Certification Practice Statement

“SINAM” Certificate Authority (SCA)

VERSION CONTROL

Date	Version	Editor	Change
20.05.2025	1.0	Uzeyir Gurbanli	First draft based on the workgroup discussion
25.05.2025	2.0	Islam Ahmadov	Updated Version
26.05.2025	2.1	Islam Ahmadov	Minor changes concerning revocation

1. INTRODUCTION

This document is Certification Practice Statement (CPS) establishes practices that the SCA employs during issuing and managing its digital certificates. The CPS sets forth business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing digital certificates within "SINAM" Certification Authority (SCA) and providing associated trust services for participants of Public Key Infrastructure environment. This CPS applies to all certificates issued by the SCA.

This CPS complies with International standards. The headings in this document follow the structure set forth in Internet Engineering Task Force Request for Comment (RFC) 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

1.1. Overview

SCA is intended to issue electronic certificates and manage lifecycle of the issued electronic certificates. Individuals as well as legal entities are eligible to get trusted electronic certificates within the framework of procedural and operational requirements described in this CPS and the related CP Certification Policy (CP).

This CPS is intended for:

- Individuals and legal entities that going or already issued digital certificates to understand the practices requirements for the lifecycle management of the Certificates issuing by the SCA.
- Relying parties, that need to understand practice and policy of SCA in providing electronic certificate related services.

1.2. Document name and identification

This document title: Certification Practice Statement for SCA.

Document date: May 2025
The Object Identifier (OID) assigned: 1.3.6.1.4.1.63647.2.1

OID specified in chart below:

OID Component	Meaning
1.3.6.1	Internet attribute of IANA
4	Private entity attribute of IANA
1	Private enterprise attribute of IANA
63647	IANA PEN (Private Enterprise Number) of SINAM
2.1	CPS version of SINAM

1.3. PKI Participants

This section identifies and describes main participants within the Public Key Infrastructure interacting with SCA .

1.3.1.Certification authorities

The SCA represent the second level CA subordinated to Kenya ROOT CA owned and operated by Communications Authority of Kenya. The SCA issues digital certificates to subscribers for purposes stipulated within this CP.

1.3.2. Registration authorities

SCA may designate specific Registration Authority (RA) to perform identification, authentication, and registration of Subscribers, as well as accepting applications for certificate blocking and/or revocations as defined in this CPS and corresponding CP. Registration Authority functions can be delegated to regional government institutions as well as to Huduma service centers with appropriate agreements between SCA and these institutions.

1.3.3.Subscribers

Subscribers are individuals or legal entities whose name appears in corresponding Certificate under subject attribute. Subscribers responsible to use their key pair and certificate in accordance with this CPS and corresponding CP.

1.3.4.Relying parties

Relying party is any entity involved in a transaction based on electronic signature and certificates or other certification services provided by SCA. The Relying party use the information in the certificate to determine the suitability of the certificate for a particular use, including the following areas:

- Purpose for which a certificate is used.
- Digital signature verification responsibilities.
- Revocation and suspension checking responsibilities.
- Acknowledgement of applicable liability caps and warranties.

1.3.5.Other participants

1.3.5.1. Executive Power Body

The Communications Authority of Kenya acting as executive power body and responsible for Certification Service Centers accreditation. Accreditation process performed in accordance with Law of the Republic of Kenya on electronic signature and electronic document (Legislation).

1.3.5.2. Certificate Service Center

Certificate Service Center is a legal entity or physical person dealing as entrepreneurship with no legal person founding, providing different certificate services set by the Legislation.

1.3.5.3. Accredited Certificate Service Center

Certificate Service Centers accredited by the Executive Power Body to provide certification services to Subscribers. The SINAM as ACSC is bound to act according to the Legislation and the terms of this CPS and corresponding CP.

1.4. Certificate usage and applicability

Certificates issued under this policy shall be used for::

- **[Authentication]** (e.g., user login, VPN access).
- **[Digital Signatures]** (e.g., document signing, code signing).
- **[Encryption]** (e.g., email encryption, TLS/SSL for secure communications).
- **[Device Identity]** (e.g., IoT devices, servers).

1.4.1.Appropriate Certificate Uses

The SCA's certificates issued under this CPS may be used for Subscriber identification, accountability and non-repudiation in digital communications and transactions.

1.4.2.Prohibited Certificate Uses

All certificates issued under this CPS are not used for purposes other than what is allowed in this CPS.

The certificates issued by the SCA shall not be used for purposes that violate the Kenya Republic or International Law.

1.4.3.Legal significance

The certificates issued under this CPS allow legal interpretations and admissible as evidence in legal proceedings.

The SINAM is indemnified from any claims arising from prohibited or inappropriate use of certificates.

1.5. Policy administration

The authority and responsibility for this CPS maintenance, endorsement, and issuance rests with SINAM.

