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

Certification Practice Statement (CPS)

Ver. 1.0

2017

Contents

1. Outline

1.1. Background & Purpose

1.1.1. Electronic Signature Certification System

"Law Nº 24/2016 of 18/06/2016 governing Information and Communication Technologies" aims to promote an information-oriented society and improving convenience for citizens by specifying basic items regarding the establishment and operation of an electronic signature certification management system. This is to ensure the security and reliability of electronic data which are processed via open information networks, such as the Internet. The law gives Rwanda Utilities Regulatory Authority (RURA) the power to be the Controller of Certification service providers in Rwanda.

The Controller shall license Certification service providers and exercise supervision over their activities. It is required to certify their public keys, lay down the standards to be maintained and perform several other functions to regulate the functioning of certification service providers in the country.

1.1.2. Purpose of Certification Practice Statement

The Certification Practice Statement (CPS) of the controller states how the PKI component(s) meet the assurance requirements defined in the Certificate Policy (CP) and also security control and operational policy & procedures and other matters relevant to obligations and responsibilities of the controller and Certification Service Providers in accordance with relevant Law and Regulations. It describes the practice used in issuing and managing the public key infrastructure.

This CPS is based on the RFC 3647- Internet X.509 PKI Certificate Policy and Certificate Practice Framework.

1.1.3. Certification Practice Related Contact Information

Controller's certification practice related contact information is as follows.

- URL: http://www.rootca.rw
- E-mail: rootca@rura.rw
- Address: P. O. Box 7289, Kigali-Rwanda
- Telephone: (+250)252584562

1.1.4. Certification Practice Related Information

The controller's certification practice related information is as follows.

- The controller's Certification Practice Statement: http://rootca.rw/eng/laws/cps.php
- certification service providers List: http://rootca.rw/eng/service/ca_list.php
- Certificate List: http://rootca.rw/eng/service/certificate.php
- Certificate Revocation List: http://rootca.rw/eng/service/arl.php

1.2. Name of Certification Practice Statement

This document is named 'Certification Practice Statement of controller for Rwanda Public Key

Infrastructure.

1.3. PKI Participants

1.3.1. Controller as a Root Certification Service Provider (RCSP)

The Rwanda Root CSP is the primary trust point for the entire PKI architecture. Controller shall carry out its duties and roles as a top-level certification service provider in the electronic signature certification management system, including the following:

- Operate as an offline Root CSP.
- Operate in accordance with this CPS.
- Accept certificate signing requests from authorized representative of Licensed CSP
- Issue Public Key certificates to the licensed CSPs.
- Accept the revocation request from the authorized representative of Licensed CSPs.
- Immediately publish the CRL after revocation of Licensed CSP.
- Preserve audit logs and certificate issuance process.
- Issuing the Authority Revocation List (ARL)
- Time-stamping
- International cooperation and support, such as cross-recognition, etc.
- Performing investigations for the designation of certifying authorities
- Inspecting certification authorities, and supporting their secure operation

1.3.1.1. Provision and Notification of Correct Information

The Root Certification Service Provider shall notify certification Service Providers and the relying parties the Information that may have an effect on the reliability or validity of a certificate, so that it can be confirmed by anyone under the electronic signature certification system.

1.3.1.2 Countermeasures to Improper Electronic Signature Creation Keys

If the Root Certification Service Provider is notified by a Certification Service Provider that electronic signature creation keys are lost, damaged, stolen, leaked, or weak, the RCSP shall revoke the certificate that was issued to the appropriate Certification Service Provider and then will promptly announce the fact so that it can be easily confirmed by anyone in the certification management system.

1.3.1.3 Countermeasures to Vulnerability in the Electronic Signature Algorithm

If the Root Certification Service Provider is notified of vulnerability in the electronic signature algorithm by a Certification Service Provider, the RCSP shall revoke the certificate which was issued to the appropriate Certification Service Provider, and then shall promptly announce the fact so that it can be confirmed by anyone in the certification management system and shall consider countermeasures for ensuring the security and reliability of certification practice.

