IN EXERCISE of the powers conferred by section 83R of the Kenya Information and Communications Act, 1998, the Minister for Information and Communications, in consultation with the Communications Commission of Kenya, makes the following
Regulations: —

THE KENYA INFORMATION AND COMMUNICATIONS (ELECTRONIC CERTIFICATION AND DOMAIN NAME ADMINISTRATION) REGULATIONS, 2010

1. Citation.
These Regulations may be cited as the Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations, 2010.

2. Interpretation.
In these Regulations, unless the context otherwise requires —

"Administrative contact" means the entity responsible for maintenance of a domain name;

"Certification personnel" means any person who has—

(a) Direct responsibility for the day-to-day operations, security and performance of any activity, relating to a certification service provider, regulated under the Act and these Regulations; or

(b) Duties that directly involve the issuance, renewal, suspension, revocation of certificates, and creation of private keys or administration of a certification service provider's computing facilities;

"Certification practice statement" means a statement of the practices that a certification service providers employs when approving or rejecting certificate applications, or issuing, managing or revoking certificates.

"Country code Top Level Domain (ccTLD) administrator" means the entity managing the .ke ccTLD;

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

“Licensee” means a person licensed under the Act;

“Registrant” means a domain name holder;

“Registrar” means an entity that is authorized under the Act to administer the process of registration and modification of domain names;

“Relying party” means an individual or organization that acts on the basis of a certificate;

“Sub domain administrator” means an entity managing a sub domain in 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;

“Technical contact” means the entity responsible for maintaining the primary name server for a domain name and for effecting technical changes to a domain name;

“time-stamp” means a cryptographical digital attestation that a document or data existed at a particular time and has not been altered since a particular point in time and serves as a trusted third party witnessing the existence and particulars of electronic data;

“time-stamp services” means issuance of time-stamps.

3. License for electronic certification services.
The Commission may, upon application in the prescribed manner and subject to such requirements as it may consider necessary, grant a licence to a person to provide electronic certification services, services.

4. Application for a licence.
A person applying for a licence shall, in addition to the requirements prescribed in the Act and any Regulations made thereunder —

(a) Submit for approval a certification practice statement, which fulfils the requirements prescribed in these Regulations;

(b) Undergo and pass an initial audit; and

(c) Fulfill other requirements relating to qualification, expertise, manpower, financial resources and infrastructure facilities necessary to issue an advanced electronic signature certificate as may be prescribed by the Commission from time to time.

5. Recognition of foreign certification service Providers.
(1) The Commission may recognize a foreign certification service provider as a certification service provider for the purposes of these Regulations, where the foreign certification service provider—

(a) Is duly licensed or authorized by the relevant government authority in the country in which it operates;

(b) Complies with internationally acceptable standards and requirements under the Act and these Regulations; and

(c) Has established a local agent to provide the certification services in Kenya.

(2) A certificate issued by a certification service provider recognized under paragraph (1) shall be valid for the purposes of the Act and these Regulations.

(3) Where the Commission is satisfied that a foreign certification service provider has contravened any of the conditions and restrictions of recognition under paragraph (1), it may revoke the recognition.

6. Certification practice statement.
(1) A certification service provider shall, before commencement of its operations, prepare a certification practice statement, in accordance with these Regulations and guidelines issued by the Commission from time to time and submit it, for approval by the Commission.

(2) A certification service provider shall not change the certification practice statement without the prior written approval of the Commission.

(3) A certification service provider shall specify, in its certification practice statement-

(a) Any limitation of its liabilities and particularly, the implication of reliance limitations specified; and

(b) The subscriber identity verification method for the issuance, suspension, revocation and renewal of a certificate.

(4) A certification service provider shall file, with the Commission, a copy of its certification practice statement and specify its effective date and publish it on its web site.

(5) A certification service provider shall log all changes to the certification practice statement and specify the effective date of each change.

(6) A certification service provider shall keep, in a secure manner, a copy of each version of its certification practice statement and record the date it came into effect and the date it ceased to have effect.

7. Responsibilities of a certification service provider.
(1) A certification service provider shall —

(a) Issue and renew certificates;

(b) Suspend, reinstate or revoke certificates;

(c) Conduct personal identification of subscribers;

(d) Publish accurate information relating to certificates;

(e) Provide a repository service listing all published certificates, records of revoked certificates that may be used to verify the validity of published certificates;

(f) Ensure protection of private information and safekeeping of data security; and

(g) Provide time-stamp services.