1.5.1.Update Procedure

This CPS and corresponding CP are prepared and reviewed by the SINAM. During review, SINAM determines whether the change is minor or major. The determination is based on an assessment of risk from the changes proposed. All modifications are enforced once the SINAM is completed.

- Minor modifications versions will be incremented in tenths (i.e., replace v1.0 with v1.1).
- Major modifications versions will be incremented in whole number increments (i.e., replace v1.0 with v2.0).

This CPS and corresponding CP and the updates shall be published at official web site of SINAM https://www.sinam.net/sca/ no less than 30 days prior to taking effect

The review and approval process assure that this CPS and corresponding CP adheres to RFC 3647.

1.5.2.Contact information

In case of any question regarding this document, contact SINAM.

- Tel: +994 12 510 11 00
- Email: info@sinam.net
- Address: AZ1141, Baku city, B.Vahabzade 9

1.6. Definitions and acronyms

A list of definitions and acronyms provided in Appendix A of this CPS.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

The SCA responsible for arrangement and maintaining own publicly accessible online repository which contain its documentation (CP, CPS, and other regulatory or legal documents).

The online repositories for SCA are publicly available at the URL: https://sinam.net/en/sca

2.2. Publication of certification information

The SCA publishes certification information in its own repository.

2.3. Time or frequency of publication

Approved versions of documents are published on the repository within 24 hours.

2.4. Access controls on repositories

Information published on a repository is publicly available. Excluding reasonable scheduled maintenance and unforeseen failures, the rate of repository availability meets 24/7 basis.

The SCA provides unrestricted read-only access into its repositories to public. The SCA implements logical and physical controls to prevent unauthorized write access to such repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1.Types of Names

Every certificate issued under this CPS has a clear distinguishable and unique Distinguished Name (DN) in the certificate subjectName field, which are described in corresponding CP.

The subject name of the applicants are compatible with X.501 standard.

3.1.2.Need for Names to be Meaningful

The subject name represents specific end entity in a clear manner and reasonably associated with its authenticated name.

3.1.3.Anonymity or Pseudonymity of Subscribers

No anonymity or pseudonymity is supported.

3.1.4.Rules for Interpreting Various Name Forms

Names are ASCII encoded and contain only alphanumeric, dot and underscore characters in accordance with section 3.1.1.

3.1.5.Uniqueness of Names

See section 3.1.1. and section 3.1.2

3.1.6.Recognition, Authentication, and Role of Trademarks

Certificate Applicants cannot use names in their application that violate the Intellectual Property Rights of others. However, the SCA and its designated RAs do not check if the applicant has the right to use the name they're requesting.

The SCA may revoke a certificate upon receipt of a properly authenticated order from a court requiring the revocation of a certificate or certificates containing a disputed name.

3.2. Initial identity validation

3.2.1.Method to Prove Possession of Private Key

The SCA is responsible for verifying that the certificate applicant possesses the private key that corresponds to the public key being certified. This verification is done by checking the signature on the certificate request, which is expected to be signed using the private key associated with the public key being certified.

3.2.2. Authentication of Organization Identity

If the certificate pertains to an organization, then a representative authorized by the organization applies for the certificate. The SCA or its designated RAs authenticates the identity and authorization of this representative.

To obtain an organizational certificate, the applicant provides certain documents, including registration documents issued by a government entity responsible for company registrations and a document that demonstrates the applicant's authority to act on behalf of the organization.

The request is accompanied by an identity proof as described in section 3.2.3.

3.2.3. Authentication of Individual Identity

Authentication of applicating representatives' individual identity is performed by SCA or its designated RAs in accordance with Legislation. The verification process requires the applicant to provide national identity card or passport.

3.2.4. Non-Verified Subscriber Information

Non-verifiable subscriber's information is not included in certificates issuing under this CPS and corresponding CP.

3.2.5. Validation of Authority

The SCA and its designated RAs are responsible for verifying that the applicant possesses rights, privileges, or authorizations to apply for the certificate prior to its issuance. See section 3.2.2. and section 3.2.3.

3.2.6. Criteria for Interoperation

No stipulation.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

The SCA requires subscribers to generate a new key pair once every three years. When re-keying, the SCA will issue a new certificate with the same attributes as the previous one, but with a different key pair and serial number. The new certificate may have a new validity period or use the same period as the old certificate.

If subscribers possess a valid authentication certificate, they may use it to identify themselves to the SCA. Otherwise, they follow the same identification and authentication procedures as when they first time obtained certificate.

3.3.2. Identification and authentication for re-key after revocation

See section 3.3.1.