1.3.2 Certification Service Provider (CSP)

A Certification Service Provider is a national agency, local autonomous entity, or corporation that has been designated/accredited/licensed by the controller in accordance with the regulation Governing Certification Service Providers**.**

The Licensed Certification Service Providers (CSPs) s must:

- Protect their private key in a secure manner.
- Have CPS approved by RCSP
- Perform the Certification Service Provider operation as per the RCSP's CP, CPS
- Update the CPS when the RCSP's CP policy change or in accordance with the RCSP guidelines
- Publish a name and contact information of the party responsible for this Licensed Certification Service Provider (CSP)
- Maintain a web site and publish subscriber certificates and CRLs.
- Should revoke all the certificates to subscribers and publish the CRL immediately in the case of compromise of their signing key and this may be reported to RCSP immediately
- Identity check
- Issuing a certificate
- Certificate suspension and revocation
- Renewing a certificate
- Giving public notification of certificate-related information
- Time-stamping

1.3.3. Registration Authority (RA)

The Certification Service Provider may designate specific RAs to perform the Subscriber Identification and Authentication and certificate request and revocation functions defined in the CP and related documents. RA has an important role to identify a user for certificate by face-to-face.

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. Keep related document safely which is required to issue certificate
3. Transmit the certificate request to the Certification Service Provider;
4. Validate certificates from the CSP Directory Server and CRL; and
5. Request revocation of certificates.

1.3.4. Subscribers

A subscriber is an individual, entity 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.

1.3.5 Relying Party

Relying parties are parties that rely on and use certificates issued by the RCSP, and include the following:

- Certification Service Provider Subscribers to Certification Service Provider

- Foreign Certification Service Providers which have entered into a cross-recognition arrangement
- Subscribers to foreign Certification Service Providers which have entered into a cross-recognition arrangement

1.3.5.1 Understanding the Purpose of Using Certificates

A relying party shall understand the purpose of using a certificate issued by the RCSP, as specified in 2.1.2 Scope and Usage of Certificates in this Certification Practice Statement.

1.3.5.2 Certificate Verification

A relying party shall verify the appropriate certificate's validity period, scope and usage, authenticity before using the certificate.

1.3.5.3 Verification of Certificate Suspension and Revocation

A relying party shall verify the validity of the appropriate certificate via the certificate suspension and revocation list before using the certificate.

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 RCSP certificate can be used for signing CA's, OCSP, TSA and CRL's.
2. Certification Service Provider certificates shall be used for signing subscriber's 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 shall 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 use of the certificate for any given purpose and that the use is not prohibited by this CPS.
2. The certificate is being used in accordance with its Key-Usage field extensions.
3. The certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or Certificate Revocation List Checks.

1.4.2. Prohibited Certificate Usage

All certificates issued under this CPS cannot be used for purposes other than what is allowed in Section 1.4.1 above.

1.5. CPS Administration

1.5.1. Organization administering this document

The controller is responsible for all aspects of this CPS 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
Controller of Certification Service Provider
C/o Rwanda Utilities Regulatory Authority
P. o. Box 7289, Kigali-Rwanda
Tel. No : (+250)252584562
E-mail: rootca@rura.rw

1.5.3. Certification Practice Statement Management

This CPS is subject to a regular review process that strives to take into consideration developments in international PKI standardization initiatives, development in technology and information security, as well as other relevant issues.

1.5.3.1 Revision Procedures

If the controller of certification service provider judges that the Certification Practice Statement needs to be changed, the Certification Practice Statement shall be revised.

The RCSP shall maintain and manage documents related to the revision of the Certification Practice Statement, which shall include the following:

- Certification Practice Statement versions
- Outlines of the practice and scope related with the revision
- Documents on the revision of Certification Practice Statement
  - Revised provisions in the existing Certification Practice Statement
  - Revision details
  - Reasons for revision.

1.5.3.2 Enforcement Procedures

The RCSP shall announce the established or revised Certification Practice Statement in '1.1.4 Certification Practice Related Information' of this Certification Practice Statement, and shall individually notify certification service providers of the fact of its establishment or revision.

The established or revised Certification Practice Statement shall become effective on the date of reporting.

1.6 Definitions & Abbreviations

DN (Distinguished Name)
A type of name that is used to identify the authority that issued a certificate and the owner of a certificate.

Subscriber
A subscriber is an individual or legal person whose name appears as the subject in a certificate

issued by a certification authority.

Certification service provider (CSP)
An authority that provides certification services after being licensed by the controller.

Relying Party
A person or an entity that relies on and uses appropriate certificate issued by a certification service provider.

Identity Check
The act of checking the authenticity of a certification service provider, an applicant, and information for ensuring the reliability of a certificate when a certificate is issued, renewed, suspended, or revoked.

