ACTS
SUPPLEMENT No. 4 **18th March, 2011.**

ACTS SUPPLEMENT

to The Uganda Gazette No. 19 Volume CIV dated 18th March, 2011.

Printed by UPPC, Entebbe, by Order of the Government.

Act 7 *Electronic Signatures Act* **2011**

THE ELECTRONIC SIGNATURES ACT, 2011.

ARRANGEMENT OF SECTIONS

Section.

Section.

THE ELECTRONIC SIGNATURES ACT, 2011.

An Act to make provision for and to regulate the use of electronic signatures and to provide for other related matters.

DATE OF ASSENT: 17th February, 2011.

Date of Commencement: See section 1.

BE IT ENACTED by Parliament as follows:

PART I—PRELIMINARY

1. Commencement

This Act shall come into force on a date appointed by the Minister by statutory instrument.

2. Interpretation

In this Act, unless the context otherwise requires—

"accept a certificate" means—

(a) to manifest approval of a certificate, while knowing or having notice of its contents; or

(b) to apply to a certification service provider for a certificate, without revoking the application by delivering notice of the revocation to the licensed certification service provider and obtaining a signed, written receipt from the certification service provider, if the certification service provider subsequently issues a certificate based on the application;

"advanced electronic signature" means an electronic signature, which is—

(a) uniquely linked to the signatory;

(b) reliably capable of identifying the signatory;

(c) created using secure signature creation device that the signatory can maintain; and

(d) linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and the signature are detectable;

"asymmetric cryptosystem" means an algorithm or series of algorithms, which provide a secure key pair;

"authorised officer" means the Controller or a police officer or a public officer performing any functions under this Act; and includes any public officer authorised by the Minister or by the controller to perform any functions under this Act;

"certificate" means a data message or other records confirming the link between a signatory and a signature creation data;

"certification service provider disclosure record" means an on-line and publicly accessible record that concerns a licensed certification service provider, which is kept by the Controller under subsection 21(5);

"certification practice statement" means a declaration of the practices, which a certification service provider employs in issuing certificates generally or employs in issuing a particular certificate;

"certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;

"certify" means to declare with reference to a certificate, with ample opportunity to reflect and with a duty to apprise oneself of all material facts;

"confirm" means to ascertain through diligent inquiry and investigation;

"Controller" means National Information Technology Authority- Uganda;

"correspond", with reference to keys, means to belong to the same key pair;

"currency point" has the meaning assigned to it in the Schedule in this Act;

"digital signature" means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine—

(a) whether the transformation was created using the private key that corresponds to the signer's public key; and

(b) whether the message has been altered since the transformation was made;

"electronic signature" means data in electronic form affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message; and includes an advance electronic signature and the secure signature;

"electronic signature product" means configured hardware or software or relevant components of it, which are intended to be used by a certification service provider for the provision of electronic signature services or are intended to be used for the creation or verification of electronic signatures;

"forge a digital signature" means—

(a) to create a digital signature without the authorisation of the rightful holder of the private key; or

(b) to create a digital signature verifiable by a certificate listing as subscriber a person who either does not exist or does not hold the private key corresponding to the public key listed in the certificate;

"hold a private key" means to be able to utilise a private key;

"incorporate by reference" means to make one message a part of another message by identifying the message to be incorporated and expressing the intention that it be incorporated;

"issue a certificate" means the act of a certification service provider in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate;

"key pair" means a private key and its corresponding public key in an asymmetric cryptosystem, where the public key can verify a digital signature that the private key creates;

"licensed certification service provider" means a certification service provider to whom a licence has been issued by the Controller and whose licence is in effect;

"message" means a digital representation of information;

"Minister" means the Minister responsible for information and communication technology;

"notify" means to communicate a fact to another person in a manner reasonably likely under the circumstances to impart knowledge of the information to the other person;

"person" includes any company or association or body of persons corporate or unincorporate;

"prescribed" means prescribed by or under this Act or any regulations made under this Act;

"private key" means the key of a key pair used to create a digital signature;

"public key" means the key of a key pair used to verify a digital signature and listed in the digital signature certificate;

"public key infrastructure" means a framework for creating a secure method for exchanging information based on public key cryptography;

"publish" means to record or file in a repository;

"qualified certification service provider" means a certification service provider that satisfies the requirements under section 23;

"recipient" means a person who receives or has a digital signature and is in a position to rely on it;

"recognised date or time stamp service" means a date/time stamp service recognised by the Controller under section 79;

