NPKI-GovCA

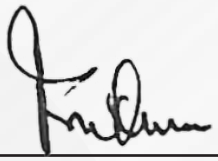
Government CA Certificate Policy (CP)

Version 1.0, March 2022

Document OID: 2.16.404.100.1.1

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

Contents

1.0 INTRODUCTION

1.1 Overview

The ICT Authority (hereafter referred as GovCA) operates the National public key infrastructure on behalf of the government to enable certificate-based authentication, data integrity and confidentiality in the government administration's ICT systems as well as its electronic document exchange and in online services. This document is the National Public Key (NPKI) Certificate Policy document (hereafter referred as CP). This CP sets out the rights, duties, and obligations of each party involved in National Public Key Infrastructure. It is compliant with the Web Trust Principles and Criteria for Certification Authorities.

This CP complies with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework and was developed following the template recommended in the Request for Comment (RFC) #3647. Any section that is not applicable for GovCA will be marked as "Not Applicable".

This CP applies and shall only be used as a guideline of the certification services provided by ICT Authority (ICTA) hereafter referred as the Government Certificate Authority (GovCA), the relying parties and all PKI participants.

1.2 Document name and identification

Document Title: Certification Policy

Author: ICT Authority (ICTA)

Document Version: Version 1.0

Document Date: March 2022

OID: 2.16.404.100.1.1

1.3 PKI participants

This section identifies roles that are relevant to the administration and operation of GovCA services under this policy.

1.3.1 Certification authorities (CA)

The National PKI uses the advanced PKI system architecture and is made of well structure of Certification Authorities. This section describes the Kenyan NPKI functional authorities. The architecture of our National PKI complies with the Root Certificate Authority (RootCA) which is the primary trust point for the entire PKI architecture. The RootCA is managed and operated by the Communications Authority of Kenya, who is also the Policy Authority (PA) that establishes all the National PKI guidelines and policies.

RootCA Obligations:

1) Operation and management of the Root CA system and its functions,
2) Management of the RootCA Keys (Re-key of the Root CA) and CA Key signing,
3) Notification of issuance, revocation, suspension, or renewal of its certificates,
4) CA accreditation, issuance, and management of the certificates of the Accredited CAs,
5) PKI policy management and establishment of the RootCA CP and CPS,
6) Provide technical expertise in the conduct of assessment of CAs and CA operation auditing,
7) Support international cooperation on certification service, including mutual recognition and cross-certification,
8) Resolution of disputes between concerned parties.

1.3.1.1 Government CA obligations:

The GovCA is responsible for issuing and managing certificates including:

1) Operation and management of GovCA systems and its functions in accordance with the Root CA CP and CPS,
2) CA key management,
3) Approving the issuance of all verified certificate issuance requests,
4) Issuance and management of user certificates or other entities, used for general or specific purpose,
5) Publish certificates revocation information,
6) Handle certificate revocation request, and
7) Notification of issuance, revocation, suspension, or renewal of its certificates.
8) Establishing and maintaining the Certification Practice Statement (CPS)

1.3.2 Registration authorities (RAs)

Registration Authorities (RAs) are trusted entities designated by the GovCA to perform the subscriber's identification and authentication under certain agreement done with the related CA. These entities help to handle the subscribers' certificate registration and revocation requests as specified by the GovCA CP/CPS and related policies. The RA obligations include:

1) Identification of the applicant and registration or verification of the applicant information
2) Transmission of the Digital Certificate request to GovCA
3) Transmission of the user's certificate revocation, suspension, and restoration request to GovCA,
4) Offer other PKI related assistance and guidance to the users.

GovCA will elaborate the RA Charter requirement and RA agreements for each RA office establishment.
RA Staff are the individuals holding trusted roles that operate and manage RA components.

1.3.3 Subscribers

A subscriber, applicant or sometimes referred as the user, is an individual or juridical entity whose name appears as the subject in a certificate. Upon the user's certificate request, GovCA securely provide a pair of keys to the subscriber, and the subscriber asserts to use the keys and certificate in accordance with the certificate policy. The subscriber obligations are the following:

1) Provision of right and accurate information for the certificate application

2) Protection of the entity's private key with adequate restriction to its access and usage

3) Notify any private key compromise or suspect of compromise.

1.3.4 Relying parties

A relying party is any entity that relies on the validity of the binding of the subscriber's name or identity to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A relying party may use the information in the certificate to determine the suitability of the certificate for a particular use as per the provided certificate usage in GovCA CPS.

1.3.5 Other participants

For a better and secure system operation and service provision, GovCA and RA may require the use of other services, applications, or other functional modules from other services providers, such as security modules These will be referred as "Other participants".

1.4 Certificate usage

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

1.4.1 Appropriate certificate uses

1) The Root CA certificate can only be used for signing subordinate CA's and CRL's.

2) Certificates issued by GovCA can only be used strictly as part of the framework of the limitations defined in the certificates.

3) Relying parties are required to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum the following must be assessed:

- The appropriateness of the use of the certificate for any given purpose and that the use meets the guidance provided in this CP.
- The certificate is being used in accordance with its Key-Usage field extensions.
- The certificate is valid at the time of reliance by reference to Online Certificate Status Protocol (OCSP) or Lightweight Directory Access Protocol (LDAP) Certificate Revocation List (CRL) checks.

1.4.2 Prohibited certificate uses

All certificates issued under this policy cannot be used for purposes other than what is allowed in Section 1.4.1 above and what is stipulated in laws of the Republic of Kenya.

1.5 Policy administration

As the Accredited Certificate Authority, the ICT Authority (ICTA) is responsible for all aspects and management of this CP.

1.5.1 Organization administering the document

This CP is under the administration and management of the Kenya ICT Authority.

Contact information:

ICT Authority

TelPosta Towers 12th, Floor, Kenyatta Avenue

Nairobi Kenya

Website: https://icta.go.ke

1.5.2 Contact person

Chief Executive Officer ICT Authority

TelPosta Towers 12th, Floor, Kenyatta Avenue

P.O Box 27150-00100

Phone: +254 2089061

Website: https://icta.go.ke

Email: info@ict.go.ke

1.5.3 Person determining CPS suitability for the policy

Attn: Director General Communication Authority - CA Centre

P.O Box: 14448-00800, Nairobi

Mobile: 0703 042000, 0730 172000

Email: dg@ca.go.ke

1.5.4 CPS approval procedures

This CP is verified and validated by the Communications Authority of Kenya (our Policy Authority) before application and publication.

The modifications and version update are documented into the document review and version record table.

1.6 Definitions and acronyms

1.6.1 Definitions:

1. Access Control:

Process of granting access to information system resources only to authorized users, programs, processes, or other systems.

2. Accreditation:

Formal declaration by a designated approving authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

3. Applicant:

The subscriber is sometimes also called an "applicant" or "user" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.

3. Archive:

Long-term, physically separate storage.

4. Audit:

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

5. Authenticate:

To confirm the identity of an entity when that identity is presented.

6. Authentication:

Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

7. Backup:

Copy of files and programs made to facilitate recovery if necessary. Binding: Process of associating two related elements of information.

