KENET ROOT CA Certificate Policy and Certification Practice Statement

Version 2.0.1

November 3rd,2015

Table of Contents

1 INTRODUCTION

Kenya Education Network (KENET) is the National Research and Education Network (NREN) for Kenya that provides broadband Internet and advanced research computing services to the higher education community in Kenya. It also promotes the use of ICT in teaching, learning; research and administration in Higher Education Institutions using e-readiness research studies (see http://www.kenet.or.ke.).

KENET is a not-for-profit membership organization that is incorporated as a Trust with five of the eight Trustees being Vice Chancellors of Private and Public universities. It is licensed as an Alternative Network Facility Provider for educational and research institutions by CCK since 2002. The Trust operates a broadband network connecting up to 130 campuses in over 25 counties using both KENET owned and leased line infrastructure. On average, it generates up to 3 Gb/s of Internet traffic daily, most of it from the 400,000 students in the connected campuses.

KENET provides shared services to its members which include data center services such as virtual hosting, Domain Name Systems(DNS), Computer Incident Response Team (CIRT) services, Virtual storage and server co-location services. Additionally, KENET provides consultancy services to member institutions in the setup of Campus Network development including backbone and wireless networks that are eduroam enabled. It supports researchers by providing access to research computing services as part of the greater Africa authentication and authorization federated service for the Africa Science Gateway.

1.1 OVERVIEW

This document contains the combined Certificate Policy (CP) and Certificate Practice Statement (CPS) of the KENET ROOT CA stating the applicable rules and procedures for the KENET ROOT Certification Authority. KENET ROOT CA is an offline CA and operates in accordance with EUGridPMA guidelines.
This document is written in accordance with the specifications outlined by RFC3647.

1.2 DOCUMENT NAME AND IDENTIFICATION

Document title: KENET ROOT CA Certificate Policy and Certification Practice Statement
Document Date: November 3rd, 2015
Object Identifier assigned: 1.3.6.1.4.1.36493.1.1.2.0.1
IANA: 1.3.6.1.4.1
KENET: 36493
KENET ROOT CA: 1
CP/CPS Document: 1
Document Version: 2.0.1

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

KENET ROOT CA is an offline Certification Authority that issues certificates to Certificate Authorities operated by KENET Research Services

1.3.2 Registration Authorities

The KENET ROOT CA shall be operated directly by the administrators. No Registration Authority services will be provided fro this CA.

1.3.3 End Entities

KENET ROOT CA shall issue certificates only to Certificate Authorities directly operated by KENET Research Services

1.3.4 Relying Parties

Relying parties are individuals or organizations using the certificates to verify the identity of CAs signed with the KENET ROOT CA.
This CP/CPS does not limit the community of relying parties.

1.3.5 Other participants

No stipulation.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Usage

Certificates issued by the KENET ROOT CA are intended to be used in compliance with this CP/CPS

1.4.2 Prohibited Certificate Usage

The KENET ROOT CA certificates shall not be used for financial transactions or purposes that violate the Kenyan or International Law.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

This CP is administered by:
Kenya Education Network
PO BOX 30244 – 00100
Jomo Kenyatta Memorial Library, University of Nairobi.
Nairobi, Kenya
phone: +254732150500, +254703044500
www.kenet.or.ke
Email: ca@kenet.or.ke

Operation of the KENET ROOT CA is effected by:
Research Services
Kenya Education Network
PO BOX 30244 – 00100
Jomo Kenyatta Memorial Library, University of Nairobi.
Nairobi, Kenya
phone: +254732150500, +254703044500

1.5.2 Contact person

The person responsible for this CP/CPS is:
Ronald Osure
E-mail: rosure@kenet.or.ke

1.5.3 Person determining CPS suitability for the policy

The person mentioned in section 1.5.2 is responsible for this policy and works with the EUGridPMA for the review and approval of this CP/CPS.

1.5.4 CPS approval procedures

Approval of the CP and CPS is effected by the EUGridPMA and the responsible person named in section 1.5.2.
The review and approval process must assure that this CP/CPS adheres to RFC 3647.

