of its own certificate and public key. Unless defined by GovCA, 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.

6.5 Computer Security Controls

CA and RA operating under this CP 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.

- Require authenticated logins
- Provide discretionary access control
- Provide a security audit capability
- Restrict access control to CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Archive audit data
- Require self-test security related services
- Require recovery mechanisms for keys and the CA system

6.6 Security 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.

6.6.4 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.

6.7 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 CP 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 its certificates.

7.1.6 Certificate Policy Object Identifier

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

7.1.7 Usage of Policy Constraints Extension

GovCA may assert policy constraints in CA certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP may contain policy qualifiers identified in RFC [3280/5280] as may be updated from time to time.

7.2 CRL Profile

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP profile

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

7.4 Version number(s)

No stipulation.

7.5 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 CP.

8.5 Actions taken as a result of deficiency

If an audit reports a material noncompliance with applicable law, this CP, or any other contractual obligations related to GovCA's services, 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 CP shall be allowed to charge fees for the issuance of certificates.

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 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 the CA.

9.1.3 Revocation or Status Information Access Fees

GovCA operating under this CP shall not charge any additional fees for accessing CRLs. Other revocation or status information may be charged for based on agreements with third parties.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation

9.3 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.

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 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.

9.4.1 Privacy Plan

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

9.4.2 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 CP shall not be released except as required by law or a court order.

9.4.3 Information Not Deemed Private

Information included in Section 7 of this CP is not subject to protection outlined in Section .4.2 above.

9.4.4 Responsibility to Protect Private Information

Confidential information must be stored securely and may be released only in accordance with the requirements of RA.

9.4.5 Notice and Consent to Use Private Information

Any disclosure of subscriber-specific information by GovCA or RA shall comply with the requirements of R.A, and must be authorized by the subscriber.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

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

9.6 Representations and Warranties

9.6.1 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 CP.
Identification and authentication procedures shall be implemented as specified in Section 3 of this CP.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

Subscribers of GovCA operating under this CP 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 CP.
iii. Promptly notify the appropriate CA/RA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through procedures consistent with the CA's CPS.
iv. Abide by all the terms, conditions and restrictions on the use of their private keys and certificates.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

9.8 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:

1) Revoked;
2) Expired;
3) Used for unauthorized purposes;
4) Tampered with;
5) Compromised; or

6) Subject to misrepresentation, misleading acts or omissions.

9.9 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:

- Any false or misleading statement of fact by the subscriber;
- Any failure by the subscriber to disclose a material fact, if such omission was made negligibly or with the intent to deceive;
- 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
- Any failure on the part of the subscriber to promptly notify the CA 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.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

The GovCA shall review this CP at least once a year. Corrections, updates or suggested changes to this CP 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.

9.12.2 Notification Mechanism and Period

Proposed changes to this CP 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 Dispute Resolution Provisions

Any dispute arising with respect to this CP or pertaining to the use and issuance of certificates, issued under this CP, shall be resolved amicably. Should the parties fail to resolve the issue, it may be submitted to controller or to competent court.

9.14 Governing Law

The issuance and use of certificates under this CP shall be covered by Law n°24/2016 of 18/06/2016 governing Information and Communication Technologies and any other applicable laws in Rwanda

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5 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:

1) Acts of God;
2) Acts of War;
3) Acts of Terrorism;
4) Epidemics;
5) Power or telecommunication services failure;
6) Earthquake;

7) Fire; or
8) Any other natural or man-made disasters.

9.17 Other Provisions

No stipulation.

10 DEFINITIONS AND ACRONYMS

10.1 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 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: is a **list** of **certificates** that have been **revoked** by the issuing **Certificate** Authority (CA) before their scheduled expiration date and should no longer be trusted.

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: Also reffered to as Root Certification Service Provider/ Controller 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.

10.2 Acronyms

CA: Certification Authority
CP: Certificate Policy
CPS: Certification Practice Statement
CRL: Certificate Revocation List
IETF: Internet Engineering Task Force
ISO: International Organization for Standardization
OID: Object Identifier
PKI: Public Key Infrastructure
PKIX: Public Key Infrastructure X.509 Working Group
RA: Registration Authority
RFC: Request for Comment
URL: Uniform Resource Locator
DN: Distinguished Name
HTTP: Hypertext Transfer Protocol
ITU: International Telecommunications Union
LDAP: Lightweight Directory Access Protocol
OCSP: Online Certificate Status Protocol
RootCA: Root Certification Authority
RSA: Rivest-Shamir-Adleman (encryption algorithm)
SHA: Secure Hash Algorithm
GovCA: Government Certification Authority

Done at Kigali, on 02/10/2018

(Sé)

Patrick NYIRISHEMA

Director General

Rwanda Utilities Regulatory Authority (RURA)