GOVERNMENT NOTICE NO. 228 published on 05/05.2016

THE ELECTRONIC TRANSACTIONS ACT

(CAP. 442)

_____

REGULATIONS

_____

TABLE OF CONTENTS

Regulation	*Title*
1.	Citation
2.	Interpretation

PART II
APPLICATION FOR CRYPTOGRAPHIC AND CERTIFICATION SERVICES PROVIDER

3.	Application to be cryptographic and certification services provider
4.	Period of validity of licences
5.	Renewal of licence
6.	Licence fee

PART III
CRITERIA FOR APPLICATION OF A LICENCE

7.	Registration
8.	Capital requirements
9.	Performance bond or banker's guarantee
10.	Applicant to ensure that trusted person is fit
11.	Operational
12.	Auditing requirements

G.N. No. 228 (contd.)

PART IV

REFUSE TO GRANT OR RENEW LICENCES IN CERTAIN CIRCUMSTANCES

13. Regulator to refuse to grant or renew licences in certain circumstances
14. Powers of Regulator in cases of misconduct
15. Effect of revocation or suspension of licence
16. Appeal against refusal to license
17. Trustworthy record keeping and archival
18. Trustworthy transaction logs
19. Types of certificates
20. Issuance of certificates
21. Renewal of certificates
22. Suspension of certificates
23. Revocation of certificates
24. Expiry date of certificates
25. Certification practice statement
26. Secure digital signatures
27. Security guidelines
28. Incident handling
29. Confidentiality
30. Change in management
31. Availability of general purpose repository.
32. Specific purpose repository
33. Waiver
34. Disclosure
35. Discontinuation of operations
36. Penalties
37. Compounding of offences

G.N. No. 228 (contd.)

THE ELECTRONIC TRANSACTIONS ACT
(CAP.442)

_____

REGULATIONS

_____

(Made under section 37)

_____

THE ELECTRONIC TRANSACTIONS (CRYPTOGRAPHIC AND CERTIFICATION SERVICES PROVIDERS) REGULATIONS, 2016

PART I
PRELIMINARY PROVISIONS

Citation

1. These Regulations may be cited as the Electronic Transactions (Cryptographic and Certification Services Providers) Regulations, 2016.

Interpretation

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

"Certificate Authority or Certification Authority (CA)" means an entity that issues digital certificates;

"cryptographic and certification services provider" means service providers associated with practice and certification of techniques for secure communication via construction and/or analysis of protocols that block adversaries/third parties and the provision of key storage, all that comply with National or International legislations.

"licence" means a licence granted under these Regulations;

"Regulator" means the Tanzania Communications Regulatory Authority which is also known by its acronym TCRA;

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

"trusted person" means any person who has direct responsibilities for the day-to-day operations, security and performance of the business activities that are regulated under the Act or these Regulations;

G.N. No. 228 (contd.)

PART II
APPLICATION FOR CRYPTOGRAPHIC AND CERTIFICATION SERVICES PROVIDER

Application to be cryptographic and certification services provider

3.-(1) Every application to be a cryptographic and certification services provider shall be made in such form and manner as the Regulator may, from time to time, determine and shall be supported by such information as the Regulator may require.

(2) Subject to section 35(2) of the Act, the Regulator may require the applicant to furnish such additional information as are necessary in support of the application.

(3) The Regulator may allow applications for renewal of licences to be submitted in the form of electronic records subject to such requirements as the Regulator may impose.

(4) A licence shall be subject to such conditions, restrictions and limitations as the Regulator may, from time to time, determine.

Period of validity of licences

4. A licence shall be valid for a period of one year or such other longer period as the Regulator may allow.

Renewal of licence

5.-(1) The provisions of regulation 3 shall apply to an application for renewal of a licence as it applies to a fresh application for a licence.

(2) A cryptographic and certification service provider shall submit an application for the renewal of licence not later than three months before the expiry of a licence.

