THE KENYA COMMUNICATIONS ACT, 1998
(No. 2 of 1998)

LEGAL NOTICE NO. ……

THE KENYA COMMUNICATIONS (ELECTRONIC TRANSACTIONS) REGULATIONS, 2009

ARRANGEMENT OF REGULATIONS

Regulation

THE KENYA COMMUNICATIONS ACT, 1998

(No. 2 of 1998)

IN EXERCISE of the powers conferred by sections 83R of the Kenya Communications (Amendment) Act 2009, the Minister for Information and Communications in consultation with the Communications Commission of Kenya makes the following Regulations –

THE KENYA COMMUNICATIONS (ELECTRONIC TRANSACTIONS) REGULATIONS, 2009

PART I – PRELIMINARY PROVISIONS

Citation

1. These Regulations may be cited as the Kenya Communications (Electronic Transactions) Regulations, 2009.

Interpretation.

2. In these Regulations, unless the context otherwise requires -

"Act" means the Kenya Communications Act, No. 2 of 1998;

"Amendment Act" means Kenya Communications (Amendment) Act, Act No. 1 of 2009;

"ccTLD" means Country Code Top-Level Domain

"ccTLD administrator" means the entity managing the .KE ccTLD;

"cc TLD Repository" means a system in which an aggregation of data on .ke ccTLD domain names is stored and retrieved;

"certification personnel" means any person who has –

i. direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or these Regulations in respect of a Certification Service Provider;
ii. or duties directly involving the issuance, renewal, suspension, revocation of certificates (including the identification of any person requesting a certificate from a licensed Certification Service Provider), creation of private keys or administration of a Certification Service

Provider's computing facilities.

" certification practice statement" means a statement of the practices that certification service providers employ in approving or rejecting certificate applications and issuing, managing and revoking certificaets.

".ke ccTLD" means Dot KE Country Code Top-Level Domain;

".ke ccTLD namespace" means a collection of uniquely-assigned identifiers within the Kenya country code Top Level Domain;

"license" refers to a licence issued under the provisions of the Amendment Act and these Regulations;

"licensee" means a person or an entity licensed by the Commission to operate communications systems and/or provide communications services;

"registrant" means a domain name holder.

"registrar" means an entity that is authorized under the Act and these regulations to administer the process of registration and modification of domain names;

"relying party" means an individual or organisation that acts in reliance on a certificate and/or advanced electronic signature.

"second level ccTLD sub-domain" means the domain namespace after the .ke ccTLD;

"Subscriber" means a certificate holder.

"subscriber identity verification method" means the method used to verify and authenticate the identity of a subscriber;

"third level ccTLD subdomain" means the domain namespace after the second level domain;

PART II- ELECTRONIC CERTIFICATION SERVICES

Functions of a Certification

3. A Certification Service Provider, licensed in accordance with the Kenya Communications (Licensing and Quality of

Service Provider

Service) Regulations, 2009 shall operate and provide advanced electronic signature certificate management services in the Republic of Kenya subject to the terms and conditions set out in their licence and these Regulations.

Operational requirements

4. 1) An applicant for a license shall comply with the following operational criteria:

(a) have a certification practice statement approved by the Commission; and

(b) undergo and pass an initial audit before grant of the licence.

Financial requirements

5. An applicant for a license shall comply shall:

a) be a company registered in Kenya;

b) take out adequate insurance, in accordance with guidelines published by the Commission from time to time, against liability for loss for claims arising out of any error or omission on the part of the applicant, its officers or employees;

c) have a paid-up capital of not less than amounts to be determined by the Commission from time to time; and

d) provide a performance bond or banker's guarantee in favour of the Commission as determined by the Commission from time to time.

Certification personnel

6. 1) A Certification Service Provider shall take all reasonable measures to ensure that every certification personnel -

a. is fit and qualified for the services provided;
b. has not been convicted, whether in Kenya or elsewhere of fraud ,theft or any offence under the Act, Amendment Act or these Regulations ;
c. is not an undischarged bankrupt or has entered into a composition or scheme of arrangement with his creditors;
d. has knowledge of the relevant provisions of the Act and these Regulations;
e. is conversant with the Certification Service Provider's certification practice statement;
f. possesses the relevant technical qualifications, expertise and experience to effectively carry out his duties; and
g. possesses any other qualifications that the

Commission may from time to time prescribe.