8. Records management.
(1) A certification service provider shall, keep securely all records relating to —

(a) Issuance, renewal, suspension or revocation of certificates, including the identity of any person requesting for a certificate;

(b) The process of generating key pairs by the subscribers or the licensed certification service provider;

(c) The administration of its computing facilities; and

(d) Such other information as may be determined by the Commission from time to time.

(2) A certification service provider may keep its records in paper- based form, electronic form or any other form approved by the Commission from time to time.

(3) A certification service provider shall index, store, and preserve the records kept under paragraph (2) in a form that the records may be reproduced in an accurate, complete, legible manner and a manner accessible to the Commission or to any authorized officer.

(4) A certification service provider shall retain copies of all the certificates it has issued and preserve them so that they shall be accessible for a period of not less than seven years.

(5) A certification service provider shall retain all records required to be kept under paragraph (1) and all the logs of the creation of the archive of certificates required under paragraph (3) for a period of not less than seven years.

9. Issuance of certificates.
(1) A certification service provider certificate shall issue a certificate containing —

(a) Information identifying the certification service provider;

(b) Information identifying the signature owner;

(c) signature-verification data which corresponds to signature- creation data;

(d) The commencement and expiry date of the certificate;

(e) Information regarding the authorization of the subscriber, if a subscriber is acting on behalf of another person;

(f) Information regarding the 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) Sufficient information that can be used 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; and

(i) Any other information as may be determined by the Commission from time to time.

(2) A certification service provider shall determine, based on official documents, the identity of the person to whom a certificate is issued and shall specify, in the certification practice statement, the subscriber identity verification method applied in the issuance of certificates.

(3) A certification service provider shall give a subscriber an opportunity to verify the contents of the certificate before the subscriber accepts it.

(4) A certification service provider shall inform a subscriber, in writing, the legal effect of an advanced electronic signature, the limitations on use of certificates and the dispute resolution procedures, applicable.

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

(6) Where the subscriber accepts the issued certificate, the certification service provider shall publish a signed copy of the certificate in a repository in accordance with regulation 8.

(7) Where the subscriber does not accept the certificate, the certification service provider shall not publish the certificate.

(8) Once a 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 that subsequently becomes known

to the certification service provider that may significantly affect the validity or reliability of the certificate.

(9) A certification service provider shall log and keep in a secure manner the date and time of all transactions relating to the issuance of a certificate.

(10) Where a certification service provider issues an additional certificate to a person on the basis of a valid certificate held by the same person and subsequently the original certificate is suspended or revoked, the certification service provider shall investigate and determine whether the new certificate should also be suspended or revoked.

10. Obligations of a subscriber.
(1) Where a subscriber has accepted a certificate, the subscriber shall generate a key pair by applying the relevant security procedure.

(2) A subscriber shall be deemed to have accepted a certificate if he publishes or authorizes the publication of the certificate to any person, in a repository; or otherwise demonstrates his acceptance.

(3) A subscriber certifies, by accepting a certificate, to all who wish to reasonably rely on the information contained in the certificate that—

(a) The subscriber holds and is entitled to hold the private key corresponding to the public key listed in the certificate;

(b) All representations made by the subscriber to the certification service provider and all the information contained in the certificate are true; and

(c) All information in the certificate is within the knowledge of the subscriber is true.

(4) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his certificate and take the necessary steps to prevent its disclosure to any person who is not authorized to affix the advanced electronic signature of the subscriber.

(5) In the event that the subscriber becomes aware that the private key has been compromised, the subscriber shall, notify the certification service provider of such compromise within twenty four hours.

11. Liability of certification service providers.
(1) A certification service provider shall, by issuing or guaranteeing a certificate to the public, accept liability for damage caused to any person who reasonably relies on the certificate unless the certification service provider can prove that it was not negligent.

(2) The liability of a certification provider under paragraph (1) shall be limited to issues relating to—

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

(b) The 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) 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 generated both of them; and

(d) The failure to publish a notice of suspension or revocation of a certificate in the repository specified in the certificate.

(3) Where a certification service provider has specified in a certificate, the limits on the use of the certificates and the limits on the values of transactions for which the certificate may be used, it shall not be liable for any damage resulting from exceeding the limits.

12. Renewal of certificates.
(1) The provisions of regulation 9 shall apply mutatis mutandis to the renewal of certificates.