Real Name
The name on a national ID/passport or equivalent document for an individual, or name on a certificate for business registration.

Certification
An act of verifying the fact that electronic signature verification keys agree with the electronic signature creation keys owned by a natural person or corporation.

Electronic Signature Certification System
A system for providing certification services, including the issue of a certificate, the management of certification-related data, etc.

Electronic Certificate
Electronic data verifying the fact that electronic signature verification keys agree with the electronic signature creation keys owned by a natural person or corporation.

Certification Practice
Practice of providing certification services, including the issue of a certificate, the management of certification-related data, etc.

Electronic Data
Information that is generated, sent and received, or stored in an electronic form by the use of data-processing devices, such as a computer, etc.

Digital Signature
Refer to the mathematical scheme for demonstrating the authenticity of a digital message or document.

2. Certificate Service Fees

2.1 Fees for the Issue, Reissue and Renewal of Certificates

If necessary, the controller may impose fees on certification service providers that apply for the issue, reissue and renewal of certificates.

2.2 Certificate Access Fee

The RCSP shall not impose any fee on a relying party that reads and checks certificates.

2.3 Certificate Revocation List Access Fee

The RCSP shall not impose any fee on a relying party that accesses the certificate suspension and revocation list.

2.4 Fees for Other Services

If necessary, the RCSP shall impose fees for other services.

3. Issue of Certificates and Certification Practice

3.1 Application for the Issue of Certificates

A certification service provider shall access the RCSP's website to receive necessary data and a form, or the same shall be directly issued, filled out, and then the certification service providers shall directly visit the controller for application.

3.1.1 Use of Names

Each CSP Applicant must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subjectName field.

Technical standards shall apply to the names used for basic areas in a certificate, certificate suspension and revocation list.

Authority names or corporation names shall be used for DNs in a certificate issued by the RCSP.

3.1.2 Need for names to be meaningful

The Subject name contained in a certification service provider certificate must be meaningful in the sense that the RCSP is provided with proper evidence of the association existing between the name and the entity to which it belongs.

3.1.3 Uniqueness of Names

The RCSP shall ensure that the set of names is unambiguous. The name shall conform to X.500 standards.

3.1.4 Information on the Issued Certificates

A certificate issued by the RCSP shall include the following items, in accordance with the regulation governing certification service providers:

- Name of certificate authority
- Certificate authority's electronic signature verification keys
- Electronic signature type used by the RCSP and certification service providers
- Certificate serial numbers
- Certificate validity period
- Name of the RCSP as a top-level certification service provider
- Relevant matters in the event that the scope or usage of a certificate is restricted

3.1.5 Certificate Validity Period

The RCSP shall determine the proper certificate validity period by considering the scope and

usage of a certificate and the security and reliability of the relevant technology, in accordance with the regulation governing certification service providers.

- The validity period of the RCSP's certificates shall be within 20 years.
- The validity period of the certificates for certification service providers issued by the RCSP are as follows.

Classification	Key Length (2048bit)
Certification service provider's Certificate	Within 5 years
Time-Stamping Certificate	Within 5 years
OCSP Certificate	Within 5 years

3.1.6 Receipt of Certificates

A certification service provider shall receive its certificates in person at the RCSP, or through an information communication network after the notification certificate issuance. A certification service provider can use its received certificates beginning on their date of validity.

3.2 Issuance of new Certificates

To establish that the applicants possess valid functioning key pairs, RCSP would require applicants to submit a Certificate Signing Request (CSR) in accordance with the PKCS#10 standard. The signing key pair of the Licensed CSP shall be stored in FIPS 140-1 level 3 or higher level device. An independent verification may be performed as a part of the auditing process.

3.2.1 Procedures for New Issuance

Before issuing a new certificate, the RCSP shall verify the following details of an application:

- The uniqueness of the electronic signature verification keys submitted by an applicant for a certificate
- The agreement of the electronic signature verification keys submitted by an applicant for a certificate with the appropriate certification service provider's own electronic signature creation keys.
- The uniqueness of a DN submitted by an applicant for a certificate.

3.3 Renewal of Certificates

3.3.1 Identity Check for Renewal

If a certification service provider applies for the renewal of a certificate, the RCSP shall conduct an identity check in accordance with the procedures involved in an application for the new issue of a certificate.