Records Management

7. 1) Every Certification Service Provider shall make and keep in a secure manner records relating to -

a. activities in issuance, renewal, suspension and revocation of certificates (including the process of identification of any person requesting a certificate from a licensed Certification Service Provider);
b. the process of generating subscribers' (where applicable) or the licensed Certification Service Provider's own key pairs;
c. the administration of a licensed Certification Service Provider's computing facilities; and
d. such critical related activity of a licensed Certification Service Provider as may be determined by the Commission from time to time.

2) A Certification Service Provider may keep its records either in paper-based document, electronic records or any other form approved by the Commission from time to time, and such records shall be indexed, stored, preserved and reproduced so as to be accurate, complete, legible and accessible to the Commission or any authorised officer.

3) Every Certification Service Provider shall archive all certificates issued by it and maintain mechanisms to access such certificates for a period of not less than 7 years.

4) Every licensed Certification Service Provider shall retain all records required to be kept under paragraph (1) and all logs of the creation of the archive of certificates referred to in paragraph (3) for a period of not less than 7 years.

Issuance of certificates

8. 1) Certificates shall contain:

a) the identity information of the Certification Service Provider;

b) the identity information by which the signature owner can be identified;

c) signature-verification data which corresponds to

signature-creation data;

d) the commencement and expiry date of the certificate;

e) the information regarding the authorization of the subscriber if such subscriber acts on behalf of another person;

f) information related to conditions of usage of the certificate and limits on the value of transactions where applicable;

g) the secure electronic signature of the certification service provider that verifies the information in the certificate;

h) information sufficient to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate would be listed if the certificate is suspended or revoked;

i) any other information required by the Commission to be included.

2) It shall be the responsibility of the certification service provider to determine reliably, based on official documents, the identity of the person to whom a certificate is issued. The subscriber identity verification method employed for issuance of certificates shall be specified in the certification practice statement.

3) Where an additional certificate is issued to a person on the basis of another valid certificate held by the same person and subsequently the original certificate is suspended or revoked, the Certification Service Provider that issued the new certificate must conduct investigations to determine whether it is necessary to suspend or revoke the new certificate.

4) A Certification Service Provider shall afford reasonable opportunity to a subscriber to verify the contents of the certificate before it is accepted.

5) A certification service provider shall be obliged to inform subscribers, in writing, that an advanced electronic signature has the same legal effect in a transaction as a handwritten signature, the limitations on

use of certificates and the dispute resolution procedures.

6) A certification service provider shall warn subscribers, in writing, not to allow third parties to use signature creation adata associated with signature verification data in the certificate.

7) Where the subscriber accepts the issued certificate, the Certification Service Provider shall publish a signed copy of the certificate in a repository referred to in paragraph (1).

8) Where the subscriber does not accept the certificate, the Certification Service Provider shall not publish it.

9) Once the certificate has been issued by the Certification Service Provider and accepted by the subscriber, the Certification Service Provider shall notify the subscriber within a reasonable time of any fact known to the Certification Service Provider that may significantly affect the validity or reliability of the certificate.

10) The date and time of all transactions in relation to the issuance of a certificate must be logged and kept in a secure manner.

Recognition of foreign certification service providers

9. 1) [Certification services provided by foreign-based Certification Service Providers may be recognized by the Commission pursuant to the Act and these Regulations, provided that such Certification Service Providers provide their services through agencies registered and based in Kenya and Licensed under the Act and these Regulations.]

Renewal of Certificates

10. 1) Regulation 8 shall apply to the renewal of certificates as it applies to the issuance of certificates.

2) The subscriber identity verification method employed for renewal of certificates shall be specified in the certification practice statement.

3) The date and time of all transactions in relation to the renewal of a certificate must be logged and kept in a secure manner.

Suspension of Certificates

11.

1) This regulation shall apply to Certification Service Providers that allow subscribers to request for suspension of certificates.

2) Certification Service Providers shall maintain facilities to receive and act upon requests for suspension at all times of the day and on all days of every year.

3) The subscriber identity verification method employed for suspension of certificates shall be specified in the certification practice statement.

4) The Certification Service Provider shall, upon receiving a valid request for suspension of a certificate, ensure that the certificate is suspended and notice of the suspension is published in the repository.