"recognised repository" means a repository recognised by the Controller under section 77;

"recommended reliance limit" means the monetary amount recommended for reliance on a certificate under section 76;

"relying party" means a person that may act on the basis of a certificate or an electronic signature;

"repository" means a system for storing and retrieving certificates and other information relevant to digital signatures;

"revoke a certificate" means to make a certificate ineffective permanently from a specified time forward;

"rightfully hold a private key" means to be able to utilise a private key—

(a) which the holder or the holder's agents have not disclosed to any person in contravention of this act; and

(b) which the holder has not obtained through theft, deceit, eavesdropping or other unlawful means;

"security procedure" means a procedure for the purpose of—

(a) verifying that an electronic record is that of a specific person; or

(b) detecting error or alteration in the communication, content or storage of an electronic record since a specific point in time, which may require the use of algorithms or codes, identifying words or numbers, encryption, answer back or acknowledgement procedures or similar security devices;

"secure signature creation device" means a signature creation device which meets the requirements laid down in section 4;

"signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents

"signature creation device" means configured software or hardware, used by the signatory to create an electronic signature;

"signature verification data" means unique data such as codes or public cryptographic keys, used for the purpose of verifying an electronic signature;

"signature verification device" means configured software or hardware, used for the purpose of verifying an electronic signature;

"signed" or "signature" and its grammatical variations includes any symbol executed or adapted or any methodology or procedure employed or adapted, by a person with the intention of authenticating a record, including an electronic or digital method;

"subscriber" means a person who—

(a) is the subject listed in a certificate;

(b) accepts the certificate; and

(c) holds a private key which corresponds to a public key listed in that certificate;

"suspend a certificate" means to make a certificate ineffective temporarily for a specified time forward;

"this Act" includes any regulations made under this Act;

"time-stamp" means—

(a) to append or attach to a message, digital signature or certificate a digitally signed notation indicating at least the date, time and identity of the person appending or attaching the notation; or

(b) the notation appended or attached;

"transactional certificate" means a certificate, incorporating by reference one or more digital signatures, issued and valid for a specific transaction;

"trustworthy system" means computer hardware and software which—

(a) are reasonably secure from intrusion and misuse;

(b) provide a reasonable level of availability, reliability and correct operation; and

(c) are reasonably suited to performing their intended functions;

"valid certificate" means a certificate which—

(a) a licensed certification service provider has issued;

(b) has been accepted by the subscriber listed in it;

(c) has not been revoked or suspended; and

(d) has not expired,

but a transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference;

"verify a digital signature" means, in relation to a given digital signature, message and public key, to determine accurately that—

(a) the digital signature was created by the private key corresponding to the public key; and

(b) the message has not been altered since its digital signature was created;

"writing" or "written" includes any handwriting, typewriting, printing, electronic storage or transmission or any other method of recording information or fixing information in a form capable of being preserved.

(2) For the purposes of this Act, a certificate shall be revoked by making a notation to that effect on the certificate or by including the certificate in a set of revoked certificates.

(3) The revocation of a certificate does not mean that it is destroyed or made illegible.

3. Equal treatment of signature technologies.

Nothing in this Act shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements for a signature in this Act or otherwise meets with the requirements of any other applicable law.

4. Compliance with a requirement for a signature.

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in light of all the circumstances, including any relevant agreement.

(2) Subsection (1) applies whether the requirement referred to in that subsection in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in subsection (1) if—

(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) where a purpose of legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(4) Subsection (3) does not limit the liability of any person—

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in subsection (1),the reliability of an electronic signature; or

(b) to adduce evidence of the non-reliability of an electronic signature.

5. Conduct of the signatory.

(1) Where signature creation data can be used to create a signature that has legal effect, each signatory shall—

(a) exercise reasonable care to avoid unauthorised use of its signature creation data;

(b) without undue delay, notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if—

(i) the signatory knows that the signature creation data have been compromised; or

(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

(c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle or which are to be included in the certificate.

6. Variation by agreement.

The provisions of this Act may be derogated from or their effect may be varied by agreement unless that agreement would not be valid or effective under any law.

7. Conduct of the relying party.

A relying party shall bear the legal consequences of his or her failure to—

(a) take reasonable steps to verify the reliability of an electronic signature; or

(b) where an electronic signature is supported by a certificate, take reasonable steps—

(i) to verify the validity, suspension or revocation of the certificate; and

(ii) to observe any limitation with respect to the certificate.