8. Certificate:

Is a digital representation of information which at least:

- identifies the certification authority issuing it,
- names or identifies its subscriber,
- contains the subscriber's public key,
- identifies its operational period, and
- Is digitally signed by the certification authority issuing it.

In this CP, the term "certificate" refers to X.509 certificates. The certificate issued by ICTA GovCA shall expressly reference the OID of this CPS in the certificate Policies extension.

9. Certification Authority (CA):

A trusted authority by one or more users to issue and manage X.509 public key certificates and CRLs.

10. CA Facility:

The collection of equipment, personnel, structures, processes, and procedures used by a certification authority to perform certification services.

11. Certification Practice Statement (CPS):

A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CPS, or requirements specified in a contract for services).

12. Certificate-Related Information:

Subscriber Information provided during the certificate application, such as a subscriber's postal address, that is not included in a certificate that may be used by a CA managing certificates.

13. Certificate Revocation List (CRL):

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

14. Client (system application):

A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.

15. Common Criteria:

A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

16. Compromise:

Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

17. Confidentiality:

Assurance that information is not disclosed to unauthorized entities or processes.

18. Cross-Certificate:

A certificate used to establish a trust relationship between two certification authorities.

19. Hardware Security Module (HSM):

The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

20. Data Integrity:

Assurance that the data are unchanged from creation to reception.

21. Digital Signature:

The result of a transformation of a message by means of a cryptographic system using keys verifiable by the relying party to determine:

- whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and
- Whether the message has been altered since the transformation was made.

22. Integrity:

Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

23. Intellectual Property:

Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

24. Key Escrow:

A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.

25. Key Exchange:

The process of exchanging public keys in order to establish secure communications.

26. Key Generation Material (Random Value):

Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

27. Key Pair:

Two mathematically related keys having the following properties:

- One (public) key can be used to encrypt a message that can only be decrypted using the other

28. Non-Repudiation:

Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.

29. Object Identifier (OID):

A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.

30. Physically Isolated Network:

A network that is not connected to entities or systems outside a physically controlled space.

31. Public Key:

The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital certificate.

32. Public Key Infrastructure (PKI):

Is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. Registration Authority (RA): An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).

33. Re-key (a certificate):

To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.

34. Relying Party:

A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate and be able to rely on them.

35. Risk:

An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

36. Root CA:

Also referred to as Root Certification Service Provider/ Controller in a hierarchical PKI, GovCA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

37. Server:

A system entity that provides a service in response to requests from clients.

38. Signature Certificate:

A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

39. Subscriber:

A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device.

40. Trust List:

Collection of Trusted Certificates used by relying parties to authenticate other certificates.

1.6.2 Acronyms

AIA: Authority Information Access

AOR: Authorized Organizational Representative

CA: Certification Authority

CP: Certificate Policy

CPS: Certification Practice Statement

CRL: Certificate Revocation List

CSS: Certificate Status Server

DN: Distinguished Name

DS: Directory System

FIPS: Federal Information Processing Standards

GovCA: Government Certification Authority

HTTP: Hypertext Transfer Protocol

IETF: Internet Engineering Task Force

ISO: International Organization for Standardization

ITL: Information Technology Laboratory

ITU: International Telecommunications Union

LDAP: Lightweight Directory Access Protocol

LRA: Local Registration Authorities

OCSP: Online Certificate Status Protocol

OID: Object Identifier

PA: Policy Authority

PKI: Public Key Infrastructure

PKIX: Public Key Infrastructure X.509 Working Group

PRNG: Pseudo Random Number Generator

RA: Registration Authority

RFC: Request for Comment

RNG: Random Number Generator

RootCA: Root Certification Authority

RSA: Rivest-Shamir-Adleman (encryption algorithm)

SHA: Secure Hash Algorithm

TAM: Trust Anchor Manager

URL: Uniform Resource Locator

2.0 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The ICT Authority (ICTA) as the Government Certificate Authority (GovCA) is responsible for the publication of this CP, and is publicly accessible at ICTA website: https://icta.go.ke
GovCA shall post its CRL issued in a directory system (DS) that is publicly accessible through the Lightweight Directory Access Protocol (LDAP) or Hypertext Transport Protocol (HTTP).
To ensure a secure, adequate, and consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information. Published CRLs may be replicated in additional repositories for performance enhancement. Such repositories will be operated by the GovCA.

2.2 Publication of certification information

- The publicly accessible directory system shall be designed and implemented to comply with the requirements stipulated in the CPS
- The GovCA CP and CPS document shall be publicly available.

2.3 Time or frequency of publication

This CP and any subsequent changes shall be made publicly available immediately after its approval. A certificate revocation list (CRL) shall be made published as specified in Section 4.9.7.

2.4 Access controls on repositories

GovCA shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. The CPS shall detail what information in the repository can be restricted or automatically published and the conditions under which, and to whom restricted information may be made available.

3.0 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The ICT Authority (GovCA) shall only generate and sign certificates that contain a non-null subject Distinguished Name (DN). The ICT Authority GovCA must have a unique and readily identifiable X.501 Distinguished.

3.1.2 Need for names to be meaningful

Names used in the certificates must identify the subscriber in a meaningful way to which they are assigned. A name is meaningful only if the names that appear in the certificates can be understood and used by relying parties. The subject name in user certificates must match the issuer name in certificates issued by the GovCA, as required by [RFC5280].

3.1.3 Anonymity or pseudonymity of subscribers

GovCA shall not issue anonymous certificates.

3.1.4 Rules for interpreting various name forms

The naming convention used by GovCA is ISO/IEC 9595:1998 (X.500) Distinguished Name (DN) and RFC822 for e-mails.

3.1.5 Uniqueness of names

The entity certificate Distinguished Names (DN) must be unique for each end entity certificate issued by the GovCA.
GovCA will ensure the DN uniqueness and reserves the right to make decisions regarding entity names in all assigned certificates. A party requesting a certificate may be required to demonstrate its right to use a particular name. The CPS shall identify the method for the assignment of unique subject names.

3.1.6 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 to prove possession of private key

In any case where the proof of subject's private key possession is required, the relying entity should use (apply) an undoubtfully method to prove that the subject in question possesses the private key that corresponds to the available public key. This can be done through data encryption and decryption or simply by the digital signature verification mechanism. The proof of the private key possession may not be required for the GovCA users as their keys generation is performed under GovCA or RA's direct control.

3.2.2 Authentication of organization identity

The organization identity include's the organization's name address and official documentation of the existence of the organization.
To process the request of organization certificate, in additional to the company authentication, GovCA shall verify the information of the requesting person and the representative's authorization (or power of attorney) to act in the name of the organization.
Juridical applicant's information shall be verified with prior submission of the following:

a. For a government agency:

- Business Registration Number & Name
- Official signed document/Power of attorney/ Appointment document

b. For non-government entities (local and foreign):

- Business registration certificate
- Power of attorney of a representative and proof of the appointment of the company representative if
  their names are not in the official company registration documents.

3.2.3 Authentication of individual identity

Prior to the acceptance or registration of the applicant information in the system, GovCA and its RAs shall ensure that the applicant identity information is well verified and validated. The relying party is responsible for due diligence before and use and trust of the entity digital certificate as the entity verification and authentication may depend on the entity type and the application for which the public keys are used. (There exist various types of entities: human, device, application or service, role holder, and code signer.)

