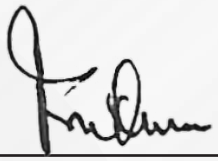
NPKI-GovCA

Subscriber Agreement

Version 1.0, March 2022

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

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
CIA	CONFIDENTIALITY, INTEGRITY AND AVAILABILITY
CP	CERTIFICATE POLICY
CPS	CERTIFICATE PRACTICE STATEMENT
CRL	CERTIFICATE REVOCATION LIST
GovCA	GOVERNMENT CERTIFICATION AUTHORITY
HR	HUMAN RESOURCE
ICTA	INFORMATION COMMUNICATION TECHNOLOGY AUTHORITY
ICT	INFORMATION AND COMMUNICATION TECHNOLOGIES
IS	INFORMATION SECURITY
IT	INFORMATION 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

Contents

Introduction

Subscriber Agreement is a legal agreement between a subscriber and GovCA. It governs the issuance and use of a digital certificate that the subscriber must read and accept before receiving a digital certificate.

1.0 Purpose

The purpose of this agreement is to provide terms and conditions that govern the contractual relationship between the subscriber and the GovCA.

2.0 Objective

The Subscriber agreement governs the subscriber's application for, acceptance, and use of, a digital certificate issued by the GovCA.

3.0 Scope

The Subscriber Agreement covers subscriber obligations to GovCA, terms of use of certificates issued by GovCA, conditions for termination of digital certificates and maintenance.

4.0. Application

This agreement applies to all GovCA subscribers.

5.0 Principles

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

6.0 Statements

GovCA's management is committed to the continuous improvement of subscriber information security and service delivery as part of its mandate. GovCA management shall ensure that the subscriber agreement is implemented and adhered.

7.0 Roles and Responsibilities

7.1 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 CA 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)

7.2 Subscriber

- Abide by all applicable laws, rules, regulations, and guidelines when using a Certificate.
- Comply with all regulations, policies, and procedures of its networks while using Certificates.
- Provide accurate and complete information at all times to GovCA in the Certificate request.

8.0 Subscriber Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE DIGITAL CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A DIGITAL CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT info@icta.go.ke

8.1 NPKI Hierarchy

The Root Certification Authority is the primary trust point for the entire NPKI architecture. The Communication Authority (CA) is designated to operate a hierarchy of the Kenyan Root Certification Service Provider (RA). ICT Authority is the government Accredited Certification Authority by the Root CA.

8.2 Authority to Use Digital Certificates

8.2.1 Grant of Authority

As from the Effective Date up to the end of validity period of any issued Digital Certificate ("Valid from" date to "Valid to" date), GovCA grants to the Subscriber the authority to use the requested Digital Certificate in conjunction with Private Key and/or Public Key operations. The obligations of the subscriber (see section 4.0) with respect to Private Key protection are applicable from the effective date.

8.2.2 Limitations on Certificate usage

The digital certificate cannot be used for purposes other than what is allowed in the certificate usage file as stipulated in the Certificate Practice Statement document.

8.3 Use of Digital Certificate

The subscriber shall use the certificate for its lawful and intended use only. The certificate shall be used in accordance with its Key-Usage field extensions as per the stipulations in the CPS. All issued certificate by GovCA cannot be used for purposes other than what is allowed in this subscriber agreement and by the CPS. GovCA shall not be liable for any claims arising from prohibited use.

8.3.1 Acceptance of a Digital Certificate

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. (Check CPS for detailed information)

8.3.2 Revocation of Digital Certificates

A certificate shall be revoked when the bind between the subscriber and the subscriber's public key is no longer valid. An end-user subscriber certificate can be requested for revocation under any of the following conditions:

a) When subscriber or the representative requests revocation of the Certificate as per the CPS guidelines

b) When a verified request for revocation is received by GovCA or RA;

c) When any of the information found in the certificate is changed or no longer applicable;

d) When the Private Key, or the media holding the Private Key, associated with the certificate is compromised;

e) When the GovCA determines that the subscriber is no longer complying with the requirements of by the CPS and this subscriber agreement; or

f) When the GovCA has the reason to believe that the certificate was issued in a manner that is not in accordance with the procedures required by the CPS and this subscriber agreement.

8.4 Subscriber Obligations

A subscriber who applies for the digital certificate shall be responsible for the following:

a) Provision of accurate information for the certificate application

b) The provisions of the RootCA CP/CPS, GovCA CP/CPS, and other pertinent documents are binding upon the subscriber.

c) The subscriber shall not, under any circumstances, allow any other person to use the digital certificate. Any such use by another person constitutes a compromise of the associated private key, requiring the revocation of the digital certificate.

d) The subscriber shall protect the confidentiality of the private key associated with his or her digital certificate as well as any PIN number or other means used to activate the private key.

e) The subscriber shall bear the responsibility of notifying the GovCA through the RA of any private key compromise or suspect of compromise.
f) The subscriber shall not use the digital certificate for any unlawful purpose, or for any purpose that does not have anything to do with accessing the PKI information systems or transactions using the digital certificates.
g) The subscriber shall not tamper, interfere with, or reverse-engineer any technical implementation of the digital certificate or its use, or in any manner seek to compromise the security provided by the RA and the National PKI system.

8.5 Notice and Consent to Use Private Information

Any disclosure of subscriber-specific information by GovCA or RA shall comply with the requirements of Root Authority, the Kenya Data Protection Act, 2019 and must be authorized by the subscriber.

8.5.1 Permission to Publish Information

The Subscriber agrees that GovCA may publish the serial number of the Subscriber's Digital Certificate in connection with GovCA's dissemination of CRL's and OCSP.

8.5.2 Disclaimer

GovCA shall not be liable for any claims arising from prohibited use of Digital Certificates issued by GovCA. GovCA will not be liable if the user has not respected his obligations mentioned in the CPS and in this agreement.

8.5.3 Certificate Operational Periods and Key Pair Usage Periods

A subscriber certificate shall be valid for 1 year and shall be renewed at the request of the subscriber.

8.6 Limitations of Liability

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

- Revoked;
- Expired;
- Used for unauthorized purposes;
- Tampered with;
- Compromised; or
- Subject to misrepresentation.

8.7 Term and Termination

This agreement shall terminate upon

(a) The expiry date of the Digital Certificate issued to the Subscriber

(b) Any failure to comply with any of the subscriber obligations mentioned in this Subscriber Agreement

8.7.1 Effect of termination

Upon termination of this Subscriber Agreement for any reason, GovCA shall revoke the Subscriber's Digital Certificate in accordance with GovCA revocation procedures.

8.7.2 Penalty fees/ Non-payment

None

8.8 CP and CPS Information

The digital certificate contains information provided by the subscriber, which is authenticated by the RA in accordance with the requirements set out in the CP and CPS, available for viewing and download at https://icta.go.ke/

9.0 Enforcement

GovCA management shall ensure awareness of and compliance with this agreement. Any subscriber or stakeholders found to have violated this agreement shall be subject to disciplinary action in compliance with applicable legal legislations.

10.0 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.

11.0 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
- The Kenya Information and Communications Act, 2011.

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