3.4. Identification and authentication for revocation request

Subscriber’s revocation requests are always authenticated. Requests to revoke a certificate may be authenticated using that certificate’s corresponding Public Key, regardless of whether the Private Key has been compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate application

This section outlines the conditions for initial application for getting a certificate from the SCA through its designated RA. When applicant applies for a certificate, the RA verifies their authorization and identity and inform the SCA that the applicant meets the authentication criteria and what information should be included in the certificate. When the SCA receives the confirmation and certificate information from the RA, it will check if it is coming from an authorized RA and perform private key ownership verification by the CA. The SCA will then issue the certificate for the applicant and send it to them and/or the requesting RA.

4.1.1. Who can submit a certificate application

The submission of certificate requests can be made by either the Applicant or a person who has been given the authority to request certificates on behalf of the Applicant. It is the responsibility of the Applicant to ensure the accuracy and validity of any information provided by themselves or their authorized representative to the SCA.

4.1.2. Enrolment process and responsibilities

To obtain a requested certificate, the subscriber ratifies a specific agreement made for subscribers. The certificate will only be issued as per the following:

1. The Applicant sends the request to SCA through its designated RAs;
2. The RA validates the application and sends it to the SCA for issuance;
3. The SCA issues the certificate and delivers it in a secure format.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

See section 3.2.

4.2.2. Approval or rejection of certificate applications

To obtain a subscriber certificate, the applicant passes the identification and authentication process. If the necessary Subscriber information cannot be authenticated, or the applicant does not provide the required supporting documentation or respond to notices within the given timeframe, the certificate application may be rejected. Additionally, if the RA believes that issuing a certificate to the applicant may harm SCA's reputation or the applicant cannot prove ownership of the private key, the application may also be rejected.

4.2.3.Time to Process Certificate Applications

The SCA will process certification applications within a reasonable commercial timeframe, as outlined in this CPS or any agreement with PKI participants. However, the SCA cannot be held responsible for delays caused by the applicant or for circumstances beyond the control of the CA.

4.3. Certificate issuance

4.3.1.CA Actions during Certificate Issuance

Before issuing a certificate, the applicant first accepts the terms of a Subscriber Agreement and complete the application form. Once the registration process is successfully completed and the request is validated, the SCA will create and sign the certificate, provided that all necessary requirements have been met, and make the certificate available to the subscriber.

4.3.2.Notification to Subscriber by the CA of Issuance of Certificate

The SCA informs subscribers that their certificates have been created and provide access to them either directly or through its designated RA.

4.4. Certificate acceptance

4.4.1.Conduct Constituting Certificate Acceptance

The acceptance of a certificate depends on the agreements, the requirements stated in this CPS and corresponding CP, and the relevant agreements related to the certificate issuance. When a person uses or depends on a certificate, they agree to be bound by the terms and conditions of the CP, this CPS, and applicable agreements, which is an irrevocable agreement.

4.4.2.Publication of the Certificate by the CA

The SCA does not make end-user certificates publicly available, but instead only shares them with the individual or entity that requested them.

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

No stipulation.

4.5. Key pair and certificate usage

4.5.1.Subscriber Private Key and Certificate Usage

Subscribers are required to use their Certificates only for authorized and lawful purposes in compliance with the Subscriber Agreement, this CPS, and applicable laws. They ensure that their Private Keys are not accessed by anyone else and inform the SCA and/or its designated RAs in case the private key is compromised or suspected to be compromised. Additionally, after the certificate's expiration or revocation, subscribers cease using the associated private key(s).

4.5.2.Relying Party Public Key and Certificate Usage

When utilizing a subscriber's public key and associated certificate, a relying party fulfills these duties:

- Verify that the key is suitable for the intended purpose as stated in this CPS, and that such usage aligns with the relevant certificate information, including but not restricted to, the key usage, extended key usage, and certificate policies extension fields.
- Confirm the certificate's status by referring to the appropriate and up-to-date CRLs or any other services indicated in SCA’s Subscriber certificates.

4.6. Certificate renewal

Certificate Renewal means the issuance of a new Certificate without changing the Public Key or any other information in the Certificate. The Certificate Renewal service is not supported under this CPS.

4.6.1.Circumstance for Certificate Renewal

No stipulation.

4.6.2.Who May Request Renewal

No stipulation.

4.6.3.Processing Certificate Renewal Requests

No stipulation.

4.6.4.Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5.Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6.Publication of the renewal certificate by the CA

No stipulation.

4.6.7.Notification of certificate issuance by the CA to other entities

No stipulation.

4.7. Certificate re-key

Certificate Re-Key is when all the identifying information from CA Certificates is duplicated in a new

Digital Certificate, but there is a different public key and a different validity period. The Certificate Re-Key service is not supported under this CPS.

4.7.1.Circumstance for Certificate Re-Key

No stipulation.

4.7.2.Who May Request Certification of a New Public Key

No stipulation.

4.7.3.Processing Certificate Re-Keying Requests

No stipulation.

4.7.4.Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5.Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation.

4.7.6.Publication of the Re-Keyed Certificate by the CA

No stipulation.