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

(3) A certification service provider shall log and keep, in a secure manner, the date and time of all transactions relating to the renewal of a certificate.

13. Suspension of certificates.
(1) A certification service provider shall maintain facilities that can receive and respond to requests for suspension of certificates at all times of the day and on all days of every year.

(2) A certification service provider shall, upon receiving a valid request under paragraph (1) suspend a certificate and publish a notice of the suspension in the respective repository.

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

(4) Where a request for suspension is received and a certification service provider determines the revocation of the certificate would be justified in the light of all the evidence available to it, the certificate service provider may revoke the certificate.

(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 revoke the certificate.

(6) A certification service provider shall, within a reasonable time, terminate a suspension initiated through a request, upon discovering and confirming that the request for suspension was made without the authorization of the subscriber.

(7) A certification service provider shall, after suspending a certificate, consult with the subscriber or his authorized agent on whether to reinstate or revoke the certificate.

(8) The provisions of regulation 11 shall apply where the suspension of a certificate leads to the revocation of the certificate.

(9) A certification service provider shall log and keep in a secure manner the date and time of all transactions relating to the suspension of certificates.

(10) A party who wishes to rely on any certificate shall, before relying on a certificate, establish the status of the certificate.

14. Revocation of certificates.
(1) A certification service providers shall revoke a certificate upon —

(a) Receiving a request for revocation from a subscriber or his authorized agent;

(b) Detecting forgery or falsification of the information existing in the database or changes in the information in database and

(c) Detecting the incapacity, bankruptcy or death of the subscriber:

Provided that where it is practicable, a certification service provider shall afford the subscriber a reasonable opportunity to be heard, before the revocation is effected.

(2) A certification service provider shall maintain facilities that can receive and act upon requests for revocation at all times of the day and on all days of every year.

(3) A certification service provider shall use the subscriber identity verification method specified in the certification practice statement to confirm the identity of the subscriber or authorized agent who makes a request for revocation.

(4) A certification service provider shall, after revoking a certificate, give a notice of revocation to the subscriber and publish the notice in the respective repository.

(5) A certification service provider shall log and keep in a secure manner the date and time of all transactions relating to the revocation of a certificate.

(6) A party who wishes to rely on any certificate shall, before relying on a certificate, establish the status of the certificate.

15. Performance audits.
The Commission shall, at least once in every year, audit the operations of a licensed certification service provider to monitor compliance with the Act and these Regulations.

16. Security guidelines.
(1) A certification service provider shall comply with the security guidelines that may be issued by the Commission.

(2) A certification service provider shall provide every subscriber with a secure and trustworthy system to generate his key pair.

(3) A certification service provider shall establish a mechanism that generates and verifies advanced electronic signatures in a secure and trustworthy manner and indicates the validity of a signature.

(4) Where the advanced electronic signature is not valid, the mechanism established under paragraph (3) should indicate the reason for invalidity and the status of the certificate.

(5) Where a verification mechanism is established by any person who is not a certification service provider, the resulting signature shall not be considered secure unless a licensed certification service provider endorses the implementation of mechanism and its certificate.

(6) A licensed certification service provider shall store the keys, including the subscriber's and the certification service provider's keys, in a secure and trustworthy manner.

17. 1ncent handling.
(1) A certification service provider shall establish an incident management plan to address, among others, incidents relating to-

(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) Where any incident referred to in paragraph (1) occurs, a certification service provider shall report the incident to the Commission within twenty four hours.

18. Confidentiality.
(1) A certification service provider shall not collect personal data directly from the subscribers or their authorised agents, unless the personal data is necessary for the purposes of issuance of a certificate.

(2) A certification service provider shall keep all information relating to a subscriber confidential.

(3) A certification service provider shall not disclose any information relating to a subscriber unless the disclosure is authorized by the subscriber:

Provided that a certification service provider may, pursuant to an order of the court, disclose information relating to a subscriber without the consent of the subscriber.

(4) The obligation to maintain confidentiality shall not apply to information relating to a subscriber which —

(a) Is contained in the certificate and is available to the public for inspection;

(b) Is otherwise provided by the subscriber to the licensed certification service provider for disclosure to the public; or

(c) Relates to the revocation or suspension of a certificate.

(5) Where a certification service provider has permitted a subscriber to use a pseudonym, the certification service provider shall, at the request of law enforcement authorities, disclose data relating to the subscriber that is required to prosecute offences or to protect against threats to public safety or public order.

