RWANDA UTILITIES REGULATORY AUTHORITY
P.O BOX 7289 KIGALI, Tel: +250 252584562
Email: info@rura.rw
Website: www.rura.rw

Certificate Policy (CP)

Ver. 1.0

2017

Contents

1. INTRODUCTION

1.1. Overview

This Certificate Policy (hereafter referred as CP) applies to Certification service providers issuing 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 a Government Certification service provider or private Certification service provider.

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: Rwanda Root Certification service provider - Certificate Policy (RCSP-CP)
Document Version: Version 1.0
Document Date: 30/08/2017

1.3. PKI Participants

Rwanda Utilities Regulatory Authority (RURA), as the accreditation and assessment body for certification service providers (CSPs).

1.3.1. Rwanda Root Certification Service Provider

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

1.3.1.1. Rwanda Root CSP obligations:

1. Operate and manage the Rwanda Root CSP system and its functions;
2. Issue and manage certificates for designated Government or Private CSPs;
3. Re-key of the Root CSP and approved CSP signing keys;
4. Establishment and maintenance of the CPS;
5. Provide technical expertise in the conduct of assessment of CSPs 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.

The Rwanda Root CSP is an off-line CSP.

1.3.1.2. Obligation of Certification service providers:

1. Operate and manage the CSP system and its functions in accordance to CSP policies, RCSP-CP and all applicable regulations;
2. Issue and manage certificates to natural person 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.

1.3.2. Registration Authority (RA)

The CSP may designate specific RAs to perform the Subscriber Identification and Authentication and certificate request and revocation functions defined in the CP 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 of certificates.

1.3.3. Subscribers

A subscriber is an individual or legal person 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.

1.3.4. 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.

1.3.5. Other Participants

CSPs and RAs operating under this CP 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 Usage

1. The Rwanda Root CSP certificate can be used for signing Certification service provider's OCSP, TSA and CRL's.
2. CSP certificates can be used for signing certificates, CRL's, OCSP and time stamp certificates as well as in the processes of verification of subject certificates and data.
3. Certificates issued by CSPs 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.

1.4.2. 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.

1.5. Policy Administration

1.5.1. Organization Administering This CP

The RCSP is responsible for all aspects of this CP and can be contacted at:
Controller of Certification Service Provider
C/o Rwanda Utilities Regulatory Authority
P. o. Box 7289, Kigali-Rwanda
Tel No: (+250) 252584562
Fax: (+250) 252 584563

1.5.2. Contact Person

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

1.5.3. Determining CP Suitability for the Policy

The CP is one of the assessment requirements by RCSP.
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

1.5.4. Approval Procedures

A Certification service provider operating under this CP shall follow the CP approval process issued by RCSP.

1.6. Definitions and Acronyms

All acronyms and abbreviations are found at:

Section 10 - Acronyms and Abbreviations

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

The Rwanda Root CSP is responsible for the publication of this CP and is publicly accessible at: http://rootca.rw/eng/laws/cps.php

All CSPs that issue certificates under this CP shall post all certificates 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 certificates and CRLs may be replicated in additional repositories for performance enhancement. Such repositories may be operated by the Certification service provider 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 at all times of the day, and on all days of every year;
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

A certificate can be published in repositories 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 seven (7) calendar days after its approval.

2.4. Access Controls on Repositories

All Certification service providers operating under this CP shall protect information not intended for public dissemination or modification. Certification service provider certificates and CRLs in the repository shall be publicly available through the Internet. The CPS for Certification service provider 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

Certification service providers operating under this CP shall only generate and sign certificates

that contain a non-null subject Distinguished Name (DN).
Each Certification service provider must have a unique and readily identifiable Distinguished Name according to the X.500 standard. Details of naming conventions for Certification service provider s are found in their respective Certificate Profiles.

3.1.2. Need for Names

Names used in the certificates must identify the Certification service provider 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

Certification service providers operating under this CP shall not issue anonymous certificates. Pseudonymous certificates may be issued under this CP to support internal operations.

3.1.4. Rules for Interpreting Various Name Forms

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

3.1.5. Uniqueness of Names

Name uniqueness must be enforced by Certification service provider s operating under this CP.