3.2.3.1 Authentication of Human Subscribers

The RA shall ensure that the subscriber's identity information is verified as specified in section 3.2.3 of the CPS.

3.2.3.2 Authentication of Devices

This section applies to identities assigned to hardware devices, not the software or applications that run on them. (Example certificates for automated inventory systems). In case computing and communications devices (routers, firewalls) require the digital certificate, an Authorized Organizational Representative (AOR), or in certain cases the device itself, must provide identifying information for the device. The AOR/ device is responsible for providing registration information which may include:

- Equipment identification (such as, serial number)
- Equipment certificate signing request CSR
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the GovCA or RA to communicate with the AOR when required.

The registration information provided by the AOR/device shall be verified. If the device itself provides this information, the identity of the device shall be authenticated. If the information is provided by an AOR for a single device or batch of devices, the AOR shall be authenticated.

3.2.3.3 Authentication of Applications or Services

This section applies to identities assigned to the services offered via a network, irrespective of the hardware running the software that implements the service. This enables services to be replaced from backup in the event of a hardware failure, without re-provisioning keys. (The hardware may have its own certificate, as described in Section 3.2.3.2 above.)
Some software applications or services will be named as certificate subjects. In such cases, an Authorized Organizational Representative (AOR) must provide identifying information for the device. The AOR is responsible for providing registration information which may include:

- Unique software application or service name (such as. DNS name)
- Software application or service certificate signing request CSR
- Software application or service authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the GovCA or RA to communicate with the AOR when required.

The registration information provided by the AOR shall be verified. The GovCA shall validate that the AOR is authorized to request a certificate for the application or service.

3.2.3.4 Authentication for Role Certificates

A role certificate shall identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name. A role certificate shall not be a substitute for an individual subscriber certificate. Multiple subscribers can be assigned to a role at the same time. Subscribers issued role certificates shall protect the corresponding role credentials to the same security level as individual credentials. The procedures for issuing role certificates shall comply with all other stipulations of this CP (such as., subscriber identity proofing, validation of organization affiliation, key generation, private key protection, and Subscriber obligations). The AOR may act on behalf of the certificate subject for certificate management activities such as issuance, renewal, re-key, modification, and revocation. GovCA or the RA shall record the information identified in Section 3.2.3.1 for an AOR associated with the role before issuing a role certificate. The GovCA or RA shall verify the identity of the AOR using an individual certificate in his or her own name issued by GovCA with equivalent assurance as the role certificate, or other commensurate methods. AORs shall be responsible for:

- Authorizing subscribers for a role certificate,
- Recovery of the private decryption key,
- Revocation of subscriber's role certificates,
- Always maintaining a current up-to-date list of subscribers who are assigned the role, and
- Always maintaining a current up-to-date list of subscribers who have been provided the private keys for the role.

3.2.3.5 Authentication for Code Signing Certificates

Code signing indicates to the recipient of the code that the code comes from an authorized source, and that the integrity of the source has been protected during distribution (i.e., that the code hasn't been modified). A code signing certificate identifies the person or organization authorized to make those claims to the code recipient.

The procedures for issuing code signing certificates shall comply with all other stipulations of this CP (such as., subscriber identity proofing, validation of organization affiliation, key generation, private key protection, and Subscriber obligations). One or more AORs shall be assigned to act on behalf of the code

signing certificate subscriber for certificate management activities such as issuance, renewal, re-key, modification, and revocation. GovCA or the RA shall record the information identified in Section 3.2.3.1 for an AOR associated with the code signing certificate. The GovCA or RA shall verify the identity of the AOR using an individual certificate issued by GovCA with equivalent assurance as the code signing certificate, or other commensurate methods.

AORs shall be responsible for:

- Authorizing subscribers for a code signing certificate
- Revocation of subscriber's code signing certificates
- Always maintaining a current up-to-date list of subscribers who are authorized to hold code signing certificates and their associated private keys.

3.2.4 Non-verified subscriber information

Any information that is not verified shall not be included in certificates. All certificate contents are verified by GovCA or RA, either directly or by an attestation from the AOR who is authoritative for the certificate subject.

3.2.5 Validation of authority

Before issuing signature certificates that assert organizational authority, the GovCA shall validate the subscriber's authority to act in the name of the organization. For role certificates that identify subjects by their organizational roles, GovCA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role. An example of signature certificates that assert organizational authority is code signing certificates.

3.2.6 Criteria for interoperation

The interoperability criteria are defined by the Root CA.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

For re-key of any subscriber certificate issued under this certificate policy, identity may be established through use of current signature key, except that identity shall be established following the same procedures as the initial registration at least once per (1) or max 2 years (if requested) from the time of original registration. Note: This will be possible only in the last 90 days prior to the subscriber's certificate expiration and the GovCA will send a reminder to the subscriber 60 days and 30 days before certificate expiration time.

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 CRL in all repositories of such list;
3) Requests for revocation shall be received and acted upon any time; and
4) Record and keep, in trustworthy manner, the date and time of all transactions in relation to the revocation request.

4.0 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS (11)

4.1 Certificate Application

An application for a certificate shall be made directly with GovCA under this CP or through its accredited RA and fulfilling the application requirements as enumerated in Section 3 of this CP.

4.1.1 Who can submit a certificate application

The certificate application shall be submitted toGovCA by the Subscriber, AOR, or an RA on behalf of the 14 Subscriber. Multiple certificate requests from one RA or AOR may be submitted as a batch.

4.1.2 Enrollment process and responsibilities

All communications among PKI Authorities supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.
Subscribers are responsible for providing accurate information on their certificate applications.

4.2 Certificate application processing

Information in certificate applications must be verified as accurate before certificates are issued.

4.2.1 Performing identification and authentication functions

The identification and authentication of the subscriber shall meet the requirements specified for subscriber authentication as specified in Sections 3.2 and 3.3.

4.2.2 Approval or rejection of certificate applications

Any certificate application that is received by GovCA under this policy, for which the identity and authorization of the applicant has been validated, will be duly processed. However, GovCA shall reject any application for which such validation cannot be completed, or when GovCA has cause to lack confidence in the application or certification process.

4.2.3 Time to process certificate applications

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 CA actions during certificate issuance

Upon receiving the request, the GovCA or respective RAs shall:

- Verify the identity of the requester as specified in Section 3.2
- Verify the authority of the requester and the integrity of the information in the certificate request as specified in Section 4.1.
- Build and sign a certificate if all certificate requirements have been met (This is only done by GovCA).
- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in Section 9.6.3.

In case of online application or automated application systems, the certificate request may already contain a to-be-signed certificate built by either the RA or the subscriber. The certificate shall not be signed until all verifications and modifications, if any, have been completed as per the GovCA requirements. All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate.

4.3.2 Notification to subscriber by GovCA of issuance of certificate

GovCA or its RAs operating under this CP shall inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber. For device certificates, GovCA shall issue the certificate according to the certificate requesting protocol used by the device (this may be automated) and, if the protocol does not provide inherent notification, also notify the authorized organizational representative of the issuance.