19. Winding up of operations of a certification service provider.
(1) A certification service provider may, where the certification service provider intends to discontinue its operations-

(a) Arrange for its subscribers to re-subscribe to another licensed certification service provider;

(b) Make arrangements for its records and certificates to be archived in a secure manner; and

(c) Transfer its records to another licensed certification service provider in a secure manner.

(2) A certification service provider shall, where the certification service provider intends to discontinue its operations-

(a) give the Commission and its subscriber a minimum of six months notice, in writing, of its intention to discontinue its operations; and

(b) Publish, in at least one local daily newspaper with nationwide circulation and in such other manner as the Commission may determine, at least two months notice of its intention to discontinue its operations.

20. Licensing for updating of a repository and administering a sub domain in the .ke ccTLD.

(1) The Commission may, upon application in the prescribed manner and subject to such conditions as it may consider necessary, grant a licence for updating a repository or administering a sub-domain in the Kenya country code top level domain.

(2) A person shall not create a new sub-domain under the Kenya country code Top Level Domain without the approval of the Commission.

(3) The Commission may issue guidelines for assignment of sub domains under the ccTLD namespace and prescribe-

(a) Words, phrases or abbreviations that may not constitute a sub-domain name; or

(b) Words, phrases or abbreviations that are reserved for special purposes.

21. Responsibilities of .ke ccTLD administrator.
(1) The administrator of the shall —

(a) Be the administrative technical and contact for the ccTLD;

(b) Administer the .ke ccTLD;

(c) Maintain the operational stability and utility of the ccTLD;

(d) Notify the Commission of any change in the ccTLD data;

(e) Provide name service for the ccTLD and ensure that the database is secure and stable;

(f) Comply with the Commission's guidelines for the administration of the ccTLD; and

(g) Allow the Commission to access ccTLD zone files.

22. Winding up of operations of the .ke ccTLD administrator.
The administrator of the ccTLD shall, where the

(a) Give the Commission and administrators of sub domains in the ccTLD a minimum of six months, notice in writing, of its intention to discontinue its operations;

(b) Publish, in at least one local daily newspaper with nationwide circulation and in such other manner as the Commission may determine, at least four months notice of its intention to discontinue its operations;

(c) Furnish the Commission with an up-to-date copy of its zone files; and

(d) Seek the Commission's approval for the transfer of the zone files to another entity, in a secure manner.

23. Responsibilities of a sub-domain administrator.
(1) The administrator of a sub-domain in the .ke ccTLD shall —

(a) Administer a sub-domain in the .ke ccTLD;

(b) At all times, maintain a website that contains registration information;

(c) Maintain the operational stability and utility of the sub-domain in the .ke ccTLD;

(d) Notify the Commission of any change in the data of a sub-domain;

(e) Provide the name service for a sub-domain and ensure that the database is secure and stable;

(f) Provide a domain registration system for the sub-domain;

(g) Allow the Commission to access the zone files and registration data for the sub-domain; and

(h) Comply with the Commission's guidelines for the administration of sub-domain in the .ke ccTLD;

24. Winding up of operations of a sub domain administrator.
The administrator of a sub-domain shall, where the administrator intends to discontinue its operations—

(a) Give the Commission and its registrants a minimum of six months notice, in writing, of its intention to discontinue its operations;

(b) Publish, in at least one local daily newspaper with nationwide circulation and in such other manner as the Commission may determine, at least four months notice of its intention to discontinue its operations;

(c) Furnish the Commission with an up-to-date copy of its zone files; and

(d) Seek the Commission's approval for the transfer of the zone files and registration data to another administrator of a sub domain in the .ke ccTLD, in a secure manner.

25. Performance audits.
The Commission shall, at least once in every year, audit the operations of the administrator of the .ke ccTLD and sub-domain administrators, to evaluate compliance with the Act and these Regulations.

26. Limitation of liability.
A registrant shall bear liability for the infringement of third party rights and interest arising from holding or using a domain name in the ccTLD.

27. Confidentiality.
A sub-domain administrator shall use the information obtained from its registrants for the purpose of domain name registration except where the law requires otherwise.

28. Offences and penalties.

(1) Any licensee who contravenes the provisions of these Regulations commits an offence.

(2) Any person who commits an offence under these Regulations for which no penalty is expressly provided shall be liable on conviction to imprisonment for term not exceeding five years or a fine not exceeding one million shillings or both.

Made on the 12th July, 2010

Samuel Poghisio,
Minister for Information and Communications