3.3.2 Renewal Procedures

Before the actual issue, the RCSP shall verify the following details of the application for the

renewal of a certificate;

- The uniqueness of the electronic signature verification keys submitted by an applicant for a certificate.
- The matching of the DN submitted by an applicant for a certificate to the DN stated in a previous certificate.

It should be noted that certification service providers cannot apply for the renewal of certificates with the same electronic signature creation keys.

3.4 Reissue of Certificates

3.4.1 Identity Check in Reissue

If a certification service provider applies for the reissue of its own certificate because its validity period has expired or the certificate has been revoked, the RCSP shall conduct an identity check in accordance with the procedures for an application for the new issue of a certificate.

3.4.2 Reissue Procedures

RCSP shall verify the following details of an application for the reissue of a certificate before reissuing it:

- The uniqueness of the new electronic signature verification keys submitted by the applicant for a certificate
- The agreement of the new electronic signature verification keys submitted by the applicant for a certificate with the appropriate certification service provider's own electronic signature creation keys.
- The uniqueness or identity of a DN submitted by an applicant for a certificate.

3.5 Change of Subscriber Registration Information

This is not applicable.

3.6 Suspension, Revival, and Revocation of Certificates

3.6.1 Identity Check in Application for Suspension, Reactivation, or Revocation

If a certification service provider applies for the suspension, re-activation or revocation of a certificate, RCSP shall conduct an identity check in accordance with the procedures for the application for the new issue of a certificate.

3.6.2 Certificate Suspension

3.6.2.1 Reasons for Certificate Suspension

If a certification service provider applies for the suspension of a certificate, RCSP shall suspend its certificate in accordance with the regulation governing certification service providers.

3.6.2.2 Applicant for Certificate Suspension

A certification service provider can apply for the suspension of its certificates.

3.6.2.3 Submission of an Application for Certificate Suspension

A certification service provider can submit an application for certificate suspension by visiting RCSP in person after filling out the necessary items in the application for certificate suspension provided by RCSP, or may submit an application for certificate suspension that has been

electronically signed to the RCSP using an information communication network.

3.6.2.4 Renewal and Notification of Certificate Revocation List

RCSP shall renew the certificate revocation list and promptly announce the fact of its renewal so that it can be easily confirmed by anyone through the certification management system.

3.6.3 Certificate Re-activation

3.6.3.1 Applicant for Certificate Re-activation

A certification service provider can apply for the re-activation of its suspended certificates.

3.6.3.2 Submission of an Application for Certificate Re-activation

A certification service provider shall fill out the necessary items in an application for certificate re-activation that is provided by RCSP, and then submit it to RCSP via direct visit.

3.6.3.3 Notification of Certificate Re-activation

RCSP shall promptly announce certificate re-activation, so that the fact can be easily confirmed by anyone through the certification management system.

3.6.3.4 Time Limit for Application for Certificate Re-activation

A certification service provider shall apply for certificate reactivation within six months from the date of certificate suspension, in accordance with the regulation governing certification service providers.

3.6.4 Certificate Revocation

3.6.4.1 Reasons for Certificate Revocation

RCSP shall revoke a certification service provider's certificates in accordance with the regulation governing certification service providers, if any of the following reasons occurs:

- If a certification service provider applies for certificate revocation;
- If RCSP recognizes that a certification service provider has certificates issued in deception, forgery or other through illegal methods;
- If RCSP recognizes that a certification service provider has been dissolved;
- If RCSP recognizes that a certification service provider's electronic signature creation keys have been lost, damaged, stolen or leaked.

If RCSP is notified of vulnerability in the electronic signature creation keys by a certification service provider, it shall revoke the appropriate certification service provider's certificates in accordance with the regulation governing certification service providers.

If RCSP is notified of vulnerability in the electronic signature algorithm by a certification service provider, it shall revoke the appropriate certification service provider's certificates in accordance with the regulation governing certification service providers.

3.6.4.2 Applicant for Certificate Revocation

A certification service provider can apply for the revocation of its own certificates.

3.6.4.3 Submission of an Application for Certificate Revocation

A certification service provider shall fill out all necessary items in an application for certificate revocation provided by RCSP, and then shall submit it to the RCSP via direct visit.

3.6.4.4 Renewal of Certificate Revocation List and Notification

If a reason for certificate suspension or revocation occurs, RCSP shall promptly issue

certificate suspension or revocation list for the certificate.