   Provided that where a request for suspension is received but a Certification Service Provider considers that revocation is justified in the light of all the evidence available to it, the Certificate Service Provider may revoke the certificate instead.

5) A Certification Service Provider may, regardless of the subscriber's consent, suspend a certificate that it has issued if it has reasonable grounds to believe that the certificate is unreliable.

   Provided that the Certification Service Provider shall conduct and complete its investigation into the reliability of the certificate and decide within a reasonable time whether to reinstate or to revoke the certificate.

6) It shall be the responsibility of relying parties to check the status of certificates they wish to rely upon.

7) A Certification Service Provider shall confirm with the subscriber or his authorised agent whether to reinstate or revoke the certificate after suspension.

8) A Certification Service Provider shall, within a reasonable time, terminate a suspension initiated by request, upon discovery and confirmation that the request for suspension was made without due authorisation of the subscriber.

9) Where the suspension of a certificate leads to revocation of the certificate, the requirements for revocation in

Regulation 12 shall apply.

10) The date and time of all transactions in relation to the suspension of certificates must be logged and kept in a secure manner.

Revocation of Certificates

12. 1) Certification Service Providers shall immediately revoke a certificate upon:

a) the request of a subscriber;
b) the detection of forgery or falsification of the information existing in the database or changes in such information; and
c) the detection of disability to act, bankruptcy or legally accepted disappearance or death of the subscriber.

2) Certification Service Providers shall maintain facilities to receive and act upon requests for revocation at all times of the day and on all days of every year.

3) In order to confirm the identity of the subscriber or authorised agent making a request for revocation, the Certification Service Provider must use the subscriber identity verification method specified in the certification practice statement.

4) A Certification Service Provider shall, upon revoking a certificate, give notice of the revocation to the subscriber and publish notification thereof in the repository.

5) The date and time of all transactions in relation to the revocation of certificates must be logged and kept in a secure manner.

6) It shall be the responsibility of relying parties to check the status of certificates they wish to rely upon.

Certification Practice Statement

13. 1) Certification Service Providers shall prepare certification practice statements in accordance with guidelines issued by the Commission from time to time and submit them for approval by the Commission before commencement of operations.

2) Any change to the certification practice statement shall

require prior written approval of the Commission.

3) A Certification Service Provider shall, in its certification practice statement, highlight to its subscribers any limitation of its liabilities and, in particular, draw the subscribers' attention to the implication of reliance limits on their certificates.

4) The subscriber identity verification method for the issuance, suspension, revocation and renewal of a certificate must be specified in the certification practice statement.

5) A copy of the latest version of the certification practice statement, together with its effective date, shall be filed with the Commission and published on the Certification Service Provider's website accessible to members of the public.

6) Certification Service Providers shall log all changes to the certification practice statement together with the effective date of each change.

7) A licensed Certification Service Provider shall keep in a secure manner a copy of each version of the certification practice statement together with the date it came into effect and the date it ceased to have effect.

Security Guidelines **14.**

1) Every licensed Certification Service Provider shall ensure that in the provision of its services it materially satisfies the security guidelines that may be issued by the Commission from time to time.

2) In determining whether a departure from the security guidelines has occurred, reasonable professional judgment shall be exercised as to whether a condition that does not strictly comply with the guidelines is or is not material, taking into consideration the circumstances and the system as a whole.

3) Without prejudice to the generality of paragraph (2), the following incidents of non-compliance shall be considered to be material:

    a. any non-compliance relating to the validity of a certificate;
    b. the performance of the functions of a certification personnel by a person who is not suitably qualified; or

c. the use by a Certification Service Provider of any system other than a secure system.

4) Every Certification Service Provider shall provide every subscriber with a secure and trustworthy system to generate his key pair.

5) Every Certification Service Provider shall provide the mechanism to generate and verify advanced electronic signatures in a secure and trustworthy manner and the mechanism provided shall also indicate the validity of the signature.

6) If the advanced electronic signature is not valid, the mechanism provided should indicate if the invalidity is due to the integrity of the document or the signature and the mechanism provided shall also indicate the status of the certificate.

7) For mechanisms provided by third parties other than the licensed Certification Service Provider, the resulting signature is considered secure only if the licensed Certification Service Provider endorses the implementation of such mechanisms in conjunction with its certificate.