8. Trustworthiness.

When determining whether or to what extent any systems procedures and human resources utilised by a certification service provider are trustworthy, regard may be had to the following factors—

(a) financial and human resources, including existence of assets;

(b) quality of hardware and software systems;

(c) procedure for processing of certificates and applications for certificates and retention of records;

(d) availability of information to signatories identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the state, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or

(g) any other relevant factor.

9. Conduct of the certification service provider.

(1) Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall—

(a) act in accordance with representations made by it with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to ascertain from the certificate—

(i) the identity of the certification service provider;

(ii) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(iii) that signature creation data were valid at or before the time when the certificate was issued;

(d) provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise—

(i) the method used to identify the signatory;

(ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(iii) that the signature creation data are valid and have not been compromised;

(iv) any limitation on the scope or extent of liability stipulated by the certification service provider;

(v) whether means exist for the signatory to give notice under section 4(1);

(vi) whether a timely revocation service is offered;

(e) where services under paragraph (d) (v) are offered, provide a means for a signatory to give notice under section 4(1)(b) and, where services under paragraph d(vi) are offered, ensure the availability of a timely revocation service;

(f) utilize trustworthy systems, procedures and human resources in performing its services.

(2) A certification service provider shall be liable for its failure to satisfy the requirements of subsection (1).

10. Advanced signatures.

(1) An advanced electronic signature, verified with a qualified certificate, is equal to an autographic signature in relation to data in electronic form and has therefore equal legal effectiveness and admissibility as evidence.

(2) The advanced signature verification process shall ensure that—

(a) the data used for verifying the electronic signature correspond to the data displayed to the verifier;

(b) the signature is reliably verified and the result of the verification and identity of the certificate holder is correctly displayed to the verifier;

(c) the verifier can reliably establish the contents of the signed data;

(d) the authenticity and validity of the certificate required at the time of signature verification are verified;

(e) the use of a pseudonym is clearly indicated;

(f) any security-relevant changes can be detected.

11. Secure electronic signature.

Where, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, an electronic signature is executed in a trustworthy manner, reasonably and in good faith relied upon by the relying party, that signature shall be treated as a secure electronic signature at the time of verification to the extent that it can be verified that the electronic signature satisfied, at the time it was made, the following criteria—

(a) the signature creation data used for signature creation is unique and its secrecy is reasonably assured;

(b) it was capable of being used to objectively identify that person;

(c) it was created in a manner or using a means under the sole control of the person using it, that cannot be readily duplicated or compromised;

(d) it is linked to the electronic record to which it relates in such a manner that if the record was changed to electronic signature would be invalidated;

(e) the signatory can reliably protect his or her signature creation data from unauthorised access.

12. Presumptions relating to secure and advanced electronic signatures.

(1) In any civil proceedings involving a secure electronic record, it shall be presumed, unless the contrary is proved, that the secure or advanced electronic record has not been altered since the specific point in time to which the secure status relates.

(2) In any civil proceedings involving a secure or advanced electronic signature, the following shall be presumed unless the contrary is proved—

(a) the secure or advanced electronic signature is the signature of the person to whom it correlates; and

(b) the secure or advanced electronic signature was affixed by that person with the intention of signing or approving the electronic record.

(3) In the absence of a secure or advanced electronic signature, nothing in this Part shall create any presumption relating to the authenticity and integrity of the electronic record or an electronic signature.

(4) The effect of presumptions provided in this section is to place on the party challenging the genuineness of a secure or advanced electronic signature both the burden of going forward with evidence to rebut the presumption and the burden of persuading the court of the fact that the non-existence of the presumed fact is more.

13. Secure digital signatures.

When a portion of an electronic record is signed with a digital signature the digital signature shall be treated as a secure electronic signature in respect of that portion of the record, if—

(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to a public key listed in the certificate; and

(b) the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity because—

(i) the certificate was issued by a certification service provider operating in compliance with regulations made under this Act;

(ii) the certificate was issued by a certification service provider outside Uganda recognised for the purpose by the Controller pursuant to regulations made under this Act;

(iii) the certificate was issued by a department or ministry of the Government, an organ of state of statutory corporation approved by the minister to act as a certification service provider on such conditions as the regulations may specify; or

(iv) the parties have expressly agreed between themselves to use digital signatures as a security procedure and the digital signature was properly verified by reference to the sender's public key.