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

No stipulation.

4.8. Certificate modification

Certificate modification is performed when change occurs in any of the information of an existing certificate. After modification, the original certificate may or may not be revoked but it’s not allowed to be rekeyed, renewed, or modified anymore. The Certificate modification service is not supported under this CPS.

4.8.1.Circumstance for Certificate Modification

No stipulation.

4.8.2.Who May Request Certificate Modification

No stipulation.

4.8.3.Processing Certificate Modification Requests

No stipulation.

4.8.4.Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5.Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6.Publication of the Modified Certificate by the CA

No stipulation.

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

No stipulation.

4.9. Certificate revocation and suspension

4.9.1.Circumstances for Revocation

The SCA has the authority to revoke Subscribers' Certificates for several reasons, which are not limited to:

- Failure by the Subscriber to fulfill their duties under this CPS or other applicable laws, regulations, or agreements;
- The SCA determines that a Certificate was issued incorrectly as per this CPS;
- The Subscriber or another authorized agent requests revocation of their Certificate due to suspected compromise of the Subscriber's private key, loss or theft of the Subscriber's cryptographic storage device or no longer requiring the certificate;
- The SCA will revoke a Subscriber's Certificate if they are no longer part of the organization;
- Termination of the Registration Authority's Agreement.

4.9.2.Who can Request Revocation

The following entities can request revocation of a Certificate:

- Communications Authority of Kenya
- SINAM

4.9.3.Procedure for Revocation Request

To revoke a certificate, one specifies which certificate is being revoked, provides a reason for the revocation, and ensure that the request is authenticated. The SCA and its designated RA verifies both the request and the requester's authorization in accordance with relevant agreements.

4.9.4.Revocation Request Grace Period

Upon a revocation request has been verified it applies immediately.

4.9.5.Time within which must process the revocation request

See section 4.9.4.

4.9.6.Revocation Checking Requirement for Relying Parties

Relying parties complies with the signature validation requirements defined in this CPS.

4.9.7.CRL Issuance Frequency (if applicable)

See corresponding CP.

4.9.8.Maximum Latency for CRLs (if applicable)

See corresponding CP.

4.9.9.On-Line Revocation/Status Checking Availability

See corresponding CP.

4.9.10. On-Line Revocation Checking Requirements

See corresponding CP.

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

The certificate status service is available from CRL's in the repositories and via an OCSP responder.

4.10.1. Operational Characteristics

No stipulation.

4.10.2. Service Availability

Public service of certificate status check available 24/7/365.

4.10.3. Optional Features

No stipulation.

4.11. End of subscription

No stipulation.

4.12. Key escrow and recovery

Key escrow and recovery are not allowed.

4.12.1. Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This section describes non-technical security controls requirements to be applied by SCA.

5.1. Physical controls

The SCA implements physical and environmental security policies for the systems used in certificate issuance and management. These policies address various concerns such as controlling physical access, protecting against natural disasters and fire hazards, preparing for failures of utilities such as power and telecommunications, preventing building collapse, and safeguarding against theft, burglary, and potential disasters. Furthermore, appropriate measures are taken to prevent any harm, damage, or loss to assets, minimize disruptions to business activities, and prevent theft or misuse of information and information processing facilities.

5.1.1.Site Location and Construction

The SCA operator secure premises are located in an area appropriate for high-security operations.

5.1.2.Physical Access

The site for SCA satisfies the following requirements:

- manually or electronically always monitored for unauthorized intrusion.
- access to the server rooms is limited to those personnel identified on an access list.
- dual access control implemented to the server rooms.
- all personnel not on the access list are properly escorted and supervised.
- site access log is maintained and inspected periodically.

5.1.3.Power and Air Conditioning

Power supply and air conditioning in use provides high degree of redundancy.

5.1.4.Water Exposures

The site for the SCA is protected from any water exposures.

5.1.5.Fire Prevention and Protection

The site for the SCA implements detection and protection measures against fire exposures.

5.1.6.Media Storage

Backups and electronic media utilized by SCA for its operations are stored securely.

5.1.7.Waste Disposal

To prevent unwanted disclosure of waste that could contain sensitive data related to SCA is disposed in secure manner.

5.1.8.Off-Site Backup

The SCA maintains backup of critical system data or any other sensitive information, including audit data, in a secure off-site facility.

5.2. Procedural controls

The SCA follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties related.

5.2.1.Trusted Roles

The SCA's staff involved in infrastructure operations, administrators, security officers, auditors and any other operations that materially affect such operations are considered as serving in a trusted position.

The SCA conducts appropriate background check of all members of staff who are candidates to serve in trusted roles.

5.2.2.Number of Persons Required per Task

The SCA implements security controls about the duties and performance of the members of its staff.

