KENET CA
Certificate Policy and Certification Practice Statement

Version 1.0.1

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 CA stating the applicable rules and procedures for the KENET Certification Authority. KENET CA is an online CA and operates in accordance with EUGridPMA guidelines for online CAs.
This document is written in accordance with the specifications outlined by RFC3647.

1.2 DOCUMENT NAME AND IDENTIFICATION

Document title: KENET CA Certificate Policy and Certification Practice Statement
Document Date: November 3rd, 2015
Object Identifier assigned: 1.3.6.1.4.1.36493.1.1.1.0.1
IANA: 1.3.6.1.4.1
KENET: 36493
KENET CA: 1
CP/CPS Document: 1
Document Version: 1.0.1

1.3 PKI PARTICIPANTS

The KENET CA provides PKI services to Kenyan researchers.

1.3.1 Certification Authorities

KENET CA is an on-line CA subordinate to the KENET ROOT CA. The requirements described in this CP/CPS are binding for KENET CA

1.3.2 Registration Authorities

The KENET CA delegates identification and authorization of certificate subjects to trusted individuals (Registration Authorities). These intermediaries are formally appointed by the Director of the Structure in which they operate. Their identities are published in an on-line repository.
RA's must perform their tasks in accordance with this CP/CPS.

1.3.3 End Entities

KENET CA issues certificates for natural persons, legal entities and digital processing entities involved in GRID related activities and any other requirements of the Kenyan based research and academic communities.

1.3.4 Relying Parties

Relying parties are individuals or organizations using the certificates to verify the identity of end entities and to secure communication with these end entities.
Relying parties may or may not be subscribers of the KENET CA.

1.3.5 Other participants

No stipulation.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Usage

Certificates issued by the KENET CA are intended to be used primarily by users who are researchers and hosts within the KENET community

1.4.2 Prohibited Certificate Usage

The KENET 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 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

The online repositories will be published at the URL https://ca.kenet.or.ke

2.2 PUBLICATION OF CA INFORMATION

The KENET CA operates an on-line repository that contains:

1. The KENET CA's PEM, DER, CER and text format of CA certificate.
2. Issued certificates.
3. The PEM-formatted and DER-formatted CRL.
4. A copy of this CP/CPS document.
5. An official contact e-mail address.
6. A physical contact address.
7. Other relevant information.

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificates will be published as soon as issued.
CRL will be updated immediately after revocation is issued.
KENET CA CRL are issued at least 7 days before expiration, the CRL lifetime is 30 days.
Once approved, changes to this document will be published.
Previous versions will remain available on-line.

2.4 ACCESS CONTROLS ON REPOSITORIES

KENET 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 subject name of the applicants shall be compatible with X.509 standard; which forms are:

1. User: The subject name must include the person's full name in the CN field; in case of personal certificate.

2. Host: The subject name must include FQDN as registered to DNS in the CN field; in case of host/server certificate

All end entity DNs in certificates issued under this CPS SHALL start with invariable part identifying the CA (DC=ke,DC=kenet)

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 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 CA. In the case of user certificates, additional numbers or letters may be appended to the real name to ensure the uniqueness of the name within the domain of certificates issued by the KENET 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

A request of a personal certificate is initiated by a key generation tag or control which the user's web browser reads on the CA's user registration web page. Key and certificate signing request generation and submission are tied together in a single SSL session, and there is a reasonable presumption of possession of private key in requests originating in web browser functions. Keys generated by other means (such as OpenSSL), have separate key generation, certificate signing request generation and submission stages. No test for proof of possession of private key is made in these cases. Re-keying employs a proof of possession of private key.

3.2.2 Authentication of Organization Identity

The RA shall verify that the requesting party's organization or a unit of an organization is entitled (see 1.3.3) to get a certificate from the KENET CA and that it consents to the request. The first time an organization/unit wants to get a certificate for a user or a server, it has to announce this officially to the RA or the KENET CA. The RA has to ascertain that the organization or organizational unit exists and is entitled to request a KENET CA certificate. It must also get competent information on who is entitled to sign on behalf of the institution.

3.2.3 Authentication of Individual Identity

a) User
The subscriber is authenticated by meeting him/her personally by the RA using a valid photo ID document, and the RA will keep the subscriber information like his/her E-mail, phone and address number.
b) Host
The RA confirms that the requester is from the institution that the FQDN of the host is registered under. The RA also confirms the host name is on the online internet DNS. KENET is already the registrant of domains for most of its member institutions.