1.5.5 Modification of the CP/CPS

Modification of this CP/CPS may be effected at any time in accordance with the procedures specified in section 1.5.4.

1.6 DEFINITIONS AND ACRONYMS

Activation Data:
Data values, other than keys, that are required to operate cryptographic modules and need to be protected (i.e a PIN, a passphrase, or a manually-held key share).

Authentication:
In the context of a PKI, authentication is the process of confirming that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization as they claimed to be

Certification Authority (CA):
The system that signs X.509 identity certificates

Certificate Policy (CP):

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

Certification Practice Statement (CPS):
A statement of the practices that a Certification Authority employs i n issuing, managing, revoking, and renewing certificates.

Identification:
The process of establishing the identity of an individual or organization showing that the same is a specific individual or organization. In the context of a PKI, identification refers to two processes:

1. Establishing that a given name of an individual or organization corresponds to a real world identity of an individual or organization.
2. Establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or
3. organization.

Certificate Revocation Lists (CRL):
A stamped list making out revoked certificates signed by CA and made freely available in public repository

Host Certificate:
A certificate used for server authentication and encryption of communications, it will represent a single machine.

Issuing Certification Authority (Issuing CA):
In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

User Certificate:
A certificate used for authentication to establish a Grid Person Identity. It will represent an individual person

Policy Qualifier:
The Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

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., an RA is delegated certain tasks on behalf of a CA).

Relying Party:
A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Repository:

A storage area, usually on-line, which contains lists of issued certificates, CRLs, policy documents, etc.

End Entity:
Or sometimes called Subscriber is a person or server to whom a digital certificate is issued.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

KENET ROOT CA shall publish its certificates, CRLs and this CP/CPS at the online repository which is accessible at the URL https://ca.kenet.or.ke

2.2 PUBLICATION OF CA INFORMATION

The KENET ROOT CA shall make the following publicly available on the on-line repository:

1. The KENET ROOT CA's PEM, DER, CER and text format of CA certificate.
2. The PEM-formatted and DER-formatted CRL.
3. A copy of this CP/CPS document and the previous versions.

2.3 TIME OR FREQUENCY OF PUBLICATION

CRL will be updated immediately after revocation is issued.
KENET ROOT CA CRL are issued at least 30 days before expiration, the CRL lifetime is 400 days.
Once approved, changes to this document will be published.
Previous versions will remain available on-line.

2.4 ACCESS CONTROLS ON REPOSITORIES

KENET ROOT CA imposes no access control restrictions to the published information including policy, certificate, issued certificates and CRL. Excluding reasonable scheduled maintenance and unforeseen failures, the online repository will be available 24/7 basis.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

The KENET ROOT CA assigns each entity a non-empty X.501 Distinguished Name (DN) which serves as a unique identifier of the entity. The DN is inserted into the subject field of the certificate(s) issued to the entity.

3.1.2 Need For Names to be Meaningful

The Subject Name must represent the subscriber in a clear manner and must be reasonably associated with the subscriber's authenticated name.

3.1.3 Anonymity Or Pseudonymity of Subscribers

KENET ROOT CA will neither issue nor sign pseudonymous or anonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Names should be in ASCII encoding and should contain only alphanumeric and the dot and underscore characters in accordance with section 3.1.1.

3.1.5 Uniqueness of Names

The subject name listed in a certificate must be unambiguous and unique for all certificates issued by the KENET ROOT CA.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

The requester must prove possession of the private key which corresponds to the public key in the certificate request. This is done through the submission of a digitally signed PKCS #10 request.

3.2.2 Authentication of Organization Identity

KENET ROOT CA shall issue certificates only to CAs operated by the KENET Research Services.

3.2.3 Authentication of Individual Identity

Subject CAs signed by the KENET ROOT CA are operated by members of the KENET Research Services

3.2.4 Non-verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

See section 3.2.2 & 3.2.3

3.2.6 Criteria for Inter-operation

No stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION OF RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine re-Key

Routine re-key shall be accomplished using the same procedures as for initial registration.