(3) Where the cryptographic and certification service provider has no intention to renew its licence, the cryptographic and certification service provider shall -

(a) inform the Regulator in writing not later than three months before the expiry of the licence;

(b) inform all its subscribers in writing not later than two months before the expiry of the licence; and

(c) advertise such intention in such daily newspaper and in such manner as the Regulator may determine, not later than two months before the expiry of the licence

G.N. No. 228 (contd.)

Licence fee

6-(1) An application fee shall be prescribed by the Regulator and shall be payable to the Regulator on every application for the grant or renewal of a licence to be a cryptographic and certification service provider.

(2) Where the application referred to in sub regulation (1) is approved, there shall be payable to the Regulator an annual licence fee.

(3) There shall be payable to the Regulator on every grant of the renewal of a licence a fee which will be prescribed by the Regulator.

(4) The Regulator shall not refund any fee paid if the application is not approved, withdrawn or discontinued or where the licence is suspended or revoked.

PART III
CRITERIA FOR APPLICATION OF A LICENCE

Registration

7. An applicant for a licence shall be-

(a) a company registered or incorporated under the laws of Tanzania; and

(b) insured against liability for loss of the amount to be determined by the Regulator for each claim arising out of any error or omission on the part of the applicant, its officers or employees.

Capital requirements

8. The applicant for a licence shall have-

(a) a paid up capital of such amount shall be as determined by the Regulator; and

(b) proof of available financing to be determined by the Regulator.

banker's guarantee

9.-(1) The applicant shall furnish a banker's guarantee in favour to the Regulator in a form approved and in such amount as may be determined by the Regulator.

(2) The performance banker's guarantee referred to in sub regulation (1) may be invoked for payment of-

(a) an offer of composition made by the Regulator;

(b) liabilities and rectification costs attributed to the negligence of the certification authority, its officer or employees; or

(c) the costs incurred in the discontinuation or

transfer of operations of the cryptographic and certification service provider, where the certification authority's licence or operations in discontinued.

Applicant to ensure that trusted person is fit

10.-(1) An applicant shall take reasonable measures to ensure that every trusted person-

(a) is a fit and qualified person to carry out the duties assigned to him;

(b) is not an undercharged bankrupt in Tanzania or elsewhere or has made a composition or an arrangement with his creditors; and

(c) has not been convicted in six month prior to an application, whether in Tanzania or elsewhere, of -

(i) an offence the conviction for which involved a finding that he acted fraudulently or dishonestly; or

(ii) an offence under this Regulations.

(2) Every trusted person shall-

(i) have a good knowledge of the Act and these Regulations;

(ii) be trained in the cryptographic and certification service provider certification practice statement; and

(iii) possess the relevant technical qualifications, expertise and experience to effectively carry out his duties

Operational

11.-(1) An applicant shall, before grant of a licence-

(a) have a certification practice statement approved by the Regulator;

(b) undergo and pass an initial operational audit before a licence is granted by the Regulator; or

(c) undergo and pass such audit as the Regulator may, by notice in writing, require.

(2) The audits referred under sub regulation (1) shall be -

(a) conducted in accordance with the auditing requirements specified in regulation 10; and

(b) completed within such time as the Regulator may, by Notice published in the *Gazette*, specify.

G.N. No. 228 (contd.)

Auditing requirements

12.-(1) An applicant shall pass any audit required under regulation 9(1) for compliance with -

(a) security guidelines as referred to in regulation 26;

(b) licensing conditions;

(c) certification practice statement;

(d) rules and guidelines as may be issued from time to time by the Regulator;

(e) the provisions of the Act and these Regulation; and

(f) any other written laws.

(2) Audit shall be done by a person registered as an auditor under the Auditors and Accountants (Registration) Act, 1972, appointed by the Regulator on such terms and conditions as the Regulator may determine;

(3) Auditing fees shall be borne by the cryptographic and certification service provider.

(4) A copy of every audit report shall be submitted to the Regulator within four weeks of the completion of an audit.

(5) Failure to pass the audit may be a ground for revocation of a licence.