5.2.3.Identification and Authentication for Each Role

The SCA ensures that all actions within the PKI infrastructure could be attributed to the specific system and the member staff that has performed particular action.

5.2.4.Roles Requiring Separation of Duties

The SCA applies dual control for all critical functions.

5.3. Personnel controls

The SCA applies certain security controls about the job duties and performance of its staff.

5.3.1.Qualifications, Experience, and Clearance Requirements

The SCA performs checks to evaluate the background, qualifications, and experience required to perform specific tasks.

5.3.2.Background Check Procedures

The SCA makes the relevant checks to prospective employees by means of status reports issued by a government authority or third-party feedback memos.

5.3.3.Training Requirements

The SCA defines training plan for its personnel on annually basis.

5.3.4.Retraining Frequency and Requirements

The SCA applies continuity education approach to ensure updates in the knowledge of the personnel.

5.3.5.Job Rotation Frequency and Sequence

No stipulation.

5.3.6.Sanctions for Unauthorized Actions

The SCA defines playbook with set of actions and sanctions to internal and external personnel who breached Cyber Security policies.

5.3.7.Independent Contractor Requirements

For SCA applies for independent subcontractors and their personnel the same background checks as the SCA 's personnel.

5.3.8.Documentation Supplied to Personnel

The SCA makes available to personnel only that documentation, trainings or other material required to perform job duties well.

5.4. Audit logging procedures

The SCA enforces all major event logging in all critical information systems.

5.4.1.Types of Events Recorded

The SCA implements and properly applies event monitoring system with workbook automation.

5.4.2.Frequency of Processing Log

The SCA enforces all major event logging in all critical information systems.

5.4.3.Retention Period for Audit Log

The SCA stores and retains all logged information for a year.

5.4.4.Protection of Audit Log

The SCA arranges collection and external storage for logged information.

5.4.5.Audit Log Backup Procedures

The SCA performs regular backup of audit trails.

5.4.6.Audit Collection System.

The SCA utilizes internal system for audit archive collection (log collection).

5.4.7.Notification to Event-Causing Subject

The SCA implements and properly applies event monitoring system with workbook automation.

5.4.8.Vulnerability Assessments

The SCA performs regular vulnerability assessments for external and internal infrastructure.

5.5. Records archival

The SCA defines archive operations regulatory.

5.5.1.Types of Records Archived

The SCA defines archive operations regulatory.

5.5.2.Retention Period for Archive

The SCA defines archive operations regulatory.

5.5.3.Protection of Archive

The SCA defines archive operations regulatory.

5.5.4.Archive Backup Procedures

The SCA defines archive operations regulatory.

5.5.5.Requirements for Time-Stamping of Records

The SCA defines guidelines for information security record management and implements then in to cyber security infrastructure.

5.5.6.Archive Collection System (Internal or External)

The SCA defines archive operations regulatory.

5.5.7.Procedures to Obtain and Verify Archive Information

The SCA defines archive operations regulatory.

5.6. Key changeover

No stipulation.

5.7. Compromise and disaster recovery

The SCA develops specific Disaster Recovery Plan.

5.7.1.Incident and Compromise Handling Procedures

The SCA develops and implement cyber incidents ticketing solution and playbooks for security incidents and compromise events handling.

5.7.2.Computing Resources, Software, and/or Data are Corrupted

The SCA develops specific Disaster Recovery Plan.

5.7.3.Entity Private Key Compromise Procedures

The Disaster Recovery Plans (DRP) include playbook for the case when SCA's private key is compromised or suspected to be compromised.

5.7.4.Business Continuity Capabilities after a Disaster

The SCA deploys the capability to recover its mission critical operations immediately following a disaster with full support for all the key functions.

5.8. CA or RA termination

The SCA's termination procedures are performed in accordance the Kenyan legislation.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1.Key Pair Generation

The SCA key pair are generated through dedicated Key Generation Ceremony. The SCA private keys are protected within a hardware security module (HSM) that conformant to FIPS 140-2 at least level 3.

To ensure the security the key pairs are either generated or safeguarded in cryptographic modules that meet at least FIPS 140-2 Level 2 standards.

6.1.2.Private Key Delivery to Subscriber

The SCA is responsible for providing Subscriber private keys in a secure format. This secure format could be in the form of cryptographic tokens or smartcards, especially when the keys are generated in cryptographic hardware.

6.1.3.Public Key Delivery to Certificate Issuer

The Subscriber's public keys are delivered to SCA using industry standard secure protocol.

6.1.4.CA Public Key Delivery to Relying Parties

SCA ensure that their Subscribers and Relying Parties receive and maintain the trust anchor in a trustworthy manner.

6.1.5.Key Sizes

For details, refer to corresponding CP.

6.1.6.Public Key Parameters Generation and Quality Checking

The SCA generates key pairs that adhere to the best industry standards and employs appropriate methods to verify that the Subscriber key pairs are appropriate.