The RCSP shall renew the certificate revocation list and promptly announce the fact of its renewal so that it can be easily confirmed by anyone through the certification management system.

3.6.4.5 Certificate Revocation Delay Period

RCSP shall not have any delay period for handling certificate revocation. If the legitimacy of a reason for certificate revocation is verified, RCSP shall promptly revoke the appropriate certificate.

3.7 Other Additional Services

RCSP can provide other additional services, such as time-stamping, OCSP services, if applicable.

3.8 Certificate Profile

RCSP shall issue and announce certificates conforming to the standards for X.509 Version 3 Certificate.

3.9 Certificate Revocation List (CRL) Profile

RCSP shall create and announce a certificate revocation list conforming to the standards for X.509 Version 3 Certificate Revocation List.

In the event of the suspension of certificates, RCSP shall show that an appropriate certificate has been suspended using the field for revocation reason code in the zone for the expansion of certificate revocation list.

3.10 Renewal of Electronic Signature Keys

RCSP shall create new electronic signature keys to issue certificates before the validity period of its certificates has expired.

A certification service provider shall create new electronic signature keys to apply for the renewal of certificates before the validity period of its certificates has expired.

4. Announcement of Information Related to Certification

4.1 Announcement System

RCSP shall announce the information related to the issue and management of certificates, so that these can be confirmed by anyone through the certification management system.

4.2 Announcement Method

RCSP shall handle the information related to the issue and management of certificates, and shall promptly announce the same, so that these can be confirmed by anyone through the certification management system.

5. Certification Practice System and Equipment Protection Measures

5.1 Physical Protection Measures

5.1.1 Physical Access Control

All sites where a certification system is installed shall be protected from all physical risks, such as the intrusion of an outsider, illegal access, etc.

The certification system shall be installed and operated in a separate restricted area, in the

corresponding system inside a security cabinet to enable physical access control.

Certification system shall be controlled using a monitoring control system, such as a CCTV camera, a monitoring system, an intrusion detection system, etc., which has a warning function to prepare against any abnormal situation.

The entry control system shall control access to a restricted area through a multi-level identification that combines an identity check card, a fingerprint identification system and weight detection device, etc.

5.1.2 Power Supply

Certification system shall use an uninterruptible power supply to prevent serious damage in the event of sudden power failure.

5.1.3 Flood Control

Certification system shall be installed away from the floor to ensure that it is protected in the event of a flood.

5.1.4 Fire Prevention

A fire detector, a portable fire extinguisher, and automatic extinguishing equipment, shall be installed in a certification system laboratory.

5.1.5 Storing Media

Physical access shall be controlled by storing the main storing and recording media in a safe.

5.1.6 Waste Handling

Documents, diskettes, etc. shall be physically destroyed if necessary.

5.1.7 Off-Site Backup

RCSP shall physically back up Off-site areas with certificates, certificate revocation list, etc. issued by RCSP, which it shall retain for at least 10 years after the appropriate certificate has expired.

5.2 Procedural Protection Actions

5.2.1 Work Classification by Role

RCSP shall classify certification practice according to role to ensure its security and reliability.

5.2.2 Personnel by Main Work

The creation of keys shall be carried out jointly by at least three persons, and other certification practices shall be carried out jointly by at least two persons.

5.3 Technical Protection Actions

5.3.1 Creation of Electronic Signature Keys

Only the authorized persons shall be allowed to create electronic signature keys.
RCSP shall create electronic signature keys in a security module that is protected from physical intrusion, which is not connected to internal and external information communication networks, and which satisfies a secure key creation system or the technical standards.

5.3.2 Key Size and Hash Value

Rwanda Certification system shall use the following key size and hash value to use a secure and reliable electronic signature algorithm:

- RSA: Over 2,048 bits
- SHA-2: Over 256 bits

5.3.3 Device for Storing Electronic Signature Creation Keys

The electronic signature creation keys shall be securely stored and managed using a security module that satisfies the technical standards, so that the electronic signature creation keys are not lost, damaged, stolen or leaked.

5.3.4 How to Delete and Destroy Electronic Signature Creation Keys

If RCSP's certificate expires, or if its electronic signature creation keys are damaged and/or leaked, it shall completely destroy the corresponding medium for storing the electronic signature creation keys, or shall delete the electronic signature creation keys in accordance with the technical standards.