In both a) and b) above, the credentials required to generate the certificate through the online website are handed over to the requester/subscriber during the face to face meeting.

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

Re-key before the certificate expires can be done by sending a re-key request email signed with the current user certificate. Re-key after expiration follows the same authentication procedures as for a new certificate.

3.3.2 Identification and Authentication for re-Key after Revocation

A revoked certificate cannot be renewed, user has to request a new certificate with the rules defined in section 3.2.3

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Certificate revocation requests should be authenticated in one of the following ways:

1. By signing a revocation request e-mail via a valid personal KENET CA issued certificate
2. By personal authentication as described in 3.2.3.

In case of emergency the revocation can be initiated via oral communication with the RA or the KENET CA. The RA or the KENET CA has to use their best effort to authenticate the request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

The KENET CA issues certificates to its member institutions and persons affiliated to the institutions for:

1. Natural persons.
2. Hosts administered by the requesting organization.

4.1.2 Enrollment Process and Responsibilities

Personal Certificate
The requesting party generates the key pair with a size of at least 1024 bit on their system through the form provided at the KENET CA web site. After the form has been completed the encrypted private key will be stored on the system where the browser runs, in a file only accessible to the requester (if the operating system allows such a restriction), and the CSR will be stored in the KENET CA system. The subscriber has to login to the web site to access the form using credentials given by the RA (see section 3.2.3).

Host Certificate
The requesting party generates a CSR on their system. The subscriber then uses a form provided on the KENET CA web site to import the certificate request, generate and download the certificate.

Subscribers must:

1. Read and adhere to the procedures published in this document.
2. Use the certificate for the permitted purposes only.
3. Authorize the processing and conservation of personal data (as required under the data protection regulations).
4. Take every precaution to prevent any loss, disclosure or unauthorized access to or use of the private key associated with the certificate, including
    - (Personal certificates) selecting a strong pass phrase;
    - (Personal certificates) protecting the pass phrase from others and should not be sent in clear text over the network;
5. Notifying immediately the KENET CA and any relying parties if the private key is lost or compromised.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

For the users the RA operator must authenticate the individual's identity using section 3.2.3. In the case of a server request it must also check that the user is a representative from a member institution
(using section 3.2.3).

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 and the requester will be informed accordingly via e-mail.

4.2.3 Time to Process Certificate Applications

Any certificate request will not take more than 5 working days after successful verification from the RA.

4.3 CERTIFICATE ISSUANCE

After receipt and successful verification of a certificate application, the KENET CA will create a new end entity instance and inform the subscriber of the credentials required to generate the certificate online through the KENET CA website (see section 3.2.3).

4.3.1 CA Actions during Certificate Issuance

Certificate issuance is done through secured web access to the online signing server without any actions from the CA. The certificate once issued is then automatically published to the online repository.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Information on the issuance of the certificate is passed to the subscriber during the face to face meeting with the RA. The RA will be informed of issuance through email

4.4 CERTIFICATE ACCEPTANCE

The subscriber is obliged to verify the correctness of his own certificate once he has received it.

4.4.1 Conduct Constituting Certificate Acceptance

The requesting party shall notify the KENET CA of the rejection of a certificate, explaining the KENET CA and the RA the reasons for the rejection. Certificates whose rejection have not been received by the KENET CA within a month shall be considered accepted.

4.4.2 Publication of the Certificate by the CA

All certificates issued by the KENET CA will be published in the online repository.

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

A subscriber may use the certificate issued as they wish but in accordance with section 1.4.1; It will not be used for purposes identified in section 1.4.2.

4.5.2 Relying Party Public Key and Certificate Usage

A relying party must before relying on a certificate:

- use the certificate in compliance with this CP/CPS
- verify the validity of the certificate before using it

- use the certificate in accordance with the specific purpose for which it has been issued

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances for Certificate Renewal

KENET CA does not undertake renewing subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.2 Who May Request Renewal

KENET CA does not undertake renewing subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.3 Processing Certificate Renewal Requests

KENET CA does not undertake renewing subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.4 Notification of New Certificate Issuance to Subscriber

KENET CA does not undertake renewing subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

KENET CA does not undertake renewing subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.6 Publication of the Renewal Certificate by the CA

KENET CA does not undertake renewing subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

KENET CA does not undertake renewing subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Re-key

Subscribers must generate a new key pair for each certificate they request to be signed by the KENET 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

Expiration warnings will be issued to subscribers when re key time arrives. Re-key before expiration can be accomplished by sending a re-key request signed with the current user certificate. Re-key after expiration follows the same authentication procedure as for a new certificate. At least once every 3 years the subscriber must go through the same authentication procedure as the one described for a new certificate.
In case the request for a new certificate is due to revocation or compromise of certificate the subscriber must follow the same procedure as the one described in for a new one.