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

For details, refer to corresponding CP.

6.2. Private key protection and cryptographic module engineering controls

6.2.1.Cryptographic Module Standards and Controls

Cryptographic modules, smartcards or tokens employed for private key protection issued by the SCA comply with FIPS-PUB 140-2 "Security Requirements for Cryptographic Modules".

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

No stipulation.

6.2.3.Private Key Escrow

No private keys are escrowed.

6.2.4.Private Key Backup

The private keys are not backed up by SCA.

6.2.5.Private Key Archival

Subscriber's private keys are not archived by SCA.

6.2.6.Private Key Transfer into or from a Cryptographic Module

The SCA prohibits the transfer of Private Keys to and from cryptographic modules or devices. Any such keys generated within these secure cryptographic devices remain within them and not be transferred outside of them.

6.2.7.Private Key Storage on Cryptographic Module

The Private Keys are in devices that comply with FIPS 140-2 level 2 standards.

6.2.8.Method of Activating Private Key

To activate their subscriber private keys, the subscriber provides the passphrase that was set during the initial certificate generation process.

6.2.9.Method of Deactivating Private Key

Activated subscriber private keys will not be left unattended. It is the responsibility of subscribers to deactivate their private keys by logging out of the cryptographic device or by having them automatically deactivated after a period of inactivity as configured.

6.2.10. Method of Destroying Private Key

No stipulation.

6.2.11. Cryptographic Module Rating

No stipulation.

6.3. Other aspects of key pair management

6.3.1.Public Key Archival

The public key is archived as part of the certificate archive process.

6.3.2.Certificate Operational Periods and Key Pair Usage Periods

For details, refer to corresponding CP.

6.4. Activation data

6.4.1.Activation Data Generation and Installation

The strength of the activation data, along with any other access control measures, is sufficient to safeguard the private keys. The activation data is to be chosen by the user.

6.4.2.Activation Data Protection

The activation data is safe from any disclosure or compromise. If the data is written down, it will be secured at the same level as the data that the cryptographic device is used to protect, and not stored with the cryptographic device.

6.4.3.Other Aspects of Activation Data

No stipulation.

6.5. Computer security controls

6.5.1.Specific Computer Security Technical Requirements

The computer security 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

The SCA software is certified under the Common Criteria or ITSEC.

6.6. Life cycle technical controls

6.6.1.System Development Controls

The SCA's design, installation, and operation is documented by qualified personnel. The SINAM operational personnel develop and produce appropriate qualification documentation establishing that SCA components are properly installed and configured and operate in accordance with the technical specifications.

6.6.2.Security Management Controls

The configuration of the SCA systems as well as any modifications and upgrades are documented

and controlled. There is a mechanism for detecting unauthorized modification to software or configuration. A formal configuration management methodology is used for installation and ongoing maintenance of the system.

6.6.3.Life Cycle Security Controls

No stipulation.

6.7. Network security controls

The SCA employs appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. These network security controls include effective firewall management, including port restrictions and IP address filtering. Any boundary control devices used to protect the network on which PKI equipment is hosted denies all but the necessary services to the PKI equipment.

6.8. Time-stamping

All SCA components regularly synchronize with a time service. A dedicated authority, such as a timestamping authority, may be used to provide this trusted time.

Time derived from the time service is used for establishing the time of:

- Initial validity time of the SCA's certificate.
- Revocation of the SCA's certificate.
- Posting of CRL updates.
- Issuance of Subscriber end entity.
- Certificates.
- OCSP response.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as stipulated in Section 5.4.1. When providing a certified electronic timestamp service, SCA refer.

7. CERTIFICATE, CRL, AND OCSP PROFILES

This section is used to specify the certificate format and, if CRLs and/or OCSP are used, the CRL and/or OCSP format. This includes information on profiles, versions, and extensions used.

7.1. Certificate profile

Certificates issued under this policy conform to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

The certificate profiles and attributes described in corresponding CP.

7.1.1.Version Number(s)

All certificates are X.509 v3 certificates (populate version field with integer "2").

7.1.2.Certificate Extensions

Certificate extensions of all certificates comply with RFC 5280.

7.1.3.Algorithm Object Identifiers

Certificates issued under this CPS use the Joint-ISO-ITU Object Identifier (OID).

7.1.4.Name Forms

The subject and issuer fields of the base certificate are populated with a non-empty X.500 Distinguished Name as specified in Section 3.1.1 above. Distinguished names are composed of standard attribute types, such as those identified in RFC 5280.

7.1.5.Name Constraints

No stipulation.

7.1.6.Certificate Policy Object Identifier

CA and Subscriber Certificates issued under this CPS assert a certificate policy OID.

7.1.7.Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.8.Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL profile

7.2.1.Version Number(s)

CRLs are X.509 version 2.