4.4 Certificate acceptance

Before a subscriber can make effective use of its private key, the GovCA or its RAs shall explain to the subscriber its responsibilities and obtain the subscriber's acknowledgement, as defined in Section 9.6.3. This can also be done by the RA during the subscriber identity verification.

4.4.1 Conduct constituting certificate acceptance

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

4.4.2 Publication of the certificate byGovCA

As specified in Section 2.1, GovCA certificates shall be published in repositories.
This policy makes no stipulation regarding publication of subscriber certificates.

4.4.3 Notification of certificate issuance byGovCA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The intended scope of usage for a private key shall be specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate. The certificates issued by the GovCA can be used for the signature and for the encryption.

4.5.2 Relying party public key and certificate usage

Certificates may specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. Relying parties are required to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

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

GovCA shall issue CRLs specifying the status of all unexpired certificates except for OCSP responder certificates. It is recommended that relying parties process and comply with this information whenever using certificates in a transaction.

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 with a new, extended validity period and a new serial number. Renewal of a certificate does not require a change to the subject Name and does not violate the requirement for name uniqueness.
After the certificate renew, any copy of the old certificate is automatically expired at the end of the validity period, and may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.1 Circumstance for certificate renewal

Any 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 requirements listed in Section 3.3.1 shall also be met.
The GovCA certificate and OCSP responder certificates may be renewed if the aggregated lifetime of the public key does not exceed the certificate lifetime specified in Section 6.3.2.
The GovCA may renew previously issued certificates during recovery from CA key compromise without subject request or approval ifGovCA is confident of the accuracy of information to be included in the certificates.

4.6.2 Who may request renewal?

The Subscriber, RA, LRA, or AOR may request the renewal of a subscriber certificate.

4.6.3 Processing certificate renewal requests

Digital signatures on subscriber renewal requests shall be validated before electronic renewal requests are processed per Section 3.3. Alternatively, subscriber renewal requests may be processed using the same process used for initial certificate issuance.

4.6.4 Notification of new certificate issuance to subscriber

GovCA shall inform the subscriber of the renewal of his or her certificate and the contents of the certificate. The notification of a renewed certificate to a subscriber follows the same routine as when a new certificate is issued as specified in Section 4.3.2 of this CP. GovCA

4.6.5 Conduct constituting acceptance of a renewal certificate

Failure to object to the renewal of the certificate or its contents within thirty (30) days, after notification of the renewal of the certificate, constitutes acceptance of the certificate.

4.6.6 Publication of the renewal certificate by GovCA

Publication of renewed subscriber certificates is subject to the requirements in Section 2 and Section 9.4.3 of this policy.

4.6.7 Notification of certificate issuance by GovCA to other entities

The notification of a renewed certificate to other entities follows the same routine as when a new certificate is issued as specified in Section 4.3.2 of this CP.

4.7 Certificate re-key

Re-keying a certificate consists of creating new certificates with a different public key (and serial number and key identifier) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the subject Name and does not violate the requirement for name uniqueness. An old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified. 34 Subscribers shall identify themselves for the purpose of re-keying as required in section 3.3.

4.7.1 Circumstance for certificate re-key

It is highly recommended that a subscriber periodically obtains new keys. (Section 6.3.2 establishes usage periods for private keys for both RAs and subscribers.) Examples of circumstances requiring certificate re-key have been defined in section 4.7.1 of the CPS extensive.:
There is no limitation of re-key request in a year.

4.7.2 Who may request certification of a new public key?

Requests for certification of a new public key shall be considered as follows:

- Subscribers with a currently valid certificate may request certification of a new public key.
- CAs and RAs may request certification of a new public key on behalf of a subscriber.
- For device, application/service, or role certificates, an AOR that owns or controls the device may request re-key.

Section 3.3.1 of this CP shall be followed to verify and validate the subscriber's information.

4.7.3 Processing certificate re-keying requests

Digital signatures on subscriber re-key requests shall be validated before electronic re-key requests are processed per Section 3.3. Alternatively, subscriber re-key requests may be processed using the same process used for initial certificate issuance. All re-key requests shall be authenticated by RAs and authorized by GovCA.

4.7.4 Notification of new certificate issuance to subscriber

GovCA shall inform the subscriber of the rekey of his or her certificate and the contents of the certificate.

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 certificate.

4.7.6 Publication of the re-keyed certificate by GovCA

Publication of re-keyed subscriber certificates is subject to the requirements in Section 2 and Section 9.4.3 of this policy.

4.7.7 Notification of certificate issuance by GovCA to other entities

The notification of a rekeyed certificate to other entities follows the same routine as when a new certificate is issued as specified in Section 4.3.2 of this CP.

4.8 Certificate modification

Modifying a certificate means creating a new certificate that has the same key, a different serial number, and that differs in one or more other fields from the old certificate. Because of the requirement to validate particular field changes, it is often simpler and more secure to require re- certification than to offer certificate modification.

4.8.1 Circumstance for certificate modification

GovCA may perform certificate modification for a subscriber whose characteristics have changed and requires updating the information contained in the certificate (such as., name change due to marriage).

If the subscriber's information contained in the certificate has changed, the subscriber shall undergo the initial registration process.

4.8.2 Who may request certificate modification?

Requests for certificate modification shall be considered as follows:

- Subscribers with a currently valid certificate may request certificate modification.
- CAs and RAs may request certificate modification on behalf of a subscriber.
- For device, application, and role certificates, an AOR may request certificate modification.

4.8.3 Processing certificate modification requests

A certificate modification shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2
- Identification & Authentication using a subscriber-signed certificate modification request, as described in Section 4.7.3. In addition, the validation of the changed subject information shall be in accordance with the initial identity-proofing process as described in Section 3.2

The RA shall complete all required re-verification prior to issuing the modified certificate. Proof of all information changes must be provided to the GovCA or its RAs before the modified certificate is issued.

4.8.4 Notification of new certificate issuance to subscriber

GovCA shall inform the subscriber of the modification of his or her certificate and the contents of the certificate.

4.8.5 Conduct constituting acceptance of modified certificate

Failure to object to the certificate or its contents within thirty (30) days, after notification of the issued certificate, constitutes acceptance of the certificate.

4.8.6 Publication of the modified certificate by GovCA

Publication of modified subscriber certificates is subject to the requirements in Section 2 and Section 9.4.3 of this policy.

4.8.7 Notification of certificate issuance by GovCA to other entities

The notification of a modified certificate to other entities follows the same routine as when a new certificate is issued as specified in Section 4.3.2 of this CP.

4.9 Certificate revocation and suspension

GovCA issue CRLs, and/or provide OCSP responses covering all unexpired certificates issued under this policy as described in section 2 of this CP. Certificate revocation information shall be given to subscribers during certificate request or issuance and shall be readily available to any potential relying party. Revocation requests must be authenticated as per section 3.4 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 the certificate is no longer considered valid. When this occurs, the associated certificate shall be revoked and placed on the CRL and/or added to the OCSP responder. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire. Refer to section 4.9.1 of CPS for detailed list of circumstances that invalidate the binding.

4.9.2 Who can request revocation?

GovCA may revoke certificates within its domain. A written notice and brief explanation for the revocation should subsequently be provided to the subscribers.
The RA can request the revocation of a subscriber's certificate on behalf of any authorized party.
A subscriber may request that its own certificate be revoked.
The AOR of the organization that owns or controls a device can request the revocation of the device's certificate. Other authorized individuals of the organization may request revocation.