14. Satisfaction of signature requirements.

(1) Where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that rule shall be satisfied by a digital signature where—

(a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification service provider;

(b) that digital signature was affixed by the signer with the intention of signing the message; and

(c) the recipient has no knowledge or notice that the signer—

(i) has breached a duty as a subscriber; or

(ii) does not rightfully hold the private key used to affix the digital signature.

(2) Notwithstanding any written law to the contrary—

(a) a document signed with a digital signature in accordance with this Act shall be as legally binding as a document signed with a handwritten signature, an affixed thumbprint or any other mark; and

(b) a digital signature created in accordance with this Act shall be taken to be a legally binding signature.

(3) Nothing in this Act shall preclude a symbol from being valid as a signature under any other applicable law.

15. Unreliable digital signatures.

(1) Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances.

(2) Where the recipient decides not to rely on a digital signature under this section, the recipient shall promptly notify the signer of its determination not to rely on a digital signature and the grounds for that determination.

16. Digitally signed document taken to be written document.

(1) A message shall be as valid, enforceable and effective as if it had been written on paper if—

(a) it bears in its entirety a digital signature; and

(b) that digital signature is verified by the public key listed in a certificate which—

(i) was issued by a licensed certification service provider; and

(ii) was valid at the time the digital signature was created.

(2) Nothing in this Act shall preclude any message, document or record from being considered written or in writing under any other applicable law.

17. Digitally signed document deemed to be original document.

A copy of a digitally signed message shall be as valid, enforceable and effective as the original of the message unless it is evident that the signer designated an instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, enforceable and effective message.

18. Authentication of digital signatures.

A certificate issued by a licensed certification service provider shall be an acknowledgement of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgement appear with the digital signature and regardless of whether the signer physically appeared before the licensed certification service provider when the digital signature was created, if that digital signature is—

(a) verifiable by that certificate; and

(b) was affixed when that certificate was valid.

19. Presumptions in adjudicating disputes.

In adjudicating a dispute involving a digital signature, a court shall presume—

(a) that a certificate digitally signed by a licensed certification service provider and—

(i) published in a recognised repository; or

(ii) made available by the issuing licensed certification service provider or by the subscriber listed in the certificate, is issued by the licensed certification service provider which digitally signed it and is accepted by the subscriber listed in it;

(b) that the information listed in a valid certificate and confirmed by a licensed certification service provider issuing the certificate is accurate;

(c) that where the public key verifies a digital signature listed in a valid certificate issued by a licensed certification service provider—

(i) that digital signature is the digital signature of the subscriber listed in that certificate;

(ii) that digital signature was affixed by that subscriber with the intention of signing the message; and

(iii) the recipient of that digital signature has no knowledge or notice that the signer—

(aa) has breached a duty as a subscriber; or

(ab) does not rightfully hold the private key used to affix the digital signature; and

(d) that a digital signature was created before it was time-stamped by a recognised date or time stamp service utilising a trustworthy system.

20. Sphere of application.
This Part applies to digital signatures or signatures that are able to use the public key infrastructure (PKI).

21. Controller.

(1) The Controller shall, in particular be responsible for monitoring and overseeing the activities of certification service providers and shall perform the functions conferred on the Controller under this Act.

(2) The Controller shall exercise its functions under this Act subject to such directions as to the general policy guidelines as may be given by the Minister.

(3) The Controller shall maintain a publicly accessible database containing a certification service provider disclosure record for each certification service provider, which shall contain all the particulars required under regulations made under this Act.

(4) The Controller shall publish the contents of the database in at least one recognised repository.

22. Certification service providers to be licensed.

(1) A person shall not carry on or operate or hold himself out as carrying on or operating, as a certification service provider unless that person has a valid licence issued under this Act.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both; and in the case of a continuing offence is in addition liable to a daily fine not exceeding ten currency points for each day the offence continues.

(3) The Minister may, on an application in writing being made in accordance with this Act, exempt a person operating as a certification service provider within an organisation from the requirement of a licence under this section where certificates and key pairs are issued to members of the organisation for internal use only; but the Minister shall not delegate that power to the Controller.

(4) The liability limits specified in Part IV shall not apply to an exempted certification service provider and Part V shall not apply in relation to a digital signature verified by a certificate issued by an exempted certification service provider.

23. Qualifications of certification aservice providers.

(1) The Minister in consultation with National Information Technolology Authority- Uganda shall, by regulations made under this Act, prescribe the qualifications required for certification service providers.