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 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 subscriber does not apply the obligations binding by virtue of this policy.
2. The certificate is not required any more by the subscriber.
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

The CA, RA, and subscriber of the certificate or any person presenting proof that any of the circumstances in section 4.9.1 is fulfilled.

4.9.3 Procedure for Revocation Request

The entity requesting revocation of a certificate is authenticated by verifying the digital signature in an e-mail request or else authentication will be performed with the same procedure as described in section 3.2.3.

4.9.4 Revocation Request Grace Period

KENET CA will process the revocation requests as soon as practicable and without unnecessary delay.

4.9.5 Time within which CA must Process the Revocation Request

All revocations will be processed within one day.

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

1. KENET CA CRLs will be published in the online repository as soon as issued and at least once every 23 days;
2. The KENET CA minimum CRL lifetime is 30 days;
3. KENET CA CRLs are issued at least 7 days before expiration.

4.9.8 Maximum Latency for CRLs

No stipulation

4.9.9 On-line Revocation/Status Checking Availability

The KENET CA operates an online repository containing all the CRLs which have been issued. After revocation, the CRL or certificate status database in the repository shall be updated.

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 CA does not suspend certificates.

4.9.14 Who can Request Suspension

KENET CA does not suspend certificates.

4.9.15 Procedure for Suspension Request

KENET CA does not suspend certificates.

4.9.16 Limits on Suspension Period

KENET CA does not suspend certificates.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

KENET CA online repository contains list of root, valid certificates and list of revoked certificates where all of lists are continuously updated.

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 subscriber requests the revocation of the certificate.

4.12 KEY ESCROW AND RECOVERY

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

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

The KENET CA is located at KENET's secretariat in the University of Nairobi. The data center

where the KENET CA is hosted is located in the Hyslop Building within the University of Nairobi Main Campus.

5.1.2 Physical Access

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

5.1.3 Power and Air Conditioning

Installation of the power supply is in compliance with applicable standards and adequate air conditioning for the data center hosing the KENET CA has been provided.

5.1.4 Water Exposures

The KENET data center is equipped with adequate protection against exposure to water.

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

All removable media 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 CA will be employees of KENET who are members of its PKI 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 PKI 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 CA personnel and RA operators.

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

No stipulation.

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:

On the CA Server

- System boots and shutdowns.
- User logins and logouts.
- Creation and signing of certificates.
- CRL issues.
- Activation and deactivation of the signing key.
- Synchronization of certificates with the OCSP Server

On the Online Server

- System boots and shutdowns.
- OCSP responses
- Access to the online repository

5.4.2 Frequency of Processing Log

Audit logs will be analyzed once per month.

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 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 CA is internal.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 RECORDS ARCHIVAL

5.5.1 Types of records archived

KENET 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 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 CA are publicly available. Data used for the registration and identification of subscribers are for internal use only. The integrity of KENET 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 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

If the keys of an end entity are lost or compromised due to corruption of their computing basis, the appropriate RA must be informed immediately in order to start the certificate revocation process.
If an RA Operator' s private key is compromised or suspected to be compromised, the RA Operator or Manager must inform the CA and request the revocation of the RA Operator' s certificate.
If the KENET CA private key is compromised, destroyed or lost, the KENET CA will:

1. Assume immediate annulment action for such private key.
2. Notify subscribers, RAs, and Relying Parties.
3. Terminate the issuance and distribution of certificates and CRLs.
4. Generate new CA certificate with a new key pair and publish it on the web site.

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 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, the user must promptly inform the RA in order to start certificate revocation accordingly. All relying parties known to accept the key should be informed by the owner of the key.
After that the user is entitled to claim a new certificate instead. And in case the private key of server is compromised, the administrator of the certificate must ask for revocation. After that the administrator is entitled to claim a new certificate instead.

5.7.4 Business Continuity Capabilities after a Disaster

No stipulation.

5.8 CA or RA TERMINATION

Upon permanent termination, KENET CA will:

1. Inform the EUGridPMA
2. Announce termination on KENET's website.
3. Terminate the issuance and distribution of certificates and CRLs.
4. Notify subscribers and RA.
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 CA shall generate and store its private keys in a hardware security module which is conducted by KENET's PKI team in a key generation ceremony.
Subscribers will be responsible for generating their own private keys.