4.9.3 Procedure for revocation request

The GovCA or its RAs shall verify the identity and authority (for juridical entity) of a subscriber making the request for revocation.
A request to revoke a certificate shall identify the certificate to be revoked and allow the request to be authenticated (such as., digitally or manually signed). GovCA may request information sufficient to explain the reason for revocation.

4.9.4 Revocation request grace period

There is no grace period for revocation under this policy.

4.9.5 Time within which CA must process the revocation request

GovCA shall revoke certificates as quickly as practical upon receipt of a proper revocation request and after the requested revocation was accepted. Revocation requests shall be processed immediately of the receipt.

4.9.6 Revocation checking requirement for relying parties

Relying Parties should validate any presented certificate against updated CRL or through OCSP.

4.9.7 CRL issuance frequency (if applicable)

GovCA shall publish the CRL at least once every twenty-four (24) hours. The publication and frequency of CRL issuance shall be in conformance with Section 2 of this CP. Circumstances related to emergency CRL issuance are specified in section 4.9.12.

4.9.8 Maximum latency for CRLs (if applicable)

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 for same scope.

4.9.9 On-line revocation/status checking availability

GovCA supports on-line revocation status checking, and the revocation status information shall be updated and available to relying parties in less than 24 hours of the decision to revoke. OCSP services are highly recommended for more credible online revocation status check.

4.9.10 On-line revocation checking requirements

Relying party client software should support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

No stipulation.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

GovCA shall provide both Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) vi the CRL server repository.

4.10.1 Operational characteristics

CRL/LDAP service are provided by default for all the relying entities. OCSP services are provided on demand and may be subjected to charges.

4.10.2 Service availability

To be defined

4.10.3 Optional features

OCSP services may not be compulsory for all the services. Relying parties may choose to use it or not.

4.11 End of subscription

Subscription is synonymous with the certificate validity period. The subscription ends when the certificate is revoked or expired.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Private keys of the subscriber certificates issued by GovCA shall never be escrowed.
Under no circumstances shall a subscriber signature key be held in trust by a third party.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation

5.0 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS (11)

5.1 Physical controls

All CA and RA equipment, including cryptographic modules, shall always be protected from theft, loss, and unauthorized access. Unauthorized use of CA and RA equipment is prohibited. CA equipment shall be dedicated to performing CA functions. RA equipment shall be operated to ensure that the equipment always meets all physical controls.

5.1.1 Site location and construction

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

5.1.2 Physical access

The GovCA equipment including remote workstations used to administer the GovCA systems shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment. Refer to section 5.1.2 of CPS for details on Physical access security:

5.1.3 Power and air conditioning

GovCA environment shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. In addition, directories (containing issued certificates and CRLs) shall be provided with Uninterrupted Power sufficient for operation in the absence of commercial power.

5.1.4 Water exposures

The GovCA equipment shall be installed such that it is not in danger of exposure to water.
Potential water damage from fire prevention and protection measures (such as., sprinkler systems) are excluded from this requirement.

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

CA and Operations Staff and RA Staff shall remove and destroy normal office waste in accordance with local policy. Media used to collect or transmit privacy information shall be destroyed, such that the information is unrecoverable, prior to disposal. Sensitive media and paper shall be destroyed in accordance with the applicable policy for destruction of such material.

5.1.8 Off-site backup

A full system backup shall be made when a CA system is activated. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy of CA system shall be stored in an off-site location separate from the GovCA's equipment.
The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system. Backups shall be stored offsite. Only the latest backup needs to be retained.

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 role operations include the GovCA Administrator, GovCA Operations Staff, Security Auditor, RA Staff. Their tasks shall be defined in section 5.2.1 of the CPS.
The people selected to fill these roles must be extraordinarily responsible for their roles otherwise the integrity of GovCA or RA is weakened. The functions performed in these roles form the basis of trust for all uses of the national certification scheme for digital signatures. Approaches shall be taken to increase the likelihood that these roles can be successfully carried out. The first shall ensure that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. GovCA detailed role and functions are described in the CPS.

5.2.2 Number of persons required per task

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role except for audit functions.

5.2.3 Identification and authentication for each role

All individuals shall identify and authenticate themselves before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Roles requiring separation of duties

Individuals serving as Security Auditors shall not perform or hold any other trusted role.
Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (such as., configuring, archiving, deleting) that require multi- person control.

5.3 Personnel controls

Personnel Security plays a critical role in GovCA facility's overall security system. Personnel Security shall be designed to prevent both unauthorized access to GovCA facility and CA systems and compromise of sensitive CA operations by CA personnel.

5.3.1 Qualifications, experience, and clearance requirements

GovCA shall identify at least one individual or group responsible and accountable for the operation of the accredited CA. All persons filling trusted roles shall be selected based on loyalty, trustworthiness, and integrity. All trusted roles are required to be held by Kenyan citizens and in accordance with the requirements stipulated in section 5.3.1 of the CPS

5.3.2 Background check procedures

Persons fulfilling Trusted Roles shall pass a comprehensive background check and investigation procedure covering the following areas:

- Employment
- Education
- Place of residence
- Law Enforcement
- 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.
Factors revealed in a background check that should be considered grounds for rejecting candidates for Trusted Roles or for acting against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person
- Highly unfavorable or unreliable professional references
- Certain criminal convictions
- Indications of a lack of financial or personal responsibility

5.3.3 Training requirements

All personnel performing duties with respect to the operation of GovCA or RA shall receive comprehensive training in all operational duties they are expected to perform, including good knowledge of PKI Policies, regulation, and related laws.
In addition, personnel performing duties with respect to the operation of GovCA shall receive comprehensive training or demonstrate competence as described in section 5.3.3 of the CPS.
Documentation shall be maintained identifying all personnel who received training and the level of training completed. Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.

5.3.4 Retraining frequency and requirements

All individuals responsible for PKI Trusted Roles shall be made aware of changes in GovCA, and RA 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 CA software or hardware upgrade, changes in automated security systems, and relocation of equipment. Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Appropriate administrative and disciplinary actions as documented in organization policy shall be taken against personnel who perform unauthorized actions (i.e., not permitted by this CP or other policies) involving GovCA's systems, the certificate status verification systems, and the repository.

GovCA employees failing to comply with this CP, whether through negligence or malicious intent, shall be subject to administrative or disciplinary actions as stipulated in section 5.3.6 of the CPS.

5.3.7 Independent contractor requirements

Contractor personnel filling trusted roles shall be subject to all requirements stipulated in this document. Independent contractors and consultants who have not completed or passed the background check procedures specified above shall be permitted access to GovCA's secure facilities only to the extent they are escorted and directly supervised by people holding trusted roles at all times.

5.3.8 Documentation supplied to CA staff

CA shall provide sufficient documentation to define duties and procedures for each 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 GovCA, and RAs. 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 and made available during compliance audits.

5.4.1 Types of events recorded

A message from any source requesting an action by GovCA, CSS or RA is an auditable event. The audit record must also include message date and time, source, destination, and contents. Where the event cannot be electronically logged, the GovCA or RA shall supplement electronic audit logs with physical logs as necessary.
Details of events to be recorded must meet the minimum requirements stated in section 5.4.1 of the CPS.
All essential events auditing capabilities of GovCA'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, GovCA shall implement manual procedures to satisfy this requirement.

5.4.2 Frequency of processing log

Real-time automated analysis tools should be used. All alerts generated by such a system shall be analyzed.
The audit log shall be reviewed at least once every thirty (30) days and before being archived. All significant events shall be explained in an audit log summary. Actions taken because of these reviews shall be documented.

5.4.3 Retention period for audit log

Audit logs shall be retained on-site until reviewed, as well as being retained for at least ninety (90) days in addition to being archived as described in section 5.5.

5.4.4 Protection of audit log

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing.
Electronic logs shall be protected to prevent alteration and detect tampering. Examples include digitally signing audit records or the use of a data diode to transfer logs to a separate system to prevent modification after the log is written to media.
Physical logbooks shall implement controls to allow for the detection of the removal of pages or deletion of entries.
Security audit data shall be moved to a safe, secure storage location separate from the location where the data was generated.
CA or RA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data.
Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access).
The off-site storage location for audit logs shall be a safe and secure location separate from the location where the data was generated.

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

The audit log collection system may or may not be external to GovCA/CSS/RA system. Automated audit processes shall be invoked at system or application startup and cease only at system or application shutdown.

Audit collection systems shall be configured such that security audit data is protected against loss (such as., overwriting or overflow of automated log files).

5.4.7 Notification to event-causing subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device or application that caused the event.

5.4.8 Vulnerability assessments

Once a year, the GovCA shall assess the vulnerability of its CA system or its components. A routine assessment of GovCA system shall be performed regularly. See Section 6.6.3 detailed information about Life cycle security controls.

5.5 Records archival

GovCA or its RA shall comply with their respective records retention policies.

5.5.1 Types of records archived

GovCA shall make and keep in a trustworthy manner the records relating to the following:

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

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 GovCA itself.

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

GovCA archive records shall be automatically time-stamped as they are created.

5.5.6 Archive collection system (internal or external)

Archive data shall be collected in an expedient manner.

5.5.7 Procedures to obtain and verify archive information

Procedures, detailing how to create, verify, package, transmit, and store GovCA archive information, shall be published in the CPS or a referenced document.

5.6 Key changeover

To minimize risk from compromise of a CA's private signing key may be changed often. From that time on, only the new key will be used to sign CA and subscriber certificates. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected. GovCA's signing key shall have a validity period as described in section 6.3.2. When a CA updates its private signature key and thus generates a new public key, GovCA shall notify all RAs, and subscribers that rely on GovCA's certificate that it has been changed. When the RootCA that distributes self-signed certificates updates its private signature key, GovCA shall generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Key rollover certificates are optional for CAs that do not distribute self-signed certificates.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

CA organizations shall have an Incident Response Plan and a Disaster Recovery Plan.
If compromise of a CA is suspected, certificate issuance by that CA shall be stopped immediately. An independent, third-party investigation shall be performed to determine the nature and the degree of damage. The scope of potential damage shall be assessed to determine appropriate remediation procedures. If a CA private signing key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed.

GovCA shall notify the trust anchor managers in the case of a root CA or notify the superior CA in the case of a subordinate CA if any of the following occur:

- Suspected or detected compromise of any CA system or subsystem
- Physical or electronic penetration of any CA system or subsystem
- Successful denial of service attacks on any CA system or subsystem,
- Any incident preventing a CA from issuing and publishing a CRL or OCSP response prior to the time indicated in the next Update field in the currently published CRL or OCSP response.

5.7.2 Computing resources, software, and/or data are corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this policy shall respond as described in section 5.7.2 of the CPS.

5.7.3 Entity private key compromise procedures

If GovCA signature keys are compromised or lost (such that compromise is possible even though not certain), below are the procedures to follow:

1) The Root CA and its entire member entities shall be notified so that entities may issue CRLs revoking any cross-certificates issued to the compromised CA, new key pair shall be generated by GovCA; and new certificates shall be issued to subscribers also.
2) If GovCA 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) GovCA governing body shall also investigate and report to the Root CA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business continuity capabilities after a disaster

GovCA shall elaborate a clear Disaster Recovery Plan which shall be coordinated with any overarching Disaster Recovery Plan that the broader organization may have. The Disaster Recovery Plan shall identify what procedures are in place to mitigate risks to environmental controls, procedures for annual testing of processes to restore service, individuals on call for this type of activity, and the order of restoral of equipment and services. In the case of a disaster in which GovCA equipment is damaged and inoperative, GovCA operations shall be re-established as quickly as possible, giving priority to the ability to revoke Subscriber's certificates If GovCA cannot re-establish revocation capabilities prior to date and time specified in the nextUpdate field in the currently published CRL issued by GovCA, then the inoperative status of GovCA shall be reported to the trust anchor managers and Superior CA. The trust anchor managers and Superior CA shall decide whether to declare GovCA private signing key as compromised and re-establish GovCA keys and certificates or allow additional time for reestablishment of GovCA's revocation capability.

In the case of a disaster whereby a CA installation is physically damaged, and all copies of GovCA signature key are destroyed as a result, GovCA shall request that its certificates be revoked. GovCA installation shall then be completely rebuilt by re-establishing GovCA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates. Finally, all Subscriber certificates will be re-issued.

In such events, any Relying Parties who continue to use certificates signed with the destroyed private key do so at their own risk, and the risk of others to whom the data is forwarded, as no revocation information will be available (if the CRL signing key was destroyed).

5.8 CA or RA termination

In the event that GovCA terminates its operation, it shall provide termination notice to the Root CA, and all entities shall be given as much advance notice as circumstances permit.

Prior to CA termination, notice shall be provided to all cross-certified CAs requesting revocation of all certificates issued to it.

In addition:

- GovCA shall issue a CRL revoking all unexpired certificates prior to termination. This CRL shall be available until all certificates issued by GovCA expire.
- GovCA, CSS, and RA shall archive all audit logs and other records prior to termination.
- GovCA, CSS, and RA shall destroy all private keys upon termination.
- GovCA, CSS, and RA archive records shall be transferred to an appropriate authority specified in the CPS.
- If a Root CA is terminated, the Root CA shall use secure means to notify the subscribers to delete all trust anchors representing the terminated CA.

6.0 TECHNICAL SECURITY CONTROLS

GovCA private keys are protected within a Hardware Security Module (HSM) meeting at least Level 2 of the Federal Information Processing Standard 140 (FIPS 140). Access to the HSM within GovCA environment is restricted. The HSM is always stored in a physically secure environment and subject to security controls throughout its lifecycle.

6.1 Key pair generation and installation

6.1.1 Key pair generation

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

6.1.2 Private key delivery to subscriber

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.
When CAs or RAs generate keys on behalf of the subscriber, then the private key must be delivered securely to the subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module as described in section 6.1.1 of the CPS.

6.1.3 Public key delivery to certificate issuer

Where key pairs are generated by the subscriber or RA, the public key and the subscriber's identity must be delivered securely (such as., using TLS with approved algorithms and key lengths) to GovCA for certificate issuance. The delivery mechanism shall bind the subscriber's verified identity to the public key.

6.1.4 CA public key delivery to relying parties

The RootCA and GovCA public keys shall be provided to the subscribers acting as relying parties in a secure manner so that it is not vulnerable to modification or substitution. When GovCA updates its signature key pair, GovCA shall publish or distribute the new public key in a secure fashion.

6.1.5 Key sizes

GovCA that generate certificates and CRLs under this CP shall use signature keys of at least 2048 bits for RSA.
GovCA that generate certificates and CRLs under this CP shall use SHA- 512 hash algorithm when generating digital signatures.

6.1.6 Public key parameters generation and quality checking

Public key parameters shall always be generated and validated in accordance with [FIPS 186-4].

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

GovCA shall use a hardware cryptographic module validated to [FIPS 140] Level 3 (or higher), or some other equivalent standard for signing operations. RAs shall use a hardware cryptographic module validated to [FIPS 140] Level 2 (or higher), or some other equivalent standard for signing operations.
Subscribers should use a cryptographic module validated to [FIPS 140], or some other equivalent standard, for all cryptographic operations.

6.2.2 Private key (n out of m) multi-person control

GovCA private keys shall be accessed through multi-person control.
GovCA signing keys shall be backed up only under multi-party control.
Access to GovCA signing keys backed up for disaster recovery shall be under multi-party control.
The names of the parties used for multi-party control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private key escrow

GovCA private keys shall never be escrowed.

6.2.4 Private key backup

The private keys of GovCA are stored in encrypted state and access is only by multi-person control as specified in Section 6.2.2 of this CP. The private keys are backed up under further encryption and maintained on-site and in secure off-site storage.
Subscribers may choose to back up their private keys by backing up their hard drive or the encrypted file containing their keys.

6.2.5 Private key archival

GovCA private signature keys and subscriber private signature keys shall not be archived.

6.2.6 Private key transfer into or from a cryptographic module

GovCA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4.1. At no time shall GovCA private key exist in plaintext outside the cryptographic module. All other keys shall be generated by 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; private keys must never exist in plaintext form outside the cryptographic module boundary. 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

Cryptographic modules may store private keys in any form as long as the keys are not accessible without the use of an authentication mechanism that is in compliance with [FIPS 140] or equivalent standard.

6.2.8 Method of activating private key

The subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered). A device or application may be configured to activate its private key without requiring activation data, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The AOR shall be responsible for ensuring that the system has security controls commensurate with the level of threat in the device's environment. These controls shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

6.2.9 Method of deactivating private key

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, such as., via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CPS. CA cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 Method of destroying private key

Individuals in trusted roles shall destroy CA, RA, and CSS (such as., OCSP server) private signature keys when they are no longer needed. Subscribers shall either surrender their cryptographic module to CA/RA personnel for destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are 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. Physical destruction of hardware is not required.

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 described in Section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

The maximum usage period for the GovCA key pair is of 15 years. GovCA shall not issue a certificate that extends beyond the expiration date of its own certificate and public key. Unless defined by GovCA, a subscriber's certificate shall have a maximum validity period of one (1) year renewable.

6.4 Activation data

6.4.1 Activation data generation and installation

GovCA activation data shall be user-selected (by each of the multiple parties holding that activation data). If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module. RA and subscriber activation data may be user selected. The strength of the activation data shall meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in [FIPS 140], or some other equivalent standard. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation data protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be either:

- memorized,
- biometric in nature, or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module and shall not be stored with the cryptographic module

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

CA and RA operating under this CP shall follow the rules and guidelines issued by GovCA for the information security requirements. 6.5.1

6.5.1 Specific computer security technical requirements

GovCA shall have a formal Information Security Policy that documents the policies, standards and guidelines relating to information security. The computer security functions listed below are required. These functions may be provided by the operating system or through a combination of operating system, software, and physical safeguards.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

GovCA system shall be implemented and tested in a non-production environment prior to implementation in a production environment. No change shall be made to the production environment unless the change has gone through the change control process as defined for the system baseline. To prevent incorrect or improper changes to GovCA system, GovCA system shall require multi- party control for access to GovCA system when changes are made.

6.6.2 Security management controls

GovCA shall maintain a list of acceptable products (third party systems/software) and their versions. Mechanisms and/or procedures shall be in operation designed to prevent the installation and execution of unauthorized software.

6.6.3 Life cycle security controls

For flaw remediation, the GovCA shall scan all online CA systems for vulnerabilities using at least one vulnerability scanner every one (1) month. Each vulnerability found shall be entered into a vulnerability tracking database, along with the date and time of location, and shall be remediated within 72 hours. Remediation shall be entered into the vulnerability database as well (including date and time).
GovCA shall monitor relevant notification channels daily for updates to packages installed on CA systems (including networking hardware). GovCA shall have a plan for receiving notification of software and firmware updates, for obtaining and testing those updates, for deciding when to install them, and finally for installing them without undue disruption.

6.7 Network security controls

All access to GovCA 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

Asserted times shall be accurate to within fifteen (15) minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as per Section 5.4.1.

7.0 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.
Each certificate issued by GovCA shall be given a serial number consisting of a unique, positive integer, not longer than 20 octets. They shall contain at least a 20 bits random number.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

GovCA shall use standard certificate extensions that comply with RFC [3280/5280].
The key usage extension (keyUsage) shall be marked as critical. Certificates shall assert the minimum number of key usages required for functionality. Signature certificates shall assert digital Signature. Encryption certificates shall assert either keyEncipherment or keyAgreement. GovCA certificates shall assert keyCertSign and cRLSign. Certificates shall assert the minimum number of extended key usages (extKeyUsage) required for functionality. The anyExtendedKeyUsage key purpose shall not be asserted. The basic constraints extension (basicConstraints) shall be marked critical in GovCA issued certificates, and the path length constraint should be set to two (2).

7.1.3 Algorithm object identifiers

Certificates issued under this CP shall use the Object Identifier (OID) related with the recommend appropriate algorithms.

7.1.4 Name forms

The subject field in certificates issued under this policy shall be populated with an X.500 distinguished name as specified in section 3.1.
The issuer field of certificates issued under this policy shall be populated with a non-empty X.500 Distinguished Name as specified in section 3.1.

7.1.5 Name constraints

GovCA may assert name constraints in its certificates.

7.1.6 Certificate policy object identifier

Certificates issued under this CP shall use the OID number that points to the correct CA as well as Certificate Policy as specified by the Policy Authority (RootCA)

7.1.7 Usage of Policy Constraints extension

GovCAs may assert policy constraints in CA certificates.

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

CRLs issued by a CA under this policy shall conform to the CRL profile specified in RFC [3280/5280].

7.2.1 Version number(s)

GovCA operating under this CP shall issue X.509 Version two (2) CRLs.

7.2.2 CRL and CRL entry extensions

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

7.3 OCSP profile

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

7.3.1 Version number(s)

GovCA shall use at minimum OCSP version 1.

7.3.2 OCSP extensions

Detailed CRL/OCSP profiles addressing the use of each extension are specified in RFC 2560.

8.0 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

GovCA and its RAs shall be subject to a periodic compliance audit at least once per year in respect to the Policy Authority (RootCA) recommendation.