5.3.5 Electronic Signature Creation Keys Use Period

RCSP's electronic signature creation keys and those of a certification service provider can be used only for the corresponding certificate validity period.

5.3.6 Computer and Network Security Control

The intrusion detection system and intrusion prevention system shall be used to ensure network security.

5.4 Personnel Security

Among RCSP's personnel who manage electronic signature management system, the director and security manager of a certification management centre shall hold a second-class certificate for security clearance.

5.5 Audit Data

5.5.1 Types of Cases in Audit Data

The cases occurring in a system (hereinafter called as "certification system") that supports registration information management, the creation and management of electronic signature keys, the creation and issue of certificates, and time-stamping shall be recorded.

5.5.2 Review and Protection of Audit Data

RCSP shall designate a staff member as an audit manager in accordance with its internal regulations of certification practice, and the designated audit manager shall review and archive audit data.

The audit data of each system shall be managed by an audit manager, and each person who manages a system can read only the audit data of the appropriate practice.

5.5.3 Notification of the Occurrence of Incidents

If a security violation incident occurs, notification of such shall promptly be given to the person in charge.

5.6 Archiving

5.6.1 Types of Objects for Archiving

RCSP shall record and archive the data related to the following practice:

- Certification practices, including the issue and management of the certificates held by certification service providers
- Other practices, including the operation of the RCSP's key certification system, etc.

5.6.2 Protection of Archives

RCSP shall designate a staff member as a data manager in accordance with its internal regulations of certification practice, and the designated data manager shall manage all archives, while other managers can search only the archives within their work scope.

To prevent archives from being forged and/or damaged, RCSP shall protect archives as follows:

- Securely retaining electronic data after it has been electronically signed
- Keeping general documents in a cabinet that has a lock mounted

5.7 Recovery from Glitches and Disasters

5.7.1 Countermeasures in the event of the Occurrence of Glitches in System Sources and Software

If a glitch occurs in a system source, software, etc., the system shall recover the same by using double-installed system sources and software.

5.7.2 Countermeasures in the event of Damaged and/or Destroyed Data

If main data such as certification service providers ' certificates are damaged or destroyed, RCSP shall recover the same using archived data.

6. Miscellaneous Provisions, Including Certification Practice Guarantee

6.1 Guarantee

6.1.1 Liability for Guarantee

RCSP shall guarantee the following in connection with the certificates that it issues:

- The accuracy of the contents of an issued certificate
- The fact that certificates have been issued in accordance with the provisions of the regulation governing certification service providers
- The accuracy of the details of Certificate Revocation

6.1.2 Exemptions

RCSP shall not be liable for any damage caused by reasons not prescribed in the regulation governing certification service providers, or any damage caused by the delay or impossibility of certification practice treatment due to reasons beyond human control, such as wars, natural disasters, etc.

6.2 Dispute Resolution

6.2.1 Observance Laws

This Certification Practice Statement shall be interpreted and applied in accordance with the laws of Rwanda and more particularly the law n°24/2016 of 18/06/2016 governing Information and Communication Technologies, Regulation governing certification service providers and the guidelines issued and clarifications made from time to time by RCSP shall govern the construction, validity, enforceability and performance of actions per this CPS.

6.2.2 Jurisdiction

Rwanda Competent Court shall be designated for the resolution of disputes related to certification practice between RCSP and a certification service provider or relying party whenever the parties fail to resolve the issue amicably.

6.2.3 Dispute Mediation

Any dispute arising with respect to this CPS or pertaining to the use and issuance of certificates, issued under this CPS, shall be resolved amicably. Should the parties fail to resolve the issue,

it may be submitted to RCSP or to competent court.

6.3 Private Information Protection

A top-level certification service provider shall conform to the regulation governing certification service providers for the protection of the private information related to the performance of certification practice.

6.4 Audit and Check

6.4.1 Security Check

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

6.5 Observance of Relevant Laws

In accordance with copyright laws and other relevant laws, the intellectual property rights of the following shall belong to the RCSP:

- Software and hardware developed by RCSP
- RCSP's Certification Practice Statement
- RCSP's names
  - Corporations' names
  - Internet domain names
- Electronic signature keys, etc. created by RCSP

6.6 Validity of Certification Practice Statement

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

Done at Kigali, on 30/08/2017

(Sé)

Eng. Coletha U. RUHAMYA

Chairperson of the Regulatory Board