7.2.2.CRL and CRL Entry Extensions

CRLs use RFC 5280 CRL and CRL entry extension.

7.3. OCSP profile

7.3.1.Version Number(s)

OCSP responses conform to version 1 of RFC 2560.

7.3.2.OCSP Extensions

OCSP response signing certificates using the following extensions:

- Key usage (not critical)
- Authority key ID (not critical)
- Extended key usage (critical)
- OCSP no check (not critical)

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Refer to Clause 6.7 of ETSI EN 319 411-1 [8] and ETSI EN 319 411-2 [9].

9. OTHER BUSINESS AND LEGAL MATTERS

8.1. Fees

8.1.1.Certificate issuance or renewal fees

The SINAM charges fees for Certificate issuance, renewals, renewals or re-key.

8.1.2.Certificate access fees

The SINAM charges no fee to for making a Certificate available in a repository.

8.1.3.Revocation or status information access fees

The SINAM reserves the right to charge a fee for providing customized CRLs or other value-added revocation and status information services.

8.1.4.Fees for other services

See Section 9.1.3.

8.1.5.Refund policy

No stipulation.

8.2. Financial responsibility

No stipulation.

8.2.1.Insurance coverage

No stipulation.

8.2.2.Other assets

No stipulation.

8.2.3.Insurance or warranty coverage for end-entities

No stipulation.

8.3. Confidentiality of business information

8.3.1.Scope of confidential information

The following items are classified as being confidential information and therefore are subject to reasonable care and attention CAs:

- Personal Information as detailed in Section 9.4.
- Audit logs from CA and RA systems.

- Activation data used to active CA Private Keys as detailed in Section 6.4.
- CAs business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP).
- Audit Reports from an independent auditor and internal auditor as detailed in Section 8.
- Vulnerability assessment results.

Unless required by law or court order, any disclosure of such information requires the subscriber's written prior consent.

8.3.2.Information not within the scope of confidential information

Information appearing in CA certificates or stored in the Repository considered as non-confidential.

8.3.3.Responsibility to protect confidential information

The SINAM is responsible for protecting an information, which considered as confidential and are under their possession, custody, and control.

8.4. Privacy of personal information

8.4.1.Privacy plan

Any information that can identify an individual, as specified in the Privacy Policy of SINAM, is safeguarded against unauthorized exposure.

8.4.2.Information treated as private

Information pertaining to Subscribers that cannot be accessed by the general public via the content of the certificate, repository, and online Certificate Revocation Lists (CRLs) is considered confidential.

8.4.3.Information not deemed private

The details found in Subscriber Certificates, such as the public key and the subscriber's name, is not considered confidential. SINAM’s Privacy Policy specifies the types of personally identifiable information that can be gathered for the purpose of issuing a certificate.

8.4.4.Responsibility to protect private information

SINAM’s staff, vendors, and service providers treat personal information with utmost confidentiality, as per the contractual obligations that are at least as protective as the provisions outlined in section 9.4.1.

8.4.5.Notice and consent to use private information

The requirements for providing notification and obtaining consent for the use of confidential information are outlined in the relevant Agreements and SINAM’s Privacy Policy.

8.4.6.Disclosure pursuant to judicial or administrative process

SINAM's Privacy Policy is followed when managing any information that is revealed.

8.4.7.Other Information Disclosure Circumstances

See Section 9.4.1.

8.5. Intellectual property rights

All participants operating under this CPS follow the intellectual property right legislation.

8.6. Representations and warranties

8.6.1.CA representations and warranties

SINAM is committed to provide its services for issuing certificates in compliance with this CPS.

8.6.2.RA representations and warranties

SINAM mandates that all RAs operating under its PKI Hierarchy guarantee that they conform to this CPS and the corresponding CP. They also have the option to incorporate supplementary statements in their CPS or RA agreement.

8.6.3.Subscriber Representations and Warranties

Subscriber is committed to provide its services for issuing certificates in compliance with this CPS.

8.6.4.Relying Party Representations and Warranties

Relying parties use certificates issued by the SCA in accordance with this CPS.

8.6.5.Representations and Warranties of Other Participants

No stipulation.

8.7. Disclaimers of warranties

The SCA assumes no liability except as stated in the relevant contracts.

8.8. Limitations of liability

The SCA is 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 certificate issued and has been expired, revoked, tampered, compromised, subject to misrepresentation, used not in-line with this CPS.

8.9. Indemnities

Relying and other parties agree to indemnify and hold the SCA free from any claims, actions or

demands that are caused by the use or publication of a certificate.

8.10. Term and termination

8.10.1. Term

This CPS and amendments to this CPS become effective upon publication in the Repository.

8.10.2. Termination

This CPS remains in force until it is amended or replaced by a new version.

8.10.3. Effect of Termination and Survival

Upon termination of this CPS, the SCA is bound by its terms for all issued certificates until periods of their validity.