PART IV

REFUSE TO GRANT OR RENEW LICENCES IN CERTAIN CIRCUMSTANCES

Regulator to refuse to grant or renew licences in certain circumstances

13. The Regulator may refuse to grant or renew a licence under the following circumstances-

(a) the applicant has not provided the Regulator with such information relating to it or any person employed by or associated with it for the purposes of its business, and to any circumstances likely to affect its method of conducting business, as the Regulator may require;

(b) the applicant or its majority shareholderis in the course of being wound up or liquidated;

(c) a receiver or and manager has been appointed by the applicant or its substantial shareholder;

(d) the applicant or its majority shareholder has, whether in Tanzania or elsewhere, entered into a compromise or scheme of arrangement with its creditors, being a compromise or scheme of arrangement that is still in operation;

(e) the applicant or the majority shareholder or any trusted person has been convicted, whether in Tanzania or elsewhere of an offence and the conviction involved a finding that he acted fraudulently or dishonestly or has been convicted of an offence under the Act or these Regulations;

(f) the Regulator is not satisfied as to the qualifications or experience of the trusted person who is to perform duties in connection with the holding of the licence by the applicant;

(g) the applicant fails to satisfy the Regulator that he or the trusted person is a fit and proper person to be licensed are or the trusted persons and majority shareholders;

(h) the Regulator has reason to believe that the applicant may not be able to act in the best interest of its subscribers, customers or participants having regard to the reputation, character, financial integrity and reliability of the applicant or any of its substantial shareholders or trusted persons;

(i) the Regulator is not satisfied as to the financial standing of the applicant or its substantial shareholder;

(j) the Regulator is not satisfied as to the record of past performance or expertise of the applicant or its trusted person having regard to the nature of the business which the applicant may carry on in connection with the holding of the licence;

Powers of Regulator in cases of misconduct

14.-(1) The Regulator may inquire into any allegation that a certification authority, its officers or employees, is or has been guilty of any misconduct or is no longer fit to continue to remain licensed by reason of any other circumstances which have led, or are likely to lead to the

improper conduct of business by it or to reflect discredit on the method of conducting business.

(2) Where, after inquiring into an allegation under sub regulation (1), the Regulator is of the opinion that the allegation is proved, the Regulator may if he thinks fit -

(a) revoke the licence of the cryptographic and certification service provider;

(b) suspend the licence of the cryptographic and certification service provider for such period as the Regulator may determine; or

(c) reprimand the cryptographic and certification service provider.

(3) The Regulator shall, at the hearing of an inquiry into an allegation under sub regulation (1) against a cryptographic and certification service provider, give the cryptographic and certification service provider an opportunity of being heard.

(4) Where the Regulator is satisfied, after making an inquiry into an allegation under sub regulation (1), that the allegation has been made in bad faith or that it is otherwise frivolous or vexatious, the Regulator may, by order in writing, require the person who made the allegation to pay any costs and expenses involved in the inquiry.

(5) The Regulator may issue directions to the cryptographic and certification service provider for compliance under the Act as a result of making the inquiry.

(6) For the purposes of this regulation, "misconduct" means-

(a) any failure to comply with the requirements of the Act or these Regulations or its certification practice statement; and

(b) any act or omission relating to the conduct of business of a cryptographic and certification service provider which is or is likely to be prejudicial to public interest,

Effect of revocation or suspension of licence

15.-(1) A cryptographic and certification service provider whose licence is revoked or suspended under regulation 12 or 13 shall, for the purposes of this regulation, be deemed not to be licensed from the date that the Regulator revokes or suspends the licence, as the case may be.

(2) A revocation or suspension of a licence of a cryptographic and certification service provider shall not operate so as to -

(a) avoid or affect any agreement, transaction or arrangement entered into by the cryptographic and certification service provider, whether the agreement, transaction or arrangement was entered into before or after the revocation or suspension of the licence; or

(b) affect any right, obligation or liability arising under any such agreement, transaction or arrangement.