8.2 Identity/qualifications of assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with GovCA's CPS and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity.
In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 Assessor's relationship to assessed entity

The compliance auditor either shall be a private firm that is independent from the entities (GovCA and RAs) being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. To ensure independence and objectivity, the compliance auditor must not have served the entity in developing or maintaining the entity's CA Facility or certificate practices statement within the last two (2) years. The Policy Authority shall determine whether a compliance auditor meets this requirement.

8.4 Topics covered by assessment

The purpose of a compliance audit is to verify that a GovCA and its recognized RAs comply with all the requirements of the current versions of GovCA's CP and CPS. All aspects of GovCA/RA operation shall be subject to compliance audit inspections.
The audit must conform to industry standards, cover GovCA's compliance with its business practices disclosure, and evaluate the integrity of GovCA's PKI operations.
The audit must verify that GovCA is compliant with this CP.

8.5 Actions taken as a result of deficiency

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI, the following actions shall be performed:

- The compliance auditor shall document the discrepancy.
- The compliance auditor shall promptly notify notify the parties identified in section 8.6 of the discrepancy.

- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the appropriate PKI Authorities, as defined in Section 1.3.1.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Policy Authority may decide to temporarily halt operation of the GovCA or RA, to revoke a certificate issued to GovCA or RA or take other actions it deems appropriate. The Policy Authority shall provide to the GovCA its procedures for making and implementing such determinations.

8.6 Communication of results

An Audit Compliance Report shall be provided to CEO – ICTA & DG Communication Authority. The Audit Compliance Report and identification of corrective measures shall be provided to the appropriate PKI Authorities within thirty (30) days of completion. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

9.0 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

GovCA or RA, operating under this CP shall be allowed to charge fees for the issuance of certificates as per the Policy Authority guidelines.

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

GovCA shall publish certificates and the CRL as per Section 2.4 of this policy. Thus, GovCA shall not charge additional fees for access to this information.

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

This CP contains no limits on the use of certificates issued by GovCA under the policy.
Entities, acting as relying parties, with the help of the Policy Authority shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

GovCA shall protect the confidentiality of sensitive business information stored or processed on GovCA systems that could lead to abuse or fraud.
Public access to GovCA organizational information shall be determined by the GovCA.

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

9.4 Privacy of personal information

9.4.1 Privacy plan

GovCA shall develop, implement, and maintain a privacy plan. The privacy plan shall document what personally identifiable information is collected, how it is stored and processed, and under what conditions the information may be disclosed.

9.4.2 Information treated as private

GovCA shall protect all subscriber personally identifiable information from unauthorized disclosure. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by GovCA shall not be released except as allowed by the privacy plan in section 9.4.1 and by the laws of the Republic of Kenya.

9.4.3 Information not deemed private

Information included in certificates (shown in Section 7 of this CP) shall not be deemed private and will not be subject to the protections outlined in Section 9.4.2.

9.4.4 Responsibility to protect private information

Sensitive information must be stored securely and may be released only in accordance with other stipulations in section 9.4.

9.4.5 Notice and consent to use private information

GovCA may not provide any notice or obtain the consent of the subscriber to release private information in accordance with other stipulations of section 9.4.

9.4.6 Disclosure pursuant to judicial or administrative process

GovCA shall not disclose any private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction according to established legal procedure and guideline.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

GovCA shall not knowingly violate intellectual property rights held by others. The intellectual property rights held by other individual, organization or entities shall always be upheld by GovCA or RA.

9.6 Representations and warranties

9.6.1 CA representations and warranties

GovCA procedures shall be implemented in accordance with this CP, and any certificates issued that assert the policy OIDs identified in this CP are issued in accordance with the stipulations of this policy.
GovCA shall conform to the stipulations of this document, including:

- Providing the CP and CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance to the stipulations of the CP and the CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an approved CP and CPS.
- Including only valid and appropriate information in certificates and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.

- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3.
- Operating or providing for the services of an on-line repository and informing the repository service provider of their obligations if applicable.

9.6.2 RA representations and warranties

An RA that performs registration functions as described in this policy shall comply with the stipulations of this policy and comply with other policies approved by the Policy Authority for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy shall conform to the stipulations of this document, including:

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificate requests and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
- Ensuring that obligations are imposed on subscribers in accordance with section 9.6.3, and that subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber representations and warranties

A GovCA subscriber (or AOR for device certificates) shall be required to acknowledge acceptance of the subscriber's responsibilities and requirement to meet respecting protection of the private key and use of the certificate before being issued the certificate.
Subscribers shall:

- Accurately represent themselves in all communications with the PKI authorities.
- Always protect their private key(s), in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notification shall be made directly or indirectly through mechanisms consistent with the
- CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).

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

All relying parties (including subscribers) operating under this policy shall not disclaim any responsibilities described in this CP.

9.8 Limitations of liability

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

- Revoked,
- Expired,
- Used for unauthorized purposes,
- Tampered with,
- Compromised, or
- Subject to misrepresentation, misleading acts, or omissions.

9.9 Indemnities

Subscribers and relying parties shall agree to indemnify and hold GovCA or its RA harmless from any claims, actions or demands that are caused by the use or publication of a certificate and that arises from:

- Any false or misleading statement of fact by the subscriber,
- Any failure by the subscriber to disclose a material fact, if such omission was made negligibly or with the intent to deceive,
- Any failure on the part of the subscriber to protect its private key and/or token if applicable or to take the precautions necessary to prevent the compromise, disclosure, loss, modification, or unauthorized use of the subscriber's private key; or
- Any failure on the part of the subscriber to promptly notify GovCA or RA of the compromise, disclosure, loss, modification, or unauthorized use of the subscriber's private key once the subscriber has actual or constructive notice of such event.

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

GovCA shall establish appropriate procedures for communications with RAs operating under this policy via contracts or memoranda of agreement as applicable.

9.12 Amendments

9.12.1 Procedure for amendment

GovCA shall review this CP at least once every year. Corrections, updates, or changes to this CP shall be publicly available. Suggested changes to this CP shall be communicated to the contact in section 1.5.2; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2 Notification mechanism and period

Whenever the CP is amended, it shall be published within 30 days of the date the amendment took place and all known concerned parties (OA staff, relying parties, subscribers) shall be notified. The update version shall be distributed electronically to RAs and other bodies/entities. The notification shall contain the final date for receipt of comments and the proposed effective date of change.

Older versions of the CP should be made available for reference and comparison.

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. The Policy Authority (RootCA/Controller) shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy.

9.14 Governing law

The issuance and use of certificates under this CP shall be covered by the Computer Mis-use & Cybercrimes law governing Information and Communication Technologies and any other applicable laws in Kenya

9.15 Compliance with applicable law

GovCA or RA and other relying entities operating under this CP, shall use it in compliance with any applicable laws under the Government of Kenya.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation

9.16.5 Force Majeure

GovCA or its RA accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as, but not limited to the following:

- Acts of God,
- Acts of War,
- Acts of Terrorism,
- Epidemics,
- Power or telecommunication services failure,
- Earthquake
- Fire, or
- Any other natural or man-made disasters.

9.17 Other provisions

No stipulation

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


ICT
Authority