3.3.2 Identification and Authentication for re-Key after Revocation

Identification and authentication for re-key after revocation shall be accomplished using the same procedures as for initial registration.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

A request for revocation of a certificate issued by the KENET ROOT CA shall be made by a member of the KENET Research Services team.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

An application for a certificate must be submitted by a member of the KENET Research Services team.

4.1.2 Enrollment Process and Responsibilities

No stipulations.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

A certificate application shall be delivered in person by the requester to the KENET ROOT CA personnel in a secure off-line media.

4.2.2 Approval or Rejection of Certificate Applications

If the certificate request does not meet one or more of the criteria set in item 4.1.1, it will be rejected.

4.2.3 Time to Process Certificate Applications

Certificate requests are processed as soon as the request is received.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

No stipulations

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The KENET ROOT CA shall convey the issued certificate in person to the subject personnel making request.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

No stipulations.

4.4.2 Publication of the Certificate by the CA

All certificates issued by the KENET ROOT CA will be published in the online repository except when the KENET Research Services team do not see the need.

4.4.3 Notification of Certificate Issuance by the CA to other Entities

See section 4.3.2.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The subject CA private key and certificate usage shall be guided by the respective CAs CP/CPS.

4.5.2 Relying Party Public Key and Certificate Usage

The usage of the subject CA public key and certificate by relying parties shall be specified by the respective CP/CPS.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances for Certificate Renewal

The KENET ROOT CA does not support certificate renewal.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

Not applicable

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Re-key

The KENET ROOT CA shall re-key a subject CA certificate on request made by the personnel

responsible for the respective subject CA.

4.7.2 Who May Request Certification of a New Public Key

See section 4.1.1

4.7.3 Processing Certificate Re-keying Requests

Re-keying requests shall be processed following the same procedures as for a new certificate issuance.

4.7.4 Notification of new Certificate Issuance to Subscriber

See section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See section 4.4.1

4.7.6 Publication of the Re-keyed Certificate by the CA

See section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

See section 4.4.3

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

KENET ROOT CA does not support certificate modification. A subscriber requests a new certificate instead.

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

A certificate will be revoked in the following circumstances:

1. The subject CA does not apply the obligations binding by virtue of this policy.
2. The certificate is not required any more by the subject CA.
3. The private key is lost or suspected to be compromised.
4. The information in the certificate is wrong or inaccurate.
5. The system to which the certificate has been issued has been retired.

4.9.2 Who Can Request Revocation

Any entity who can prove the occurrence of any of the circumstances for revocation listed in section 4.9.1 must request revocation of the pertinent certificate.

4.9.3 Procedure for Revocation Request

The entity requesting revocation of a certificate shall submit their revocation request to the KENET ROOT CA using the contacts in section 1.5.1.
Upon receipt of a revocation request, the KENET ROOT CA shall:

1. Verify the circumstances for revocation
2. Verify the identity of the revocation requester in accordance with section 4.9.2

If all the conditions are met, KENET ROOT CA shall then revoke the certificate.

4.9.4 Revocation Request Grace Period

Any party that becomes aware of circumstances for revocation shall request a revocation as soon as possible but not later than within one business day.

4.9.5 Time within which CA must Process the Revocation Request

All revocations will be acted on immediately.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties must download the CRL from the online repository at least once a day and implement its restrictions while validating certificates.

4.9.7 CRL Issuance Frequency

The KENET ROOT CA shall issue CRL at least once every 400 days or immediately after a certificate revocation.

4.9.8 Maximum Latency for CRLs

New CRLs will be published immediately after issuance.

4.9.9 On-line Revocation/Status Checking Availability

No stipulations.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

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

KENET ROOT CA does not suspend certificates.

4.9.14 Who can Request Suspension

KENET ROOT CA does not suspend certificates.

4.9.15 Procedure for Suspension Request

KENET ROOT CA does not suspend certificates.

4.9.16 Limits on Suspension Period

KENET ROOT CA does not suspend certificates.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

The KENET ROOT CA shall publish its full and complete CRL at the online repository.

4.10.2 Service Availability

The online repository is maintained on best effort basis with intended availability of 24x7.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

The subscription ends upon the expiry of the certificate if it is not re-keyed before that date, or if the subject CA personnel requests the revocation of the certificate.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

The KENET ROOT CA shall not provide key escrow service.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

The machine hosting the KENET ROOT CA shall be located in a closed, secure and safe location.

5.1.2 Physical Access

Access to the safe hosting the KENET ROOT CA is restricted to authorized personnel only.

5.1.3 Power and Air Conditioning

No stipulations

5.1.4 Water Exposures

The KENET office where the safe is hosted is equipped with adequate protection against exposure to water.

5.1.5 Fire Prevention and Protection

KENET office has a fire alarm system with adequate number of fire extinguishers.

5.1.6 Media Storage

All removable media with KENET ROOT CA software shall be kept in a safe and locked cabinet.

5.1.7 Waste Disposal

Waste carrying potential confidential information is physically destroyed before being trashed.

5.1.8 Off-site backup

No off-site backup is implemented currently.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

All persons with access to the systems hosting the KENET ROOT CA will be employees of KENET who are members of the KENET Research Services team.

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for Each Role

No stipulation.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

KENET's Research Services team members meet all requisite requirements with regard to Confidentiality, Integrity and Availability. All the members have general training and qualifications in the field of Information Sciences and depending on the role they fulfill as employees, they also have in-depth knowledge in the following fields:

1. IT security, cryptography, electronic signatures and PKI
2. International standards, technical standards
3. National and International law
4. Unix/Linux operating systems, TCP/IP networks and relational databases

5.3.2 Background Check Procedures

No stipulation.

5.3.3 Training Requirements

Internal training will be given to KENET ROOT CA personnel on PKI concepts, computer security and the use and operation of the KENET ROOT CA software.

5.3.4 Retraining Frequency and Requirements

Retraining shall be mandatory when new software or features, as well as new organizational procedures are introduced.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

If an unauthorized action is observed, the CA manager may revoke the privileges concerned.

5.3.7 Independent Contractor Requirements

Not applicable.

5.3.8 Documentation Supplied to Personnel

The concerned personnel are given a copy of CP/CPS, and any documentation describing his/her given tasks.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

The following events will be recorded by the KENET ROOT CA:

- System boots and shutdowns of the offline machine
- Registration fo subscriber
- Certificate application, issuance and revocation
- Activation and deactivation of the CAs signing key

5.4.2 Frequency of Processing Log

Audit logs will be analyzed once per month or immediately after discovering a security incident.

5.4.3 Retention Period for Audit Log

Audit logs will be retained for at least 3 years.

5.4.4 Protection of Audit Log

Only authorized KENET ROOT CA personnel are allowed to view and process audit logs.

5.4.5 Audit Log Backup Procedures

Audit logs are copied to a safely stored offline medium which are then stored in a safe.

5.4.6 Audit Collection System (internal vs. external)

The audit collection system adopted by KENET ROOT CA is internal.

5.4.7 Notification to Event-causing Subject

The subjects causing an audit event are generally not notified.

5.4.8 Vulnerability assessments

Audit logs shall be monitored regularly to find potential security incidents and non-standard events

5.5 RECORDS ARCHIVAL

5.5.1 Types of records archived

KENET ROOT CA will archive the following data and files:

1. all certificate application data including certification and revocation
2. all certificates and CRLs or certificate status records generated
3. the login/logout/reboot of the issuing machine.

5.5.2 Retention Period for Archive

Logs will be kept for a minimum period of three years.

5.5.3 Protection of Archive

Appropriate measures are in place to protect data from manipulation and deletion. The archive shall only be accessible by KENET ROOT CA PKI team.

5.5.4 Archive Backup Procedures

All records will be backed up on removable media which will be kept in a safe.

5.5.5 Requirements for Time-stamping of Records

No stipulation.

5.5.6 Archive Collection System (internal or external)

The adopted archive collection system is internal.

5.5.7 Procedures to Obtain and Verify Archive Information

All certificate data published by the KENET ROOT CA are publicly available. Data used for the registration and identification of subscribers are for internal use only. The integrity of KENET ROOT CA archives is verified as follows:

1. time the archive is prepared
2. time of a programmed security audit
3. time when a full security audit is required

5.6 KEY CHANGEOVER

KENET ROOT CA's private signing key is changed periodically. The overlap between the old key and the new one is for at least one year. From that time on, any new certificates are signed by the newly generated signing key. During that period any old and valid certificates must be valid to verify old signatures and to sign CRL.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

In the event of an incident which compromises the integrity of the KENET ROOT CA, the CA personnel shall initiate an incident analysis immediately. Further steps to be undertaken will depend on the outcome of the analysis.

5.7.2 Computing Resources, Software, and/or Data are corrupted

The CA will take best effort precautions to enable recovery.
In order to be able to resume operation as fast as possible after the compute basis of the CA is corrupted, the following steps shall be performed:

1. All CA software shall be backed-up on removable media after a new release of any of its components is installed.
2. All data files of the CA signing server shall be backed-up on a removable medium after each change, before the session is closed.

If any part of the running system is corrupted, a functioning hardware shall be loaded with the latest state of the software and data backed-up on a read-only medium and estimated to be uncorrupted. If not all encrypted copies of the KENET ROOT CA private key are destroyed or lost, and are not compromised, the operation shall be re-established as soon as possible without need to revoke all issued certificates.

5.7.3 Entity Private Key Compromise Procedures

In the event of private key compromise, KENET ROOT CA shall immediately revoke the corresponding certificate and stop accepting certificate applications. Subscribers will also be informed of this incident. Circumstances that led to the compromise will then be fixed and eliminated. A new key and certificate for the CA will then be re-created and operations restarted with a new certificate.

5.7.4 Business Continuity Capabilities after a Disaster

After a disaster, KENET ROOT CA shall recover its systems from backup and restart operations as soon as is possiblle. Outage should not last more than 5 working days

5.8 CA or RA TERMINATION

Upon permanent termination, KENET ROOT CA will:

1. Inform the EUGridPMA
2. Announce termination on KENET's website.
3. Terminate the issuance and distribution of certificates and CRLs..
4. Archive all relevant information in accordance with section 5.5
5. Revoke all certificates.
6. Notify relevant security contacts.
7. Destroy all copies of private keys.
8. Notify as widely as possible the end of the service.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

KENET ROOT CA shall generate and store its private keys in an offline system which is

stored in a safe in accordance with secion 5.1.

6.1.2 Private Key Delivery to Subscriber

KENET ROOT CA does not generate private keys and therefore does not deliver private keys since they are directly generated on a system that the subscriber accesses.

6.1.3 Public Key Delivery to Certificate Issuer

The subscriber's public key is delivered to the CA in the form of a PKCS#10 request.

6.1.4 CA Public Key Delivery to Relying Parties

KENET ROOT CA public keys can be downloaded from the online repository

6.1.5 Key sizes

The signing key of the KENET ROOT CA shall be at least 2048 bits long.

6.1.6 Public Key Parameters Generation and Quality Checking

The KENET ROOT CA will refuse to certify public keys not matching its quality requirements.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Keys may be used for certificate sign and CRL sign.

6.2 PRIVATE KEY PROTECTIONS AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

No stipulations.

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

No stipulation.

6.2.3 Private Key Escrow

Subscriber's private key escrow is not supported.

6.2.4 Private Key Backup

The KENET ROOT CA private key is backed up in removable media as described in section 5.1.6.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Not applicable.

6.2.7 Private Key Storage on Cryptographic Module

Not applicable.

6.2.8 Method of Activating Private Key

The private key of the KENET ROOT CA is activated by a pass phrase.

6.2.9 Method of Deactivating Private Key

No stipulation.