(3) Without prejudice to the Regulator's powers under regulation 13, the revocation or suspense of a license under regulation 14 or its expiry shall not affect the validity or effect of any certificate issued by the certification service provider concerned before such revocation, suspense or expiry.

(4) For the purpose of sub-regulation (3), the Regulator shall appoint another licensed certification service provider to take over the certificates issued by the certification service provider whose license has expired and the certificate shall, to the extent that they comply with the requirements of the appointed licensed certification service provider, be deemed to have been issued by that licensed certification service provider.

(5) Sub-regulation (4) shall not preclude the appointed licensed certification service provider from requiring the subscriber to comply with its requirements in relation to the issue of certificates or from issuing a new certificate to the subscriber for the unexpired period of the original certificate except that any additional fees or charges to be imposed shall only be imposed with the prior written approval of the Regulator.

Appeal against refusal to license

16.-(1) Where -

(a) the Regulator refuses to grant or renew a licence under regulation 11;

(b) the Regulator revokes a licence under regulation 12;

(c) the licence is revoked or suspended, or a cryptographic and certification service provider is

reprimanded, under regulation 13; or

(d) a performance bond or banker's guarantee is invoked under regulation 9,

any person who is aggrieved by the decision of the Regulator may, within fourteen days after he is notified of the decision, may appeal to the Fair Competition Tribunal whose decision shall be final.

(2) If an appeal is made against a decision made by the Regulator, the Regulator may, if he thinks fit, defer the execution of the decision, as the case may be, until a decision is made by the Minister or when the appeal is withdrawn.

(3) In considering whether to defer the execution of the decision, the Regulator shall have regard to whether the deferment is prejudicial to the interests of any subscriber of the cryptographic and certification service provider or any other party who may be adversely affected.

(4) If an appeal is made to the Minister, a copy of the appeal shall be lodged with the Regulator.

Trustworthy record keeping and archival

17.-(1) A cryptographic and certification service provider may keep its records in the form of paper-based documents, electronic records or any other form approved by the Regulator.

(2) The records referred to under sub regulation (1) shall be indexed, stored, preserved and reproduced so as to be accurate, complete, legible and accessible to the Regulator, an auditor or an authorised officer.

Trustworthy transaction logs

18.-(1) Every cryptographic and certification service provider shall make and keep in a trustworthy manner the 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 cryptographic and certification service provider);

(b) the process of generating subscribers (where applicable) or the cryptographic and certification service provider's own key pairs;

(c) the administration of a cryptographic and certification service provider's computing

facilities; and

(d) such critical related activity of a cryptographic and certification service provider as may be determined by the Regulator.

(2) Every cryptographic and certification service provider shall archive certificates issued by Regulator and maintain mechanisms to access such certificates for a period of not less than five years.

(3) Every cryptographic and certification service provider shall retain records required to be kept under sub regulation (1) and logs of the creation of the archive of certificates referred to in sub regulation (2) for a period of not less than five years.

Types of certificates

19.-(1) Subject to the approval of the Regulator, a cryptographic and certification service provider may be issued certificates of the following different levels of assurance:

(a) certificates which shall be considered as trustworthy certificates for the purposes of the Act; and

(b) certificates which shall not be considered as trustworthy certificates for the purposes of the Act.

(2) The cryptographic and certification service provider shall associate a distinct certification practice statement approved by the Regulator for each type of certificate issued.

(3) The cryptographic and certification service provider shall draw the attention of subscribers and relying parties to the effect of using and relying on certificates that are not considered trustworthy certificates for the purposes of the Act.

Issuance of certificates

20.-(1) In addition to the requirements specified in the Act, every cryptographic and certification service provider shall comply with the requirements of this regulation in relation to the issuing of certificates.

(2) The certificate shall contain or incorporate by reference such information as is sufficient to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate shall be listed if the

certificate is suspended or revoked.

(3) The practices and procedures set forth in the certification practice statement of a cryptographic and certification service provider shall contain conditions with standards higher than those conditions specified in the Act.

(4) The subscriber identity verification method employed by the cryptographic and certification service providers for issuance of certificates shall be specified in the certification practice statement and be subject to the approval of the Regulator during the application for a licence.

(5) Where a certificate is issued to a person (referred to in this regulation as the new certificate) on the basis of another valid certificate held by the same person (referred to in this regulation as the originating certificate) and subsequently the originating certificate has been suspended or revoked, the cryptographic and certification service provider shall conduct investigations to determine whether it is necessary to suspend or revoke the new certificate.

(6) The cryptographic and certification service provider shall provide a reasonable opportunity for the subscriber to verify the contents of the certificate before it is accepted.

(7) Where the subscriber accepts the issued certificate, the cryptographic and certification service provider shall publish a signed copy of the certificate in a repository referred to under sub regulation (2).

(8) Notwithstanding sub regulation (7), the cryptographic and certification service provider may contractually agree with the subscriber not to publish the certificate.

(9) Where the subscriber does not accept the certificate, the cryptographic and certification service provider shall not publish it.

(10) Once the certificate has been issued by the cryptographic and certification service provider and accepted by the subscriber, the cryptographic and certification service provider shall notify the subscriber within fourteen days of any fact known to the cryptographic and certification service provider that significantly affects the validity or reliability of the certificate.

(11) A cryptographic and certification service provider shall be logged and kept in a trustworthy manner the

date and time of transactions in relation to the issuance of a certificate.

Renewal of certificates

21.-(1) The provisions of regulation 19 shall apply to the renewal of certificates as it applies to the issuance of certificates.

(2) The cryptographic and certification service provider shall have identity verification method which shall be specified in the certification practice statement as approved by the Regulator.

(3) The date and time of all transactions in relation to the renewal of a certificate shall be logged and kept by the Regulator.

Suspension of certificates

22.-(1) This regulation shall apply to cryptographic and certification service provider which allows subscribers to request for suspension of certificates.

(2) A cryptographic and certification service provider may provide for immediate revocation instead of suspension where the subscriber has agreed in writing.

(3) Upon receiving a request for suspension of a certificate under this regulation, the cryptographic and certification service provider shall ensure that the certificate is suspended and notice of the suspension is published in the repository in accordance with these Regulations.

(4) A cryptographic and certification service provider may suspend a certificate that it has issued if the cryptographic and certification service provider has reasonable grounds to believe that the certificate is unreliable, regardless of whether the subscriber consents to the suspension; but the cryptographic and certification service provider shall complete its investigation into the reliability of the certificate and decide within a reasonable time whether to reinstate the certificate or to revoke the certificate in accordance with the provisions of these Regulations.

(5) Any person relying on a certificate shall be responsible to check whether a certificate has been suspended.

(6) A cryptographic and certification service provider shall suspend a certificate after receiving a valid request for suspension, and where the cryptographic and certification service provider considers that revocation is justified in the light of evidence available to it, the certificate

shall be revoked in accordance with the provisions of these Regulations.

(7) A cryptographic and certification service provider shall check with the subscriber or his authorised agent whether the certificate should be revoked and whether to reinstate the certificate after suspension.

(8) A cryptographic and certification service provider shall terminate a suspension initiated by request where the cryptographic and certification service provider discovers and confirms that the request for suspension was made without authorisation by the subscriber or his authorised agent.

(9) Where the suspension of a certificate leads to a revocation of the certificate, the requirements for revocation shall apply.

(10) A cryptographic and certification service provider shall be logged and kept in a trustworthy manner the date and time of all transactions in relation to the suspension of certificates.

(11) A cryptographic and certification service provider shall maintain facilities to receive and act upon requests for suspension at all times.

Revocation of certificates

23.-(1) In order to confirm the identity of the subscriber or authorised agent making a request for revocation under these Regulations, the cryptographic and certification service provider shall use the subscriber identity verification method specified in the certification practice statement for this purpose.

(2) A cryptographic and certification service provider shall, after receiving a request for revocation, verify the request, revoke the certificate and publish notification of it under these Regulations.

(3) A cryptographic and certification service provider shall maintain facilities to receive and act upon requests for revocation at all times.

(4) A cryptographic and certification service provider shall give notice to the subscriber immediately upon the revocation of a certificate.

(5) A cryptographic and certification service provider shall be logged and kept in a trustworthy manner the date and time of transactions in relation to the revocation of

G.N. No. 228 (contd.)

certificates.

Expiry date of certificates

24. A certificate shall state the date on which it expires.

Certification practice statement

25.-(1) Every licensed certification authority shall use cryptographic and certification practices framework reproduced by the Regulator as a guide for the preparation of its certification practice statement.

(2) Any change to the certification practice statement during the term of the licence requires the prior approval of the Regulator.

(3) Every cryptographic and certification service provider shall highlight to its subscribers any limitation of their liabilities and in particular, it shall 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 shall be specified in the certification practice statement.

Secure digital signatures

26.-(1) The technical implementation of the requirements in section 7 of the Act shall be such as to ensure that it is computationally infeasible for any person other than the person to whom the signature correlates to have created a digital signature which is verified by reference to the public key listed in that person's certificate.

(2) The signature on its own should be such that it -

(a) ensure that the name or other unique identifiable notation of the person to whom the signature correlates be incorporated as part of the signature and cannot be replaced or forged; and

(b) readily present such indicia of identity to a person intending to rely on the signature.

(3) The technical implementation should ensure that -

(a) the steps taken towards the creation of the signature shall be under the direction of the person to whom the signature correlates; and

(b) no other person can reproduce the sequence of steps to create the signature and thereby create a valid

signature without the involvement or the knowledge of the person to whom the signature correlates

(4) The technical implementation shall indicate to a relying party of a signature whether the document or record that the signature purports to sign has been modified in anyway and this indication shall be revealed in the process of verifying the signature.

Security guidelines

27.-(1) Every cryptographic and certification service provider shall ensure that in the performance of its services it materially satisfies the security guidelines determined and published by the Regulator.

(2) In determining whether a departure from the security guidelines is material the Regulator shall exercise reasonable professional judgment as to whether the alleged breach of the guidelines is or is not material, taking into consideration the circumstances and the system as a whole.

(3) Without prejudice to sub regulation (2), the Regulator may consider to be material the following incidents:

(a) any non-compliance relating to the validity of a certificate;

(b) the performance of the functions of a trusted person by a person who is not suitably qualified; or

(c) the use by a cryptographic and certification service provider of any system other than a trustworthy system.

(4) The security guidelines shall be interpreted in a manner that is reasonable in relation to the context in which a system is used and is consistent with other laws.

(5) Every cryptographic and certification service provider shall provide to every subscriber with a trustworthy system to generate his key pair.

(6) Every cryptographic and certification service provider shall provide the mechanism to generate, verify and indicate the validity of the digital signatures in a trustworthy manner.

(7) Where the digital signature is not valid, the mechanism provided shall indicate,-

(a) whether the invalidity is due to the integrity of the document or the signature; and

(b) the status of the certificate.

(8) For mechanisms provided by third parties other

than the cryptographic and certification service provider, the resulting signature is considered secure where the cryptographic and certification service provider endorses the implementation of such mechanisms in conjunction with its certificate.

(9) Every cryptographic and certification service provider shall be responsible for the storage of keys (including the subscriber's key and the cryptographic and certification service provider's own key) in a trustworthy manner.

(10) The Regulator may, from time to time, publish details of the security guidelines for compliance by every cryptographic and certification service provider.

Incident handling

28. A cryptographic and certification service provider shall implement an incident management plan that shall provide at the least for management of the following incidents:

(a) compromise of key;

(b) penetration of Certificate Authority system and network;

(c) unavailability of infrastructure; and

(d) fraudulent registration and generation of certificates, certificate suspension and revocation information.

Confidentiality

29.-(1) Unless it is provided by any written law, every cryptographic and certification service provider and its authorised agent shall keep all subscriber-specific information confidential.

(2) Any disclosure of subscriber-specific information by the cryptographic and certification service provider or its agent shall 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 cryptographic and certification service provider for this purpose; or

(c) relates to the fact that the certificate has been revoked or suspended.

G.N. No. 228 (contd.)

Change in management

30. A cryptographic and certification service provider shall inform the Regulator of any changes in the appointment of any person as its director or chief executive, or of any person to perform functions equivalent to that of a chief executive, within three working days from the date of appointment of that person.

Availability of general purpose repository.

31.-(1) A cryptographic and certification service provider shall maintain and keep general repository available at all times.

(2) A cryptographic and certification service provider shall ensure that-

(a) the general purpose repository under sub regulation (1) is available all times;

(b) the total aggregate period of any down time in any period of one month shall not exceed 0.3% of the period; and

(c) any down time, whether scheduled or unscheduled, shall not exceed 30 minutes duration at any one time.

Specific purpose repository

32. Subject to the approval of the Regulator, a repository may be dedicated for a specific purpose for which specific hours of operation may be acceptable.

Waiver

33.-(1) Any cryptographic and certification service provider wishes to apply for a waiver of any of the requirements specified in these Regulations may apply in writing to the Regulator at the time when it submits an application for a licence.

(2) The application shall be supported by reasons for the application including the necessary supporting documents.

Disclosure

34.-(1) The cryptographic and certification service provider shall submit half-yearly progress and financial reports to the Regulator.

(2) The half-yearly progress reports shall include information on -

(a) the number of subscribers;

(b) the number of certificates issued, suspended, revoked, expired or renewed;

(c) system performance including system up and down time and any extraordinary incidents;

(d) changes in the organisational structure of the certification authority;

(e) changes since the preceding progress report submitted or since the application for the licence;
and

(f) changes in the particulars of any trusted person since the last submission to the Regulator, including the name, identification number, residential address, designation, function and date of employment of the trusted person.

(3) The cryptographic and certification service provider has a continuing obligation to disclose to the Regulator any changes in the information submitted.

(4) All current versions of the cryptographic and certification service provider's applicable certification practice statements together with their effective dates shall be published in the cryptographic and certification service provider's Internet website.

Discontinuation of operations

35.-(1) Where a cryptographic and certification service provider intends to discontinue its operations, the cryptographic and certification service provider may arrange for its subscribers to re-subscribe to another cryptographic and certification service provider.

(2) The cryptographic and certification service provider shall make arrangements for its records and certificates to be archived in a trustworthy manner.

(3) If the records are transferred to another cryptographic and certification service provider, the transfer shall be done in a trustworthy manner.

(4) A cryptographic and certification service provider shall -

G.N. No. 228 (contd.)

(a) give the Regulator a minimum of three months written notice of its intention to discontinue its operations;

(b) give its subscribers a minimum of two months written notice of its intention to discontinue its operations; and

(c) advertise, in such daily newspaper and in such manner as the Regulator may determine, at least two months' notice of its intention to discontinue its operations.

Penalties

36. Any person who fails, without any reasonable excuse, to comply with regulation 16(2), 17, 19(2) or (11), 21(10), 22(5), or (8) or 28 shall be guilty of an offence and shall be liable on conviction to a fine not less than five million Tanzanian shillings and, in the case of a second or subsequent conviction, to a fine not less than three times the fine imposed on the first conviction.

Compounding of offences

37. Without prejudice to any other law in force in Mainland Tanzania, the Regulator may, at any time prior to the commencement of court proceedings and subject to a voluntary admission of the commission of offence under these Regulations**,** compound the offence and order that person to pay a sum of money specified by him but not exceeding the amount of fine prescribed for any of such offence.

Dar es Salaam
1st June, 2016

MAKAME MBARAWA,
Minister of Works, Transport and Communication