(2) The Minister in consultation with National Information Technolology Authority- Uganda may vary or amend the qualifications prescribed under subsection (1) but any such variation or amendment shall not be applied to a certification service provider holding a valid licence under this Act until the expiry of that licence.

24. Functions of licensed certification service providers.

(1) The function of a certification service provider shall be to issue a certificate to a subscriber upon application and upon satisfaction of the certification service providers requirements as to the identity of the subscriber to be listed in the certificate and upon payment of the prescribed fees and charges.

(2) The certification service provider shall, before issuing a certificate under this Act, take all reasonable measures to check for proper identification of the subscriber to be listed in the certificate.

25. Application for licence.

(1) An application for a licence under this Act shall be made in writing to the Controller in such form as may be prescribed.

(2) An application under subsection (1) shall be accompanied by such documents or information as may be prescribed and the Controller may, at any time after receiving the application and before it is determined, require the applicant to provide such additional documents or information as may be considered necessary by the Controller for the purposes of determining the suitability of the applicant for the licence.

(3) Where any additional document or information required under subsection (2) is not provided by the applicant within the time specified in the requirement or any extension granted by the Controller, the application shall be taken to be withdrawn and shall not be further proceeded with, without prejudice to a fresh application being made by the applicant.

26. Grant or refusal of licence.

(1) The Controller shall, on an application having been duly made in accordance with section 25 and after being provided with all the documents and information as he may require, consider the application and when he or she is satisfied that the applicant is a qualified certification service provider and a suitable licensee and upon payment of the prescribed fee, grant the licence with or without conditions or refuse to grant a licence.

(2) A licence granted under subsection (1) shall set out the duration of the licence and the licence number.

(3) The terms and conditions imposed under the licence may at any time be varied for just cause or amended by the Controller but the licensee shall be given a reasonable opportunity of being heard.

(4) The Controller shall notify the applicant in writing of his or her decision to grant or refuse to grant a licence within thirty days of receiving the application.

27. Revocation of licence.

(1) The Controller may revoke a licence granted under section 26 if satisfied that—

(a) the certification service provider has failed to comply with an obligation imposed upon it by or under this Act;

(b) the certification service provider has contravened any condition imposed under the licence, any provision of this Act or any other written law;

(c) the certification service provider has, either in connection with the application for the licence or at any time after the grant of the licence, provided the Controller with false, misleading or inaccurate information or a document or declaration made by or on behalf of the certification service provider or by or on behalf of a person who is or is to be a director, Controller or manager of the licensed certification service provider which is false, misleading or inaccurate;

(d) the certification service provider is carrying on its business in a manner which is prejudicial to the interest of the public or to the national economy;

(e) the certification service provider has insufficient assets to meet its liabilities;

(f) a winding up order has been made against the licensed certification service provider or a resolution for its voluntary winding-up has been passed;

(g) the certification service provider or its director, Controller or manager has been convicted of an offence under this Act in his or her capacity as; or

(h) the certification service provider has ceased to be a qualified certification service provider.

(2) Before revoking a licence, the Controller shall give the licensed certification service provider a notice in writing of his or her intention to revoke the licence and require the licensed certification service provider to show cause within thirty days as to why the licence should not be revoked.

(3) Where the Controller decides to revoke the licence, he or she shall notify the certification service provider of his or her decision by a notice in writing within 48 hours of making the decision.

(4) The revocation of a licence shall take effect where there is no appeal against the revocation, on the expiration of thirty days from the date on which the notice of revocation is served on the licensed certification service provider.

(5) Where an appeal has been made against the revocation of a licence, the certification service provider whose licence has been revoked shall not issue any certificates until the appeal has been disposed of and the revocation has been set aside by the Minister but nothing in this subsection shall prevent the certification service provider from fulfilling its other obligations to its subscribers during that period.

(6) A person who contravenes subsection (5) commits an offence and is liable, on conviction, to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both.

(7) Where the revocation of a licence has taken effect, the Controller shall, as soon as practicable, cause the revocation to be published in the certification service provider disclosure record he or she maintains for the certification service provider concerned and advertised in at least two English language national daily newspapers for at least three consecutive days.

28. Appeal.

(1) A person who is aggrieved by—

(a) the refusal of the Controller to license a certification service provider under section 26 or to renew a licence under section 35; or

(b) the revocation of a licence under section 27,

may appeal in writing to the Minister within thirty days from the date on which the notice of refusal or revocation is served on that person.

(2) The Minister shall, upon receipt of the appeal respond within thirty days.