6.1.2 Private Key Delivery to Subscriber

KENET 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 a way that ensures that it has not been altered using a secure public website.

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key sizes

1. The minimum key length for an End Entity certificate is 1024 bits
2. The minimum length for the KENET CA private key is 2048 bits.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

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

Keys may be used for authentication, non-repudiation, data encryption, message integrity and session establishment. Certificates and CRLs are signed by the CA private key.

6.2 PRIVATE KEY PROTECTIONS AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The HSM used to store store the KENET CA private key is operated according to the FIPS 140-2 Level 3 standard.

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 CA private key is backed up in the offline generation machine as well as removable media as described in section 5.1.6. The private key or copies of it can not leave

the HSM.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The KENET CA private key is first generated on an offline machine and then transferred into the HSM in a key generation ceremony that is documented.

6.2.7 Private Key Storage on Cryptographic Module

The KENET CA private key can not leave the HSM and therefore the key is always protected by the HSM.

6.2.8 Method of Activating Private Key

The private key of the KENET CA is activated by providing activation data for the HSM in use.

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

Refer to section 6.2.1

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The KENET CA archives all issued certificates on the servers as well as on removable storage media kept in a secure
place.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

KENET CA certificates have the following periods of validity:

1. The KENET CA certificate will be valid for ten years
2. and the maximum validity period for the subscribers' certificates is 13 months.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

KENET CA does not generate activation data for subscribers. Its upon the subscriber to generate a secure pass phrase at least 12 characters long in order to be used as activation data for his/her private key.
The pass phrase used to activate the KENET CA private key is generated on the offline machine and will have a minimum length of 20 characters.

6.4.2 Activation Data Protection

The subscriber is responsible to protect the activation data for his/her private key.
The KENET 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 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 key generation laptop 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

1. The KENET CA signing machine is connected but only traffic for certificate generation is allowed to this server
2. The KENET CA servers are all protected by host based firewalls
3. Critical security events will be immediately tracked and processed in collaboration with the KENET CERT team.

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

KENET CA uses and support the following X.509 v3 certificate extension:
a) Users certificates

1. Basic constraints (Critical),CA:FALSE
2. Key Usage: (Critical), Digital Signature, Key Encipherment, Data Encipherment
3. Extended Key Usage: clientAuth, email Protection
4. Subject key identifier: hash
5. Subject alternative name: subscriber’s E-mail address
6. Authority Key Identifier: keyid, DirName, serial
7. CRL distribution points:URI
8. Certificate policies: OID

b) Host certificates

1. Basic constraints (Critical),CA:FALSE
2. Key Usage: (Critical), Digital Signature, Key Encipherment, Data Encipherment
3. Extended Key Usage: serverAuth, clientAuth.
4. Subject key identifier: hasherver's DNS FQDN
5. Subject alternative name: Subjects FQDN
6. Authority Key Identifier: keyid, DirName, serial
7. CRL distribution points: URI
8. Certificate policies: OID

c) KENET CA Certificate

1. Basic Constraints: (Critical), CA:TRUE, pathlen:0
2. Key Usage: (Critical) Digital Signature, Certificate Sign, CRL Sign
3. Authority Key Identifier: keyid
4. Subject Key Identifier: hash
5. CRL Distribution Points: URI

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

Issuer (KENET CA): DC=ke, DC=kenet, O=Kenya Education Network Trust, OU=Research Services, CN=KENET CA

Subject (users): dc=ke, dc=kenet, O=INSTITUTE, OU=INSTITUTE DEPT/UNIT, CN=*commonName*
Where the commonName must be the full name of the subject. In case the name is not unique, additional attributes may be appended to the full name.

Subject (Hosts): dc=ke, dc=kenet, O=INSTITUTE, OU=INSTITUTE DEPT/UNIT, CN=*commonName*
Where the commonName must be the DNS FQDN of the host.

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

No stipulation.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

The OCSP service operated by the KENET CA shall use basic OCSP Response version 1 as defined in RFC 2560 [RFC2560].

7.3.2 OCSP Extensions

No stipulation.

8 COMPLIANCE, AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The KENET 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 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 CA and RA staff.
KENET 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 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 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 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 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 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 CA and all its accredited RAs.

9.4.5 Notice and Consent to Use Private Information

No stipulation.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The KENET 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 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

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

9.8 LIMITATIONS OF LIABILITY

KENET 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 or the appropriate

RA 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

No stipulation.

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