8.11. Individual notices and communications with participants

The SCA communicates all notice on official website which available for all participants.

8.12. Amendments

Material changes to the CPS is published in Repository at least 30 days in advance.

8.13. Dispute resolution provisions

Any dispute resolution between the SCA and the other parties is provision in accordance with Kenyan legislation.

8.14. Governing law

The SCA provides its services under the provisions of the Kenyan legislation.

8.15. Compliance with applicable law

This CPS is subject to applicable law.

8.16. Miscellaneous provisions

No stipulation.

8.16.1. Entire Agreement

No stipulation.

8.16.2. Assignment

No stipulation.

8.16.3. Severability

No stipulation.

8.16.4. Enforcement (attorneys' fees and waiver of rights)

No stipulation.

8.16.5. Force majeure

No stipulation.

8.17. Other provisions

No stipulation.

APPENDIX A

Definitions and acronyms

Certificate	Also called *Digital Certificate*. In this document, these terms refer to public key certificates, data structure containing the certificate holder's name and public key, as well as supplementing information (e.g., a serial number, expiration dates, admissible key usages, and links to status information services) and the electronic signature of the issuing certification authority.
Certificate Modification	The act of applying for a new certificate replacing an existing certificate with different public key and other modified contents (beyond validity and serial number).
Certificate Policy (CPS)	A public document describing the rules governing the use of a public key certificate in a particular environment.
Certificate Re-key	The act of applying for a new certificate replacing an existing certificate with different public key but otherwise unchanged contents (except validity and serial number).
Certificate Renewal	The act of applying for a new certificate replacing an existing certificate with the same public key and unchanged contents (except validity and serial number).
Certificate Revocation	The process by which the effectiveness of a certificate is terminated before the envisaged end of its validity.
Certificate Revocation List (CRL)	A list containing revoked certificates and supplementing information.

Certificate Suspension	A preliminary (i.e., reversible) revocation of a certificate.
Certification Authority (CA)	Entity in a PKI which signs digital certificates.
Certification Hierarchy	A tree-like structure consisting of the issuers and subjects in a PKI as nodes, and the certification relationships as edges. An entity is subordinated to another entity if it has received a certificate from the latter one.
Certification Practice Statement (CPS)	A public document describing the practices a CA employs in issuing and managing certificates.
Certification Service Provider (CSP)	An entity that issues certificates or provides other certification services for electronic signatures. In the context of the present document a CSP is an entity who issues certificates in Kenya.
Certification Services	Certification services for electronic signatures are services supporting the issuance and management of certificates for electronic signatures. These services CAN comprise: • Certificate generation services, i.e., CAs • Registration services, i.e., RAs • Revocation management services • Certificate dissemination services • Revocation status information services • Signing device preparation services • Timestamp services Details are given in ETSI EN 319 411.
Cross certificates	A pair of certificates mutually issued between two CAs and two key pairs of the same CA to establish certification paths between these CA's or key pairs, respectively.
Electronic Signature	Electronic data logically associated with other electronic data which serves as a method for authentication.
End Entity	An entity in a PKI that does not issue certificates.
Issuer	The CA which has signed the certificate.

SINAM	Company operating Issuing Certification Authority
OCSP	Online Certificate Status Protocol, standard specified in RFC 6960 for the interactive retrieval of certificate status information.
Public Key Infrastructure (PKI)	A set of policies, processes, and technologies used to verify, enroll, and certify users based on certificates.
RA	Registration Authority
Registration	The process for receiving and processing applications for keys and certificates.
Registration Authority (RA)	Entity in a PKI which performs registration and identification of subscribers and subjects.
KENYA ROOT CA	The highest-level entity in a certification hierarchy. In the present document, the spelling "KENYA ROOT CA" refers to the Kenyan ROOT CA operated by Communications Authority of Kenya.
Subject	Entity for who a certificate is issued.
Subscriber	Entity in a PKI who applies for a certificate for itself or another entity (the subject).
Trust Anchor	The public key (or certificate) which is a priori trusted by an entity (the relying party). The certificates of KENYA ROOT CA are supposed to be used as Trust anchors.

10. References

[1] ITU-T Recommendation X.509 (2000)/ISO/IEC 9594-8 (2017): "Information technology – Open Systems Interconnection - The Directory: Public-key and attribute Certificate frameworks"

[2] "Electronic Signature and Electronic Document" Law of the Republic of Kenya, 9 March 2004

[3] ETSI TS 101 456 V1.4.3 “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing Qualified Certificates”, May 2007

[4] RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” November 2003

[5] RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels” March 1997

[6] RFC 5280 “Internet X.509 Public Key Infrastructure: Certificate and CRL Profile”, May 2008

[7] RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013

[8] ETSI EN 319 411-1 V1.4.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;

[9]ETSI EN 319 411-2 V2.5.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates;