



NPKI-GovCA

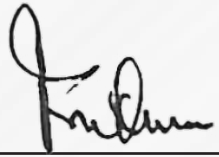
Registration Authority Charter

Version 1.0, March 2022

The ICT Authority is a State Corporation under the State Corporations Act 446
www.icta.go.ke

© ICTA 2022 - All Rights Reserved

DOCUMENT APPROVAL

Date:  _____

Prof. Fredrick Owino
Chairman, ICT Authority Board
ICT Authority

Date:  _____

Dr. Paul Kipronoh Ronoh
Ag.Chief Executive Officer
ICT Authority

DOCUMENT HISTORY

Version	Revision Date	Revision By	Revision Summary

TERMS AND DEFINITIONS

a. Applicant

Refers to an individual that applies for digital certification services. (New application, renewal, reissuance or revocation of the digital certificate).

b. Availability

Refers to ensuring timely and reliable access to and use of information.

c. Certification Practice Statement (CPS)

Refers to a statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-issuing certificates.

d. Certificate Policy (CP)

Refers to a set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements.

e. Certificate Revocation List (CRL)

Refers to a collection of electronic data containing the list of serial numbers revoked or suspended digital certificates by the Certification Authority (CA).

f. Confidentiality

Refers to preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

g. Digital Certificate

Also called identity certificate, refers to an electronic document used to prove the validity of a public key.

h. Integrity

Refers to the accuracy and completeness of data from modification.

i. Online Certificate Status Protocol (OCSP)

Refers to Internet Protocol (IP) used to obtain the real time revocation status of a digital certificate. It is used as alternative to CRL list to get real time certificate revocation status.

j. Public Key

Refers to a mathematical key which is available publicly and which is used to verify Digital Signatures created with the matched Private Key and to encrypt electronic data which can only be decrypted using the matched Private Key.

k. Private Key

Refers to a mathematical key which is kept private to the owner and which is used to create Digital Signatures or to decrypt electronic data.

l. Registration Authority (RA)

Refers to an entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (an RA is delegated certain tasks on behalf of a GovCA).

m. Subscriber

Refers to a subject of a certificate who is issued a certificate.

n. Subscriber's Agreement

Refers to an agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.

ACRONYMS

CA	CERTIFICATION AUTHORITY
CEO	CHIEF EXECUTIVE OFFICER
CIA	CONFIDENTIALITY, INTEGRITY AND AVAILABILITY
CP	CERTIFICATE POLICY
CPS	CERTIFICATE PRACTICE STATEMENT
CRL	CERTIFICATE REVOCATION LIST
DBA	DATABASE ADMINISTRATOR
GovCA	GOVERNMENT CERTIFICATION AUTHORITY
HR	HUMAN RESOURCE
ICTA	INFORMATION COMMUNICATION TECHNOLOGY AUTHORITY
ICT	INFORMATION AND COMMUNICATION TECHNOLOGIES
ID	IDENTIFICATION
IS	INFORMATION SECURITY
ISACA	INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION
ISC	INFORMATION SECURITY CERTIFICATIONS
IT	INFORMATION TECHNOLOGY
NID	NATIONAL IDENTIFICATION
NIST	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
NPKI	NATIONAL PUBLIC KEY INFRASTRUCTURE
OCSP	ONLINE CERTIFICATE STATUS PROTOCOL
PKI	PUBLIC KEY INFRASTRUCTURE
RA	REGISTRATION AUTHORITY
RootCA	ROOT CERTIFICATION AUTHORITY
SA	SUBSCRIBER AGREEMENT
SOP	STANDARD OPERATION PROCEDURES



With support from the UK Government Digital Access Program (UK DAP) through the Foreign Commonwealth and Development Office (FCDO) in partnership with KPMG and delivered by Serianu Limited.

Contents

1.0 Purpose	8
2.0 Objective	8
3.0 Scope	8
4.0 Application	8
5.0 Principles	8
6.0 Roles and Responsibilities	8
6.1 RootCA	8
6.2 GovCA Obligations	9
6.3 Registration Authority	9
6.4 RA Manager	10
6.5 GovCA Staff	10
7.0 Registration Authority Charter	11
7.1 Confidentiality, Integrity, and Availability	11
7.2 Limitation of Liability	11
7.3 Qualifications, Experience and Trustworthiness Requirements	11
7.4 Records Retention	13
7.5 Compliance	13
7.6 Audit	13
7.7 Protection of Personal Information	13
7.8 Subscriber Registration	15
7.9 Limits to Applications and Requests	16
7.10 Termination of agreement/ charter process	16
8.0 Enforcement	17
9.0 Review	17
10.0 References	17

Introduction

The Registration Authority Charter (RA Charter) is subject to the GovCA certification practice statement (CPS) and describes the practices and procedures specific to be used by RAs for validating and maintaining the confidentiality, integrity and authenticity of NPKI informational assets. The latest version of this RA Charter can be accessed and viewed on www.icta.go.ke

1.0 Purpose

This charter sets out guidelines to ensure that risks associated with Registration Authority are minimized.

2.0 Objective

The objective of this charter is to provide procedures for the operation of the Registration Authority in line with the requirements of GovCA, Root CA and WebTrust principles.

3.0 Scope

This charter covers digital certificate lifecycle processes for a Registration Authority in line with the stipulations of GovCA CP and CPS.

4.0. Application

The Registration Authority Charter is applicable to Registration Authority (RA) as well as to all parties taking part in the Registration Authority digital certification process.

5.0 Principles

- **Confidentiality:** To ensure information is secured from unauthorized disclosure and access
- **Integrity:** To observe highest ethical standards
- **Availability:** To ensure information systems are available
- **Non-Repudiation:** To assure ownership of activities carried out within GovCA systems.

6.0 Roles and Responsibilities

6.1 RootCA

The Root Certification Authority (Communications Authority of Kenya) is the primary trust point for the entire NPKI architecture. Communication Authority (CAK) is designated to operate a hierarchy of the Kenyan Root Certification Service Provider (RootCA).

RootCA (RootCA) obligations:

The RootCA obligations include the following but not limited to:

- a) Operate and manage the RootCA system and its functions;
- b) Issue and manage certificates for designated Accredited CAs;
- c) Re-key of the RootCA and approved CA signing keys;
- d) Establishment and maintenance of the CP and CPS for Root CA;

6.2 GovCA obligations:

GovCA, as the Accredited Certification Authority composed of collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers.

The GovCA is responsible for issuing and managing certificates including:

- a) Operation and management of the GovCA systems and its functions in accordance with the RootCA CP and CPS,
- b) GovCA key management,
- c) Approving the issuance of all verified certificate issuance requests,
- d) Issuance and management of user certificates or other entities, used for general or specific purpose,
- e) Publish certificates revocation information,
- f) Handle certificate revocation request, and
- g) Notification of issuance, revocation, suspension, or renewal of its certificates.
- h) Establishing and maintaining the Certification Practice Statement (CPS)

6.3 Registration Authority

The RA shall perform all functions pursuant to this RA Charter including but not limited to:

- Identification of subscribers
- Registration or verification of the applicant information
- Transmit the certificate request to GovCA;
- Validate certificates by the GovCA Directory Server and CRL; and
- Request for revocation, suspension and restoration of certificates.
- Other troubleshooting related to certificate management
- Document and define the practices that the RA uses to fulfill its obligations under the PKI policies and regulations.
- Ensuring that all aspects of registration services and operations are performed.

6.4 RA Manager

The RA Manager is responsible for running the governance of RA within an organization but not limited to:

- Ensuring the effective training of RA Agents and Sponsors within their organization.
- Ensuring the implementation, monitoring and evaluation of this charter.
- Ensuring that processes and procedures are in place to facilitate effective compliance with this charter.

6.5 GovCA Staff

- Understand and be aware of their responsibilities.
- Familiarize themselves with GovCA- NPKI policies governing the information and systems they access.

7.0 Registration Authority Charter

For better service provision, the National PKI comprises of different key participants. GovCA is responsible for performing the Certification Authority (CA) functions, and the Registration Authority is responsible for performing the Registration Authority (RA) functions. This Registration Authority Charter in conjunction with the applicable Certificate Policy (CP), and the GovCA PKI Certification Practices Statement (CPS), will serve as guideline document defining the practices that the RA uses to fulfill its obligations under the NPKI policies and regulations.

GovCA operates as a Sub-CA to the ROOT CA, Communications Authority of Kenya and subscribes to the requirements stipulated in Root CA CP and CPS.

7.1 Confidentiality, Integrity and Availability

RA shall be expected to handle the confidentiality, integrity and availability of information and in compliance with Kenya Data Protection Act, 2019.

7.2 Limitation of Liability

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

- a) Revoked;
- b) Expired;
- c) Used for unauthorized purposes;
- d) Tampered with;
- e) Compromised; or
- f) Subject to misrepresentation, misleading acts or omissions.

7.3 Qualifications, Experience and Trustworthiness Requirements

Qualifications and Experience

An entity designated as RA shall maintain GovCA pre-defined minimum education, experience, and trustworthiness requirement. That RA entity shall identify at least one individual or group responsible and accountable for the operation of the RA functions. All persons filling trusted roles shall be selected on the basis of ethics and integrity. All trusted roles are required to be held by Kenyan citizens and in accordance with the following requirements but not limited to:

- i. At least one (1) of the technical personnel shall be a full-time certified information security professional, who shall oversee the operations/management of the CA and whose certification is issued by the national government or internationally-recognized bodies such as, but not limited to ISO 27001, ISACA, SANS and (ISC)2;
- ii. Each technical personnel shall have educational qualifications of Degree or Diploma in computer engineering, computer science or information and communications technology and any other related field;
- iii. At least half of personnel shall have five (5) years' experience in the field of information security or operation and management of information and communications technology;
- iv. Not an undischarged bankrupt person in the Kenya or elsewhere, or has made arrangement with his creditors; refer to Chapter 6 of the Kenyan Constitution.
- v. Has not been convicted, whether in the nation or elsewhere, of an offense, the conviction for which involved a finding that he acted fraudulently or dishonestly.

Qualifications and Experience

Access to functions shall be role based, especially with regard to accessing subscriber information and data, server services, and other certificate related functions. RA personnel that need access to the PKI system are assigned individual accounts with a role attached to achieve privileges in the system;

- Certain roles shall require segregation of duties.
- No user shall be assigned multiple roles.

The RA shall designate the following roles:

- **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. This user does not have access to the NPKI web interface.
- **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.

7.4 Record Retention

The RA shall securely keep the record of the application, together with all documentation relevant to the authentication of the identity of the applicant and verification of supporting information securely, for a period of 6 (six) years after the expiry or revocation of the digital certificate. Procedures must be developed and implemented to protect archived data from destruction prior to the end of the audit log retention period.

7.5 Compliance

RA is required to comply with GovCA CP, CPS and any applicable laws under the Government of Kenya. A list of legislation compliance shall be developed against all GovCA's certificate lifecycle process (example: from certificate issuance, verification, resilience, modifications, revocation)

7.6 Audit

RA compliance with the practices and procedures set out in this RA Charter and GovCA CP and CPS shall be audited by GovCA (or GovCA assignee) annually. Where the results of an audit report recommend remedial action, the RA shall initiate corrective action within 30 (thirty) days of receipt of such audit report. The audit requirement shall be performed by a qualified independent assessment team comprising, but not limited to, the following:

- Certified Public Accountants; and
- Certified Information Security practitioners.

The following conditions shall also be fulfilled:

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

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

Topics covered by assessment: The audit must conform to industry standards, cover RA compliance with its business practices disclosure, and evaluate the integrity of RA PKI operations. The audit must verify that RA is compliant with:

- GovCA's Certificate Policy (CP)
- GovCA's Certificate Practice Statement (CPS.)

Actions taken as a result of deficiency: If an audit reports a material noncompliance with applicable law, CP, CPS or any other contractual obligations related to GovCA's services, then

- i. The auditor shall document the discrepancy,
- ii. The auditor shall promptly notify GovCA
- iii. GovCA and the RA shall develop a plan to cure the noncompliance.

Communication of results: A copy of the assessment report shall be submitted to the CEO – ICTA within four (4) weeks after completion of an assessment.