8) Every licensed Certification Service Provider shall be responsible for the storage of keys (including the subscriber's key and the licensed Certification Service Provider's own key) in a secure and trustworthy manner.

Incident Handling **15.** 1) A Certification Service Provider shall implement an incident management plan that must provide at the least for management of the following incidents:

a. compromise of key;
b. penetration of Certification Service Provider's system and network;
c. unavailability of infrastructure; and
d. fraudulent registration and generation of certificates, certificate suspension and revocation information.

2) If any incident referred to in paragraph (1) occurs, it shall be reported to the Commission within 24 hours.

Confidentiality **16.** 1) Except for any prosecution under any written law or pursuant to an order of court, every licensed Certification Service Provider and its authorised agent must keep all subscriber-specific information confidential.

2) Any disclosure of subscriber-specific information by the licensed Certification Service Provider or its agent must be authorised by the subscriber.

3) This regulation shall not apply to subscriber-specific information which -

a. is contained in the certificate for public disclosure;
b. is otherwise provided by the subscriber to the licensed Certification Service Provider for this purpose; or
c. relates to the fact that the certificate has been revoked or suspended.

Liability of certification service providers **17.** 1) Unless the certification service provider proves that it was not negligent, it shall, by issuing or guaranteeing a certificate to the public, be liable for damage caused to any person who reasonably relies on the certificate:

a) as regards the accuracy, at the time of issuance, of all information contained in the certificate and as regards the fact that the certificate contains all the details prescribed for the certificate;

b) for assurance that at the time of the issuance of

the certificate, the signatory identified in the certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;

c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification service provider generates them both; and

d) for failure to register revocation of the certificate.

2) Where a certification service provider has indicated in its certificates, in a manner recognisable to third parties, the limits on the use of the certificates and the limits on the values of transactions for which the certificate can be used, it shall not be liable for damage resulting from exceeding the limits.

Availability of Repositories

18. 1) A general purpose repository shall be available at all times of the day and on all days of every year.

2) Subject to the approval of the Commission, a repository may be dedicated for a specific purpose for which specific hours of operation may be acceptable.

PART III REPOSITORY FUNCTIONS AND ADMINISTRATION OF SUB DOMAINS IN THE KENYA COUNTRY CODE TOP LEVEL DOMAIN

Management of the ccTLD repository and administration of sub domains in the Kenya country code top level domain

19. 1) The Commission may, from time to time, issue guidelines for management of the ccTLD repository and administration of sub domains in the Kenya country code top level domain.

2) Without prejudice of the generality of paragraph (1), such guidelines may require that sub domains assigned under the Kenya country code top level domain do not contain words, phrases or abbreviations that are obscene, scandalous, indecent or in any manner contrary to the law.

Obligations of Registrars

20. 1) Registrars shall, before registering any domain name, satisfy themselves that the name so submitted:

a. complies with the guidelines issued pursuant to regulation 18;

b. is not contrary to the law;
c. does not infringe the rights of third parties;
d. does not improperly give the impression of pertaining to public administration or the exercise of public powers

2) The Registrant shall be the holder of the registered domain name; provided that the Registrar reserves the right to recall the registered domain name if it is established that the registration was contrary to these Regulations.

Limitation of Liability

21. Liability for the infringement of third party rights and interest arising from holding or using a domain name shall be borne by the Registrant.

Confidentiality

22. All information obtained from Registrants shall be used solely for the purpose of domain name registration except where the law requires otherwise.

Back-up and Disaster recovery plan

23. Repository managers and administrators of second level sub-domain under the .ke ccTLD domain shall ensure that copies are kept of all registered data and put in place a disaster recovery plan.

Winding up

24. When an administrator of second level sub-domain winds up whether voluntarily or pursuant to a court order, all registered data shall be transferred to the repository of the .ke ccTLD which shall administer it until such time as the Commission shall license or authorise another second level sub-domain to run the functions of the said domain name(s).

PART IV:MISCELLANEOUS PROVISIONS

Offences and Penalties

25. (1) Any licensee who contravenes the provisions of this Regulation commits an offence.

(2) Any person who commits an offence under these Regulations shall be liable on conviction to a fine not exceeding three hundred thousand shillings or to imprisonment for a term

not exceeding three years or both.

Made on the ……..……., 2009.

SAMUEL POGHISIO,

Minister for Information and Communication.