(3) A person not satisfied with the Minister's decision may appeal to the High Court.

29. Surrender of licence.

(1) A certification service provider may surrender its licence by forwarding it to the Controller with a written notice of its surrender.

(2) The surrender shall take effect on the date the Controller receives the licence and the notice under subsection (1) or where a later date is specified in the notice, on that date.

(3) The licensed certification service provider shall, not later than fourteen days after the date referred to in subsection (2), cause the surrender to be published in the certification service provider disclosure record of the certification service provider concerned and advertised in at least two English language national daily newspapers for at least three days consecutive.

30. Effect of revocation, surrender or expiry of licence.

(1) Where the revocation of a licence under section 27 or its surrender under section 29 has taken effect or where the licence has expired, the licensed certification service provider shall immediately cease to carry on or operate any business in respect of which the licence was granted.

(2) Notwithstanding subsection (1), the Minister may, on the recommendation of the Controller, authorise the licensed certification service provider in writing to carry on its business for such duration as the Minister may specify in the authorisation for the purpose of winding up its affairs.

(3) Notwithstanding subsection (1), a licensed certification service provider whose licence has expired shall be entitled to carry on its business as if its licence had not expired upon proof being submitted to the Controller that the licensed certification service provider has applied for a renewal of the licence and that such application is pending determination.

(4) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding seventy two currency points or to imprisonment not exceeding ten years or both and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding five currency points for each day the offence continues.

(5) Without prejudice to the Controller's powers under section 26, the revocation of a licence under section 27 or its surrender under section 29 or its expiry shall not affect the validity or effect of any certificate issued by the certification service provider concerned before such revocation, surrender or expiry.

(6) For the purposes of subsection (5), the Controller shall appoint another licensed certification service provider to take over the certificates issued by the certification service provider whose licence has been revoked or surrendered or 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.

(7) Subsection (6) 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 Controller.

31. Effect of lack of licence.

(1) The liability limits specified in Part IV shall not apply to unlicensed certification service providers.

(2) Part V shall not apply in relation to an electronic signature, which cannot be verified by a certificate issued by a licensed certification service provider.

(3) In any other case, unless the parties expressly provide otherwise by contract between themselves, the licensing requirements under this Act shall not affect the effectiveness, enforceability or validity of any digital signature.

32. Return of licence.

(1) Where the revocation of a licence under section 27 has taken effect or where the licence has expired and no application for its renewal has been submitted within the period specified or where an application for renewal has been refused under section 35, the licensed certification service provider shall within fourteen days return the licence to the Controller.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding seventy two eight currency points or to imprisonment not exceeding three years or to both and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding five currency points for each day the offence continues and the court shall retain the licence and forward it to the Controller.

33. Restricted licence.

(1) The Controller may classify licences according to specified limitations including—

(a) maximum number of outstanding certificates;

(b) cumulative maximum of recommended reliance limits in certificates issued by the licensed certification service provider; and

(c) issuance only within a single firm or organisation.

(2) The Controller may issue licences restricted according to the limits of each classification.

(3) A licensed certification service provider that issues a certificate exceeding the restrictions of its licence commits an offence.

(4) Where a licensed certification service provider issues a certificate exceeding the restrictions of its licence, the liability limits specified in Part IV shall not apply to the licensed certification service provider in relation to that certificate.

(5) Nothing in subsection (3) or (4) shall affect the validity or effect of the issued certificate.

34. Restriction on use of expression "certification service provider".

(1) Except with the written consent of the Controller, a person shall not being a licensed certification service provider, assume or use the expressions "certification service provider" or "licensed certification service provider", as the case may be or any derivative of those expressions in any language or any other words in any language capable of being construed as indicating the carrying on or operation of such business, in relation to the business or any part of the business carried on by that person or make any representation to that effect in any bill head, letter, paper, notice, advertisement or in any other manner.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding one hundred sixty eight currency points or to imprisonment not exceeding seven years or to both.

35. Renewal of licence.

(1) A licensed certification service provider shall submit an application to the Controller in such form as may be prescribed for the renewal of its licence at least thirty days before the date of expiry of the licence and the application shall be accompanied by such documents and information as may be required by the Controller.

(2) The prescribed fee shall be payable upon approval of the application.

(3) Where a licensed certification service provider has no intention of renewing its licence, the licensed certification service provider shall, at least thirty days before the expiry of the licence, publish the intention in the certification service provider disclosure record of the certification service provider concerned and advertise such intention in at least two English language national daily newspapers for at least five consecutive days.

(4) Without prejudice to any other grounds, the Controller may refuse to renew a licence where the requirements of subsection (1) have not been complied with.

36. Lost license.

(1) Where a certification service provider has lost its license, it shall immediately notify the Controller in writing of the loss.

(2) The certification service provider shall, as soon as practicable, submit an application for a replacement license accompanied by all such information and documents as may be required by the Controller together with the prescribed fee.

37. Recognition of other licenses.

(1) The Controller may recognise, by order published in the *Gazette,* certification service providers licensed or otherwise authorised by entities outside Uganda that satisfy the prescribed requirements.

(2) Where a license or other authorisation of an entity is recognised under subsection (1)—

(a) the recommended reliance limit, if any, specified in a certificate issued by the certification service provider licensed or otherwise authorised by such an entity shall have effect in the same manner as a recommended reliance limit specified in a certificate issued by a certification service provider of Uganda; and

(b) Part IV shall apply to the certificates issued by the certification service provider licensed or otherwise authorised by such entity in the same manner as it applies to a certificate issued by a certification service provider of Uganda.

38. Performance audit.

(1) The operations of a certification service provider shall be audited a least once a year to evaluate its compliance with this Act.

(2) The audit shall be carried out by an internationally recognised computer security professional or a certified public accountant having expertise in the relevant field.

(3) The qualifications of the auditors and the procedure for an audit shall be as may be prescribed by regulations made under this Act.

(4) The Controller shall maintain and publish, the date and result of the audit in the certification service provider disclosure record he or she maintains for the certification service provider concerned.

39. Activities of certification service providers.

(1) A certification service provider shall only carry on such activities as may be specified in its license.

(2) A certification service provider shall carry on its activities in accordance with this Act and any regulations made under this Act.

40. Requirement to display license.

A certification service provider shall at all times display its license in a conspicuous place at its place of business and on its website.

41. Requirement to submit information on business operations.

(1) A licensed certification service provider shall submit to the Controller such information and particulars including financial statements, audited balance sheets and profit and loss accounts relating to its entire business operations as may be required by the Controller within the time he or she may determine.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding twenty four currency points or imprisonment not exceedingone year or both and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding two currency points for each day the offence continues.

42. Notification of change of information.

(1) A certification service provider shall, before making an amendment or alteration to any of its constituent documents or before any change in its director or chief executive officer, furnish the Controller particulars in writing of any proposed amendment, alteration or change.

(2) A licensed certification service provider shall immediately notify the Controller of any amendment or alteration to any information or document which has been furnished to the Controller in connection with the licence.

43. Use of trustworthy systems.

(1) A certification service provider shall only use a trustworthy system—

(a) to issue, suspend or revoke a certificate;

(b) to publish or give notice of the issuance, suspension or revocation of a certificate; and

(c) to create a private key, whether for itself or for a subscriber.

(2) A subscriber shall only use a trustworthy system to create a private key.

44. Disclosures on inquiry.

(1) A certification service provider shall, on an inquiry being made to it under this Act, disclose any material certification practice statement and any fact material to either the reliability of a certificate, which it has issued or its ability to perform its services.

(2) A certification service provider may require a signed, written and reasonably specific inquiry from an identified person and payment of the prescribed fee, as conditions precedent to effecting a disclosure required under subsection (1).

45. Prerequisites to issue of certificate to subscriber.

(1) A certification service provider may issue a certificate to a subscriber where the following conditions are satisfied—

(a) the certification service provider has received a request for issuance signed by the prospective subscriber; and

(b) the certification service provider has confirmed that—

(i) the prospective subscriber is the person to be listed in the certificate to be issued;

(ii) if the prospective subscriber is acting through one or more agents, the subscriber has duly authorised the agent or agents to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(iii) the information in the certificate to be issued is accurate;

(iv) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(v) the prospective subscriber holds a private key capable of creating a digital signature; and

(vi) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.

(2) The requirements of subsection (1) shall not be waived or disclaimed by the certification service provider, the subscriber or both.

46. Publication of issued and accepted certificate.

(1) Where the subscriber accepts the issued certificate, the certification service provider shall publish a signed copy of the certificate in a recognised repository, as the certification service provider and the subscriber named in the certificate may agree, unless a contract between the certification service provider and the subscriber provides otherwise.