7.7 Protection of Personal Information

All information provided by subscribers and applicants are considered confidential and may not be shared by the RA with any person or agency.

- Access to subscriber or applicant information shall only be granted upon court warrant.
- Under no other circumstances may RA disclose any information belonging to an applicant or a subscriber.

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

Where the RA generates and stores subscriber private keys, the RA must ensure the keys are protected in accordance to GovCA CPS requirements. Access to the NPKI infrastructure within the RA environment shall be restricted and in a physically secure environment and subject to security controls throughout its lifecycle.

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

RA to exercise due diligence in the protection of personal information in line with the Kenya Data Protection Act, 2019.

7.8 Subscriber Registration

Subscriber registration process shall only apply to end users who have undergone the verification process and enrolment process stipulated in the CPS.

During verification and enrolment, the identity of the end user must be ascertained and the accuracy of the information provided by the end user must be verified.

The application process shall cover processing of the submitted documents, identification and authentication, approval or rejection of the request, and sending of the certificate.

For Subscriber registration, RAs shall ensure that the identity information is verified by prior compliance with the following but not limited to:

- Physical presence or face to face remote video call of the applicant for the facial authentication; (The RA system shall be designed to keep the evidences of this activity)
- Copy of National Identification (NID)/ Valid Passport;
- Phone number (mobile and/or landline);
- E-mail address; and
- Consent to verify the information submitted attested by the applicant signature on the application form.
- Self-Declaration form of the applicant.

Verification, Authentication and Validation Process Steps

- The RA Officer shall check the completeness and authenticity of the application form and the documentary requirements submitted.
- The RA Officer shall ensure that the information provided in the application form is accurate by conducting checks on pieces of information. This may include verifying against predefined requirement checks lists or by official verification and validation mechanism that may be provided by any competent entity.
- The RA Officer shall check the information that has been digitized to ensure that there is no discrepancy between the hard copy of the application form and the submitted documents, and the soft copy.

The application process shall be conducted within 24 hours.

7.9 Limits to Applications and Requests

- For lawful and intended purposes only.
- Must not be prohibited by the CP and CPS.
- Certificate must be used in accordance with its key usage field extensions.
- The certificate is valid at the time of reliance by reference to an online certificate status protocol or CRL checks.

7.10 Termination of agreement/ charter process

- RA shall remain active until mutual agreed upon separation with the GovCA, the natural effluxion of time or issuance of notice by either party.
- Upon termination or revocation of RA status, all files, archives, records, and logs must be forwarded to the GovCA;
- A public notice announcing the termination of the RA office must be published. In the event that an RA terminates its operation, it shall provide separate prior notice to Communication Authority of Kenya, as Root CA, and ICTA as GovCA prior to termination;
- Subscribers must be notified. In the notification, the alternate RA office where subscribers can file their requests or ask for assistance must be provided.

8.0 Enforcement

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

GovCA reserves the right to terminate the RA if it believes that functions are not being appropriately performed in a particular RA.

RA management shall ensure awareness of and compliance with this charter. Any registration authority employee, subscriber and stakeholder found to have violated this charter shall be subject to disciplinary and legal action as applicable legal legislations.

9.0 Review

This Charter shall be reviewed after a period of 3 years or as deemed necessary due to a:

- a) Significant change in GovCA systems and procedures and mandate.
- b) Major business strategy changes.
- c) Change in the prevailing IT standards and guidelines and technologies.
- d) Change in the law.

10.0 References

- WebTrust Principles and Criteria for Certification Authorities Version 2.2.1
- General Data Protection Regulation
- Kenya Data Protection Act (2019)
- The Computer Misuse and Cybercrimes Act, 2018

ICT Authority
Telposta Towers, 12th Floor, Kenyatta Ave
P.O. Box 27150 - 00100 Nairobi, Kenya
Telephone: + 254-020-2211960/62
Email: info@ict.go.ke or communications@ict.go.ke or standards@ict.go.ke
Visit: www.icta.go.ke
Become a fan: www.facebook.com/ICTAuthorityKE
Follow us on twitter: [@ICTAuthorityKE](https://twitter.com/ICTAuthorityKE)