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 KENET ROOT CA archives all issued certificates on the offline system as well as on removable storage media kept in a secure place.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

KENET ROOT CA certificates have the following periods of validity:

1. The KENET ROOT CA certificate will be valid for twenty years
2. and the maximum validity period for the subject CA certificates is ten years.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

KENET ROOT CA does not generate activation data for subject CAs. Its upon the subscriber to generate a secure pass phrase at least 20 characters long in order to be used as activation

data for his/her private key.
The pass phrase used to activate the KENET ROOT CA private key is generated on the offline machine and will have a minimum length of 32 characters.

6.4.2 Activation Data Protection

The subscriber is responsible to protect the activation data for the subject CA private key. The KENET ROOT CA uses a pass phrase to activate its private key which is securely stored in the offline machine and also backed up in removable media as indicated in section 5.1.6. A copy of the pass phrase in written form is sealed in an envelope and kept in the KENET ROOT CA safe. Old activation data is destroyed according to current best practices.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

1. The operating systems of CA computers are maintained at a high level of security by applying all relevant patches.
2. Any unauthorized software change is monitored and dealt with by the CA administrator.
3. System configuration is reduced to the bare minimum.
4. The offline system is kept powered off and not connected to any network.
5. The offline machine must be updated or patched.
6. Any unusable service on the machine will be ceased.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

Modification of CA systems shall be developed and tested on a separated development system.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The issuing system is loaded only on a dedicated offline computer.

6.8 TIME-STAMPING

No stipulation.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

All certificates referred to this Policy will be issued in the X.509 version 3 format and will include a reference to the O.I.D of this Policy within the appropriate field.

7.1.2 Certificate Extensions

The CA certificate of the KENET ROOT CA shall use the following extensions:

a) Basic Constraints (critical)
   CA: true

b) Key Usage
Digital Signature, Certificate Sign, CRL Sign
c) Subject Key Identifier
key identifier of the CA
d) Authority Key Identifier
key identifier of the CA

Subject CA certificates should typically use the following extensions:

a) Basic Constraints (critical)
CA: true
b) Key Usage
Certificate Sign, CRL Sign
c) Subject Key Identifier
key identifier of the subscriber
d) Authority Key identifier
key identifier of the KENET ROOT CA signing key
e) Authority Information Access
CA Issuers: URI: locator of the KENET ROOT CA certificate
f) CRL Distribution Point
URI: locator of the current KENET ROOT CA CRL

7.1.3 Algorithm Object Identifiers

1. Hash Function: id-sha256 1.3.14.3.2.26
2. RSA Encryption: rsaEncryption 1.2.840.113549.1.1.1
3. Signature Algorithm: sha256WithRSAEncryption 1.2.840.113549.1.1.5

7.1.4 Name Forms

The subject name of the KENET ROOT CA is:

DC=ke, DC=kenet, O=Kenya Education Network Trust, OU=Research Services, CN=KENET ROOT CA

Subject names of the intermediate CAs will take the form:

dc=ke, dc=kenet, O=Kenya Education Network Trust, OU=Research Services, CN=*commonName*

Where the commonName must be the subject CAs name

7.1.5 Name Constraints

As described in sections 3.1.1 and 3.1.2 and 7.1.4.

7.1.6 Certificate Policy Object Identifier

See section 1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL PROFILE

7.2.1 Version Number(s)

All CRLs will be X.509 version 2 format. Compliant with RFC5280.

7.2.2 CRL and CRL Entry Extensions

7.3 OCSP PROFILE

7.3.1 Version Number(s)

7.3.2 OCSP Extensions

8 COMPLIANCE, AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The KENET ROOT CA is obliged to ensure that all its procedures and processes are carried out in compliance with the provisions of the CP/CPS. The KENET ROOT CA shall make at least once a year a self-assessment to check the compliance of the operation with the CP/CPS document in effect.

The CA shall at least once a year assess the compliance of the procedure of each RA with the CP/CPS document in effect. The CA shall at least once a year assess the staff.KENET ROOT CA accepts to be audited by external CA or any relying parties in order to verify its compliance with the rules and procedures prescribed herein. Any costs associated with

such audit must be covered by the requesting party.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

No stipulation.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

No stipulation.

8.4 TOPICS COVERED BY ASSESSMENT

The audit will verify that the services provided by the CA comply with the latest approved version of the CP/CPS.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

In the event of a deficiency, KENET ROOT CA will announce the steps that will be taken to remedy the deficiency including the time-lines. If a discovered deficiency has direct consequences on the reliability of the certification process, the certificates likely to have been affected by the deficiency will be revoked with immediate effect.

8.6 COMMUNICATION OF RESULTS

The results will be made public on the KENET website.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No fees shall be charged.

9.1.2 Certificate Access Fees

See section 9.1.1.

9.1.3 Revocation or Status Information Access Fees

See section 9.1.1.

9.1.4 Fees for Other Services

See section 9.1.1.

9.1.5 Refund Policy

See section 9.1.1.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

No Financial responsibility is accepted for certificates issued under this policy.

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

9.3.1 Scope of Confidential Information

The KENET ROOT CA shall keep private keys, cryptographic data, personal data and internal CA documentation information as confidential.

9.3.2 Information not within the Scope of Confidential Information

Information included in certificates and CRLs shall not be considered confidential.

9.3.3 Responsibility to Protect Confidential Information

The KENET ROOT CA shall not disclose confidential information to any third party except law enforcement agencies.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

KENET ROOT CA will be guided by the laws of Kenya when processing personal data.

9.4.2 Information Treated as Private

Any information not publicly accessible is treated as private information.

9.4.3 Information not Deemed Private

The following information which is collected by the KENET ROOT CA is deemed as not private:

1. subscriber's email address
2. subscriber's name
3. subscriber's organization
4. subscriber's certificate

9.4.4 Responsibility to Protect Private Information

The responsibility to protect private information rests with the KENET ROOT CA.

9.4.5 Notice and Consent to Use Private Information

No stipulation.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The KENET ROOT CA may disclose any confidential information to law enforcement agencies.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

The KENET ROOT CA does not claim any Intellectual Property Rights on certificates which it has issued; parts of this document have been copied from the CP CPS documents of other CAs as posted in the EUGridPMA website mainly:

1. JUNET CA CP CPS
2. TSU CA CP CPS
3. CESNET ROOT CA CP/CPS

Anybody may freely copy from any version of the KENET CP CPS provided they include an acknowledgment of the source.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

9.6.2 RA Representations and Warranties

9.6.3 Subscriber Representations and Warranties

9.6.4 Relying Party Representations and Warranties

9.6.5 Representations and Warranties of Other Participants

9.7 DISCLAIMERS OF WARRANTIES

KENET ROOT CA denies any financial or any other kind of responsibility for damages or impairments resulting from its operations.

9.8 LIMITATIONS OF LIABILITY

KENET ROOT CA declines any liability for damages incurred by a relying party accepting one of its certificates, or by a subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party.

It also declines any liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA acting in conformance with this CP/CPS.

9.9 INDEMNITIES

9.10 TERM AND TERMINATION

9.10.1 Term

9.10.2 Termination

9.10.3 Effect of Termination and Survival

Its text shall remain available for at least 5 years after the last certificate issued under this CP/CPS expires or is revoked.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

9.12.2 Notification Mechanism and Period

9.12.3 Circumstances Under which OID Must be Changed

9.13 DISPUTE RESOLUTION PROVISIONS

Disputes arising out of the CP/CPS shall be resolved by the KENET Research Services team.

9.14 GOVERNING LAW

The interpretation, construction, and validity of this policy shall be governed by the Laws of Kenya.

9.15 COMPLIANCE WITH APPLICABLE LAW

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

9.16.2 Assignment

No provisions.

9.16.3 Severability

9.16.4 Enforcement (attorneys' fees and waiver of rights)

9.16.5 Force Majeure

9.17 OTHER PROVISIONS