3.1.6. Name Claim Dispute Resolution Procedures

RCSP shall resolve any name collisions or disputes regarding any CSP-issued certificates brought to its attention.

3.1.7. 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.
In the case where key generation is under the Certification service provider or RA's direct control, then, proof of possession is no longer required.

3.2.2. Authentication of Organization Identity

Requests for Certification service provider certificates shall include the Certification service provider name, address and documentation of the existence of the organization.
Rwanda Root CSP 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 Certification service provider.
The applicant's information shall be verified with prior submission of the following:

1. For a government agency:
   -Official signed document/power of attorney;
2. For non-government entities:
   -Business registration number/ power of attorney;

3.2.3. Authentication of Individual Identity

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

1. Physical presence of the applicant;
2. Passport Photo attached on the application form;
3. Copy of National Identification Number (NID) or passport;
4. Power of attorney for legal persons
5. Tax Payer Identification Number (TIN); / business registration number
6. Phone number (mobile and/or landline);
7. E-mail address; and
8. Consent to verify the information submitted.
9. Foreigner authentication shall base on the best practices by Service Providers requirements.

3.2.4. Non-Verified Subscriber Information

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

3.2.5. Validation of Authority

Before issuing Certification service provider certificates or signature certificates that assert organizational authority, the Certification service provider shall validate the individual's authority to act in the name of the organization.

3.2.6. Criteria for Interoperation

The Rwanda Root CSP shall determine the criteria for cross-certification or mutual recognition of certificates issued by foreign Certification service providers.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Certification service provider certificate re-key shall follow the same procedure as that of initial key generation.

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 at all times of the day and on all days of the year; 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 Certification service provider certificate shall be submitted to the RCSP by an accredited Certification service provider or his representative using the procedure mentioned in Section 3 of this CP. The RCSP shall make the procedure available to all entities. The application shall be accompanied by a CP written in the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC3647].

4.1.1. Who can submit a Certificate Application

For Certification service provider certificate requests to the RCSP, an authorized representative of the accredited Certification service provider shall submit the request to the RCSP.

For end entity certificates, the accredited Certification service provider CPS shall describe the submission process.

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 Certification service providers operating 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. Certification service provider **actions during Certificate Issuance**

The Certification service provider and/or RA shall verify the identity and authority (for legal person) of a prospective subscriber before issuance of a certificate. The responsibility for verifying a prospective subscriber data shall be described in the Certification service provider's CPS. A certificate shall be checked to ensure that all fields and extensions are properly populated. After generation, verification and acceptance by the subscriber, the Certification service provider shall post the certificate in the repository system as specified in Section 2 of this CP.

4.3.2. Notification to Subscriber by the CSP/RA of Issuance of Certificate

Certification service providers or 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 Certification service provider or RA shall convey to the subscriber its responsibilities as defined in Section 9.6.3 of this CP.

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 Certification service provider.

4.4.2. Publication of the Certificate by the Certification service provider

As specified in Section 2 of this CP, all certificates can be published in the Certification service provider's repository system.

4.4.3. Notification of Certificate Issuance by the Certification service provider to Other Entities

A Certification service provider or RA operating under this CP may choose to notify other Certification service providers or RAs of the certificate issuance.

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. Certification service providers shall have their keys stored in Hardware Security Module (HSM). 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:

1. The appropriateness of the use of the certificate for any given purpose and that the use is not prohibited by this CP.
2. That the certificate is being used in accordance with its Key-Usage field extensions.
3. That the certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or Certificate Revocation List Checks.

4.6. Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed in order to reduce the size of CRLs. 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.

4.6.1. 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 revoked or compromised, and the subscriber name and attributes are unchanged. In addition, the validity period of the certificate must not exceed the remaining lifetime of the private key, as specified in Section 5.6. The identity proofing requirement listed in Section 3.3.1 shall also be met.

4.6.2. Who May Request Renewal

A subscriber or authorized representative may request for renewal directly with the Certification service provider or through the RA.

4.6.3. Processing Certificate Renewal Requests

The Certification service provider or RA shall process requests for renewal by verifying that the subscriber information has not changed. The Certification service provider or RA 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 these CP. Certification service providers or 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 Certification service provider.

4.6.6. Publication of Renewed Certificate

As specified in Section 2 of this CP, all renewed certificates issued can be published in the Certification service provider's repository system.

4.6.7. Notification of certificate issuance by the Certification service provider to other entities

No stipulation.

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 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 legal person directly with the Certification service provider or 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 follow the same processes and procedures as when initial keys were generated.

4.7.4. Notification of Certificate with New Keys to Subscriber

Certification service provider or RA 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 Certification service provider.

4.7.6. Publication of the Re-Keyed Certificate by the Certification service provider

As specified in Section 2 of this CP, all certificates can be published in the Certification service provider's repository system.

4.7.7. Notification of Certificate Issuance by the Certification service provider to Other Entities

No stipulation.

4.8. Certificate Modification

4.8.1. Circumstance for Certificate Modification

Modifying a certificate means creating a new certificate for the same subject with authenticated information that differs slightly from the old certificate (e.g., changes to email address or non - essential parts of names or attributes) provided that the modification otherwise complies with this CP.

The new certificate may have the same or a different subject public key. After modifying a client certificate, the Issuer Certification service provider may revoke the old certificate but may not further re-key, re-new or modify the old certificate.

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 legal person directly with the Certification service provider or RA. 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 Certification service provider or RA before the modified certificate is issued.

4.8.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6. Publication of the Modified Certificate by the Certification service provider

As specified in Section 2 of this CP, all certificates can be published in the Certification service provider's repository system.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9. Certificate Revocation and Suspension

Any request for certificate revocation or suspension must be authenticated. A Certification service provider 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.

There are several circumstances under which a Certification service provider certificate will be revoked:

1. Key Compromise - The Certification service provider's private key has been compromised.
2. Certification service provider Compromise - The Certification service provider database has been compromised
3. The Certification service provider is determined to be not being compliant with its CP/CPS.
4. Cessation of Operation - The Certification service provider shall cease operation.

A Certification service provider issuing certificates to end-entities will revoke the end-entity's certificate if:

1. The Certification service provider determines that its policy requirement is no longer being met by the subscriber.
2. An authenticated request is received by a Certification service provider or RA from an individual subscriber or an authorized representative of a legal person subscriber.
3. An authorized employee determines that an emergency has occurred that may impact the integrity of the certificates issued by the Certification service provider. 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 Certification service provider itself, a subscriber or the authorized representative of a legal person directly with the Certification service provider or RA.

4.9.3. Procedure for Revocation Request

The Certification service provider and/or RA shall verify the identity and authority (for legal person) of a subscriber making the request for revocation. The responsibility for verifying the revocation request shall be described in the Certification service provider's CPS.

4.9.4. Revocation Request Grace Period

All revocations shall be performed without any delay. 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 Certification service provider must process the revocation

request

A revocation request shall be processed without delay. A Certification service provider 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.

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

4.9.7. CRL Issuance Frequency (if applicable)

1. Rwanda Root CSP shall publish its updated CRL at least once every week.
2. Certification service providers shall publish its CRL at least once every twenty-four (24) hours.
3. Special purpose Certification service providers shall publish its CRL based on the importance to provide correct status information.

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. CRLs shall be published immediately after generation. Furthermore, each CRL shall be published no later than the time specified in the next Update field of the previously issued CRL. Certification service providers must issue CRLs at least once every 24 hours, and the next Update time in the CRL may be no later than 7 days after issuance time (i.e., this Update time).

4.9.9. On-Line Revocation/Status Checking Availability

Certification service providers 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

Any alternate forms used to disseminate revocation information may be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and on-line revocation and status checking.

4.9.12. Special Requirements Re-Key Compromise

No stipulation.

4.9.13. Circumstances for Suspension

The circumstances under which a certificate issued by a Certification service provider may be suspended are the following:

1. An authenticated request for certificate suspension is received by a Certification service provider or RA from an individual subscriber or an authorized representative of a legal person subscriber; and

2. The Certification service provider has reasonable grounds to believe that the certificate is unreliable, regardless of whether the subscriber consents to the suspension or not; but the Certification service provider 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

A Certification service provider or RA shall suspend a certificate after receiving a valid request from an individual subscriber or an authorized representative of a legal person 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 CP.

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:

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

In order to mitigate the threat of unauthorized person removing the certificate from hold, the subscriber identity shall be authenticated in person using initial identity proofing process described in Section 3.2.3.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

The certificate status validation service shall deliver 99.7% availability.

4.10.2. Service Availability

Both OCSP and CRL are to be made available by a Certification service provider.

4.10.3. Optional Features

No stipulation.

4.11. End of subscription

Certificates that have expired prior to or upon end of subscription are not required to be revoked.

4.12. Key Escrow and Recovery

No stipulation.

4.12.1. Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

5.1. Physical Security Controls

All Certification service provider equipment, including cryptographic modules, shall be protected from unauthorized access at all times.

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

5.1.1. Site Location and Construction

The location and construction of the facility housing the Certification service provider equipment, as well as sites housing remote workstations used to administer the Certification service provider 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 Certification service providers.

5.1.2. Physical Access

The Certification service provider equipment, to include remote workstations used to administer the Certification service provider 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:

1. Ensure that no unauthorized access to the hardware is permitted;
2. Be manually or electronically monitored for unauthorized intrusion at all times;
3. Ensure that an access log is maintained and inspected periodically;
4. Require two-person physical access control; and
5. 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

A Certification service provider 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 Certification service provider 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 Certification service provider shall implement reasonable precautions to prevent and extinguish. 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

All media storage shall be protected from accidental damage (e.g. water, fire, electromagnetic) and from unauthorized physical access. Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the Certification service provider location.

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 periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an off-site location separate from the Certification service provider's equipment. The backup shall be stored at a site with physical and procedural controls commensurate to the operational controls of the Certification service provider.

5.2. Procedural Controls

5.2.1. Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. Trusted roles are such that no conflict of interest is possible and the roles are distributed such that no single person can circumvent the security of the Certification service provider system.

The functions performed in these roles form the basis of trust for all uses of the Rwanda 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.

Security Officer	Having overall responsibility for administering the implementation of the security policies and practices.
System Administrator	Authorized to install, configure and maintain trustworthy 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	Authorized to view archives and audit logs of the trustworthy

	system.
Database Administrator	Has 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.
Registration Officer	Responsible for approving end entity Certificate generation, revocation, suspension, renewal and re-key.

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 Certification service providers for the following tasks:

1. key generation
2. signing key activation
3. private key backup

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

Physical access to the Certification service provider does not constitute a task as defined in this section. Therefore, two-person physical access control may be attained as required in Section 5.1.2. Sub-section 1.

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 shall be enforced either by the Certification service provider equipment, or procedurally, or by both means.

Individual Certification service provider personnel shall be specifically designated to the roles defined in Section 5.2.1 above. Individuals may assume more than one role, except:

1. Individuals who assume an Officer role may not assume an Administrator or Audit Administrator role;
2. Individuals who assume an Audit Administrator shall not assume any other role on the Certification service provider; and
3. 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 Security Controls

5.3.1 Background, Qualifications, Experience and Security Clearance Requirements

Each Certification service provider shall identify at least one individual or group responsible

and accountable for the operation of the accredited Certification service provider. 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 Rwanda citizens and in accordance with the following requirements:

1. 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 (ISO 17024) bodies such as, but not limited to ISACA, SANS and (ISC)2;

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

    a. Diploma in computer engineering, computer science or information and communications technology;
    b. Government-issued license in electronics engineering; or
    c. Certification in advanced courses on computer science, information and communications technology, electronics engineering or computer engineering and other related/special courses.

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

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

5. Has not been convicted, whether in the Rwanda or elsewhere, of an offense, the conviction for which involved a finding that he acted fraudulently or dishonestly;

5.3.2 Background Check Procedures

All Certification service provider personnel acting in trusted roles shall, at a minimum, undergo a background investigation procedure covering the following areas:

1. Employment
2. Education
3. Place of residence
4. Law Enforcement
5. 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 Certification service provider or RA shall receive comprehensive training in all operational duties they are expected to perform, including good knowledge on the following:

1. Basic Public Key Infrastructure (PKI) knowledge,
2. Software versions used by the Certification service provider,
3. Authentication and verification policies and procedures,
4. Disaster recovery and business continuity procedures,

5. Common threats to the validation process, including phishing and other social engineering tactics,
6. The Certification service provider's Certification Practice Statement;
7. Regulation governing certification authorities and
8. Certification service provider security principles and mechanisms;

The Certification service provider shall maintain records of who received training and what level of training was completed. Validation Specialists must have the minimum skills necessary to satisfactorily perform validation duties before they are granted validation privileges.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for PKI roles shall be aware of changes in the Certification service 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 be provided for continuity and integrity of the Certification service provider's services.

5.3.6 Sanctions for Unauthorized Actions

Appropriate actions shall be implemented where personnel have performed actions involving the Certification service provider or its repository not authorized in this CP, the Certification service provider's CPS or other procedures published by RCSP.

5.3.7 Independent Contractor requirements

Contractor personnel employed to perform functions pertaining to the Certification service provider or RA shall meet the personnel requirements set forth in this CP or the Certification service provider's CPS, as applicable.

5.3.8 Documentation Supplied to Personnel

For the Certification service provider and RA, documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the Certification service provider 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, and legible and made available during compliance audits.

5.4.1. Types of events recorded

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

manually for each auditable event):

For each event, the Certification service provider shall record the relevant

(i) date and time,
(ii) type of event,
(iii) success or failure, and
(iv) User or system that caused the event or initiated the action.

All event records shall be made available to auditors as proof of the CA's practices;

AUDITABLE EVENT
SECURITY AUDIT
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to assume a role
The value of maximum number of authentication attempts is changed
Maximum numbers of authentication attempts occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authe ntication attempts
An administrator changes the type of authenticator, e.g., from a password to a biometric
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by the system
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
KEY GENERATION
Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys)
PRIVATE KEY LOAD AND STORAGE
The loading of Component Private Keys
All access to certificate subject Private Keys retained within the CA for key recovery purpo ses
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE SECRET KEY ST ORAGE
The manual entry of secret keys used for authentication
PRIVATE AND SECRET KEY EXPORT
The export of private and secret keys (keys used for a single session or message are exclud ed)
CERTIFICATE REGISTRATION
All certificate requests, including issuance, re-key, renewal, and revocation Certificate issuance Verification activities
CERTIFICATE REVOCATION
All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL OR REJECTION CA CONFIGU RATION

Any security-relevant changes to the configuration of a CA system component
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
Generation of CRLs and OCSP entries
TIME STAMPING
Clock synchronization
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of an Operating System
Installation of a PKI Application
Installation of a Hardware Security Module
Removal of HSMs
Destruction of HSMs
System Start-up
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set passwords
Attempts to modify passwords
Backup of the internal CA database
Restoration from backup of the internal CA database
File manipulation (e.g., creation, renaming, moving)
Posting of any material to a repository
Access to the internal CA database
All certificate compromise notification requests
Loading HSMs with Certificates
Shipment of HSMs
Zeroizing HSMs
Re-key of the Component
CONFIGURATION CHANGES
Hardware
Software
Operating System
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
Personnel access to secure area housing CA components
Access to a CA component
Known or suspected violations of physical security
Firewall and router activities
ANOMALIES
System crashes and hardware failures

Software error conditions
Software check integrity failures
Receipt of improper messages and misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of a CP or CPS
Resetting Operating System clock

All security auditing capabilities of the Certification service provider'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 Certification service provider 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

A Certification service provider audit log shall be retained as a minimum during its total life time. Other 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 Certification service provider's system configuration and procedures must be implemented together to ensure that:

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

The off-site storage location for audit logs shall be a safe, 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 Certification service provider system. Automated audit processes shall be invoked at system or application start-up 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

Twice a year, the Certification service provider shall assess the vulnerability of its system or its components. A routine assessment of the system shall be performed regularly for evidence of any malicious activity.

5.5. Records Archival

All Certification service providers or RAs shall comply with their respective records retention policies.

5.5.1. Types of Records Archived

All Certification service providers shall retain the following information in its archives:

1. Any accreditation of the Certification service provider,
2. CP and CPS versions,
3. Contractual obligations and other agreements concerning the operation of the Certification service provider,
4. System and equipment configurations, modifications, and updates,
5. Certificate and revocation requests,
6. Identity authentication data,
7. Any documentation related to the receipt or acceptance of a certificate or token
8. Subscriber Agreements,
9. Issued certificates,
10. A record of certificate re-keys,
11. CRLs,
12. Any data or applications necessary to verify an archive's contents,
13. Compliance auditor reports,
14. Any changes to the Certification service provider's audit parameters,
15. Any attempt to delete or modify audit logs,
16. Key generation,
17. Access to Private Keys for key recovery purposes,
18. Changes to trusted Public Keys,
19. Export of Private Keys,
20. Approval or rejection of a certificate status change request,
21. Appointment of an individual to a trusted role,
22. Destruction of a cryptographic module,
23. Certificate compromise notifications,

5.5.2. Retention 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 Certification service provider 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 a Certification service provider operating under this CP chooses to back up its archive records,

the CPS or a referenced document shall describe how the records are backed up and managed.

5.5.5. Requirements for Time-Stamping of Records

Certification service provider archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6. Archive Collection System (Internal or External)

5.5.7. Procedures to obtain and verify Archive Information

The contents of the archive shall not be released except as determined by the RCSP, acting as the accreditation and assessment body or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their authorized representative(s).

5.6 Key Changeover

To minimize risk from compromise of a Certification service provider'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.

Certification service providers operating under this CP either must establish key rollover certificates as described above or must obtain a new Certification service provider 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

A Certification service provider shall provide notice to controller, of any incident falling within the following requirements:

1. Compromise of certification service provider's signing key;
2. Penetration of certification service provider'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, the accredited Certification service provider shall report it to controller 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 Certification service provider shall respond as follows:

1. Before returning to operation, ensure that the system's integrity has been restored
2. If the signature keys are not destroyed, the operation shall be re-established, giving priority to the ability to generate certificate status information within the CRL issuance schedule.

3. If the signature keys are destroyed, the operation shall be re-established as quickly as possible, giving priority to the generation of a new key pair.

5.7.3 Entity Private Key Compromise Procedures

1. If the Certification service provider signature keys are compromised or lost (such that compromise is possible even though not certain):

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

2. If the Certification service provider 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.
3. The Certification service provider governing body shall also investigate and report to the RCSP 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 Certification service provider directory system shall be deployed so as to provide 24 hours, 365 days per year availability.

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

5.8 Certification service provider Termination

In the event that a Certification service provider terminates its operation, it shall provide notice to controller, shall transfer its responsibilities and records to successor entities. The Certification service provider may allow a successor to re-issue certificates if the successor has all relevant permissions to do so. If no successor Certification service provider exists, all relevant records of the Certification service provider shall be transferred to a Root CSP or legal body.

6. TECHNICAL SECURITY CONTROLS

The Certification service provider private keys are protected within a hardware security module (HSM) meeting at least Level 3 of the Federal Information Processing Standard 140 (FIPS 140). Access to the HSM within the Certification service provider 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

Certification service provider 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, Certification service provider or RA. If the Certification service provider 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 a Certification service provider 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.

A Certification service provider 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 a Certification service provider or RA for certificate issuance.

6.1.4 CA Public Key delivery to Relying Parties

When a Certification service provider updates its signature key pair, a Certification service provider shall distribute the new public key in a secure fashion.

6.1.5 Key Sizes

Certification service providers shall follow NIST timelines in using retiring signature algorithms and key sizes.

Certification service providers that generate certificates and CRLs under this CP shall use signature keys of at least 2048 bits for RSA. All certificates, except self-signed certificates, that expires after 31 December 2030 shall be signed with keys of at least 3072 bits for RSA.

Certification service providers that generate certificates and CRLs under this CP shall use SHA-256, SHA-384 or SHA-512 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that are issued after 31 December 2030 shall be generated using, at a minimum, SHA-256.

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 CP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

All Certification service providers are 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 a Certification service provider is required to meet at least level 3 of FIPS 140 in both the generation and maintenance of private keys.

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

All Certification service provider 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 Certification service providers 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

Certification service provider 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

The maximum validity period for the certificate of Rwanda Root CSP shall be twenty (20) years while the certificate of a Certification service provider shall be for five (5) years. A Certification service provider 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) years.

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. A Certification service provider is also required to use strong passwords to further prevent unauthorized access to the Certification service provider 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

An RA shall follow the rules and guidelines issued by its corresponding Certification service provider for the information security requirements.

6.5.1 Specific Computer Security Technical Requirements

A Certification service provider 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.

1. Require authenticated logins
2. Provide discretionary access control
3. Provide a security audit capability
4. Restrict access control to Certification service provider services and PKI roles
5. Enforce separation of duties for PKI roles
6. Require identification and authentication of PKI roles and associated identities
7. Archive audit data
8. Require self-test security related services
9. Require recovery mechanisms for keys and the Certification service provider system

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls
No stipulation.

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 Certification service provider 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
All Certification service providers' components shall regularly synchronize with a time service. Time derived from the time service shall be used for establishing the time of:

1. Initial validity time of a Subscriber's Certificate
2. Revocation of a Subscriber's Certificate
3. Posting of CRL updates
4. OCSP responses

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable
Events as listed in Section 5.4.1.

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

7.1.2 Certificate Extensions
Certification service provider 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
The Certification service provider 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 Certification service provider as well as Certificate Policy.

7.1.7 Usage of Policy Constraints Extension
The Certification service provider may assert policy constraints in its certificates.

7.1.8 Policy Qualifiers Syntax and Semantics
Certificates issued under this CP 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)
Certification service provider operating under this CP shall issue X.509 version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions
Certification service provider 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.

7.3.1. Version Number(s)
No stipulation.

7.3.2. OCSP Extensions
No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS
An RA operating under this CP is required to perform regular self-audit in compliance with its contractual obligation with the public or Private Certification service provider.

8.1 Frequency or Circumstances of Assessment
At least once a year, a Certification service provider shall be subject to audit in respect with its accreditation by RCSP.

8.2 Identity/Qualifications of Assessor
The audit requirement shall be performed by a qualified independent assessment team organized by the RCSP comprising, but not limited to, the following:

1. Certified Public Accountants; and
2. Certified Information Security practitioners.

All shall possess sufficient knowledge on digital signatures, digital certificates, Internet X.509

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 Certification service provider being assessed and shall not be a software or hardware vendor that is or has been providing services or supplying equipment to the Certification service provider within the last two (2) years.

8.4 Topics covered by assessment

A Certification service provider shall undergo an initial assessment covering the following:

1. Document review of the CPS in order to verify if the applicant Certification service provider addresses all the requirements of the relevant standards and RCSP requirements;
2. Pre-assessment visit which shall include all other premises of the Certification service provider from which one or more key activities are performed such as:

    a) policy formulation;
    b) process and/or procedure development;
    c) contract review;
    d) planning conformity assessments, review, approval and decisions; and
3. Follow-up visit, when required, to verify corrective actions on any non-conformity findings.

8.5 Actions taken as a result of Deficiency

Any corrective action undertaken to rectify any deficiency noted shall be verified.

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

Certification service provider operating under this CP shall be allowed to charge fees for the issuance of certificates.

9.1.1 Certificate issuance or renewal fees

Certification service providers may set any reasonable certificate issuance and renewal fees.

9.1.2 Certificate access fees

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

9.1.3 Revocation or Status Information Access Fees

A Certification service provider 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

Certification service providers may set any reasonable fees for any other services such as access to archive records or key recovery.

9.1.5 Refund Policy

Certification service provider may, but are not required to, have a documented refund process.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

A Certification service provider operating under this CP shall be insured against liabilities for damages.

9.2.2 Other Assets

Certification service providers shall also maintain reasonable and sufficient financial resources to maintain operations, fulfil duties, and address commercially reasonable liability
Obligations to PKI Participants described in Section 1.3 of this CP.

9.2.3 Insurance or Warranty Coverage for End-Entities

Certification service providers may, but are not required to offer protection to end entities that extends beyond the protections provided in this CP. Any such protection shall be offered at commercially reasonable rates.

9.3 Confidentiality of Business Information

Information about the Certification service provider 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.

Certification service provider shall maintain the confidentiality of confidential business information that is clearly marked or labelled as confidential or by its nature should reasonably be understood to be confidential, and shall treat such information with the same degree of care and security as the licensed Certification service provider treats its own most confidential information.

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

A Certification service provider shall keep all subscriber-specific information confidential except as required by law or pursuant to an order of court.

9.4.1 Privacy Plan

A Certification service provider shall have a Privacy Plan to always protect personally identifying information from unauthorized disclosure.

9.4.2 Information Treated as Private

A Certification service provider 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 a Certification service provider 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 9.4.2 above.

9.4.4 Responsibility to Protect Private Information

The Certification service provider is responsible for securely storing and protecting private information.

9.4.5 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. A Certification service provider may only use private data after obtaining the subject's express written consent or as required by applicable law or regulation.

9.4.6 Disclosure pursuant to Judicial or Administrative Process

A Certification service provider 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 a Certification service provider.

9.6 Representations and Warranties

9.6.1 Certification service provider representations and Warranties

A Certification service provider 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 a Certification service provider operating under this CP shall agree to the following:

1. Accurately represent themselves in all communications with the PKI authorities.
2. Protect their private keys at all times, in accordance with this CP.
3. Promptly notify the appropriate Certification service provider upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through procedures consistent with the Certification service provider's CPS.
4. 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

A Certification service provider assumes no liability except as stated in the relevant contracts pertaining to certificate issuance and management.

9.8 Limitations of Liability

A Certification service provider 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 a Certification service provider 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 a Certification service provider or RA harmless from any claims, actions or demands that are caused by the use or publication of a certificate and that arises from:

1. Any false or misleading statement of fact by the subscriber;
2. Any failure by the subscriber to disclose a material fact, if such omission was made negligibly or with the intent to deceive;
3. 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
4. Any failure on the part of the subscriber to promptly notify the Certification service provider 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 controller and its publication in the Root CSP Repository of documents in its website.

9.10.2 Termination

While this CP may be amended from time to time, it shall remain in force until it is amended or replaced by a new version or explicitly terminated by controller.

9.10.3 Effect of Termination and Survival

Upon termination of this CP, Certification service provider is nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates.

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

Unless otherwise specified by agreement between the parties, accredited Certification service provider shall use reasonable methods to communicate, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

RCSP shall review this CP at least once a year. Corrections, updates or suggested changes to this CP shall be communicated to every Certification service provider. 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 Certification service providers and other bodies/entities formed to oversee the implementation of the National Public Key Infrastructure. The notification shall contain the final date for receipt of comments and the proposed effective date of change.

9.12.3 Circumstances under which OID must be changed

No stipulation.

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 laws of Rwanda and more particularly the law No 24/2016 of 18/06/2016 governing Information and Communication Technologies, 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 CP.

9.15 Compliance with Applicable Law

A Certification service provider is required to comply with any applicable laws.

9.16. Miscellaneous Provisions

No stipulation.

9.16.1. Entire Agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3 Severability

If any provision of this CP is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.

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

No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CP are for convenience only and cannot be used in interpreting this CP.

9.16.5 Force Majeure

RCSP, any Certification service provider or 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. ACRONYMS AND ABBREVIATIONS

CP: Certificate Policy
CPS: Certification Practice Statement

CRL: Certificate Revocation List
IETF: Internet Engineering Task Force
ISO: International Organization for Standardization
NIST: National Institute of Standards and Technology
OID: Object Identifier
PKI: Public Key Infrastructure
PKIX: Public Key Infrastructure X.509 Working Group
RA: Registration Authority
RFC: Request for Comment
RRCA: Rwanda Root Certification Authority
Root CSP: Root Certification service provider
RURA: Rwanda Utilities Regulatory Authority
URL: Uniform Resource Locator

Done at Kigali, on 30/08/2017

(Sé)

Eng. Coletha U. RUHAMYA
Chairperson of the Regulatory Board