(2) Where the subscriber does not accept the certificate, a certification service provider shall not publish it or shall cancel its publication if the certificate has already been published.

47. Adoption of more rigorous requirements permitted.
Nothing in sections 31 and 32 shall preclude a certification service provider from conforming to standards, certification practice statements, security plans or contractual requirements more rigorous than, but nevertheless consistent with, this Act.

48. Suspension or revocation of certificate for faulty issuance.
(1) Where after issuing a certificate a certification service provider confirms that it was not issued in accordance with sections 31 and 32, the certification service provider shall immediately revoke it.

(2) A certification service provider may suspend a certificate which it has issued for a reasonable period not exceeding forty-eight hours as may be necessary for an investigation to be carried out to confirm the grounds for a revocation under subsection (1).

(3) The certification service provider shall immediately notify the subscriber of a revocation or suspension under this section.

49. Suspension or revocation of certificate by order.
(1) The Controller may order the certification service provider to suspend or revoke a certificate where the Controller determines that—

(a) the certificate was issued without compliance with sections 31 and 32; and

(b) the non-compliance poses a significant risk to persons reasonably relying on the certificate.

(2) Before making a determination under subsection (1), the Controller shall give the licensed certification service provider and the subscriber a reasonable opportunity of being heard.

(3) Notwithstanding subsections (1) and (2), where in the opinion of the Controller there exists an emergency that requires an immediate remedy, the Controller may, after consultation with the Minister, suspend a certificate for a period not exceeding forty-eight hours.

50. Warranties to subscriber.

(1) By issuing a certificate, a certification service provider warrants to the subscriber named in the certificate that—

(a) the certificate contains no information known to the certification service provider to be false;

(b) the certificate satisfies all the requirements of this Act; and

(c) the certification service provider has not exceeded any limits of its licence in issuing the certificate.

(2) A certification service provider shall not disclaim or limit the warranties under subsection (1).

51. Continuing obligations to subscriber.

Unless the subscriber and certification service provider otherwise agree, a certification service provider, by issuing a certificate, promises to the subscriber—

(a) to act promptly to suspend or revoke a certificate in accordance with Part IV; and

(b) to notify the subscriber within a reasonable time of any facts known to the licensed certification service provider, which significantly affect the validity or reliability of the certificate once it is issued.

52. Representations upon issuance.

By issuing a certificate, a certification service provider certifies to all who reasonably rely on the information contained in the certificate that—

(a) the information in the certificate and listed as confirmed by the licensed certification service provider is accurate;

(b) all information foreseeable and material to the reliability of the certificate is stated or incorporated by reference within the certificate;

(c) the subscriber has accepted the certificate; and

(d) the certification service provider has complied with all applicable laws governing the issue of the certificate.

52. Representations upon publication.
By publishing a certificate, a certification service provider certifies to the repository in which the certificate is published and to all who reasonably rely on the information contained in the certificate that the licensed certification service provider has issued the certificate to the subscriber.

54. Implied representations by subscriber.
By accepting a certificate issued by a certification service provider, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that—

(a) the subscriber rightfully holds 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 material to information listed in the certificate are true; and

(c) all material representations made by the subscriber to a certification service provider or made in the certificate and not confirmed by the certification service provider in issuing the certificate are true.

55. Representations by agent of subscriber.
By requesting on behalf of a principal the issue of a certificate naming the principal as subscriber, the requesting person certifies in that person's own right to all who reasonably rely on the information contained in the certificate that the requesting person—

(a) holds all authority legally required to apply for issuance of a certificate naming the principal as subscriber; and

(b) has authority to sign digitally on behalf of the principal, and, if that authority is limited in any way, adequate safeguards exist to prevent a digital signature exceeding the bounds of the person's authority.

56. Disclaimer or indemnity limited.

A person shall not disclaim or contractually limit the application of this part, nor obtain indemnity for its effects, if the disclaimer, limitation or indemnity restricts liability for misrepresentation as against persons reasonably relying on the certificate.

57. Indemnification of certification service provider by subscriber.

(1) By accepting a certificate, a subscriber undertakes to indemnify the issuing licensed certification service provider for any loss or damage caused by issue or publication of the certificate in reliance on—

(a) a false and material representation of fact by the subscriber; or

(b) the failure by the subscriber to disclose a material fact, if the representation or failure to disclose was made either with intent to deceive the certification service provider or a person relying on the certificate or with negligence.

(2) Where the certification service provider issued the certificate at the request of one or more agents of the subscriber, the agent or agents personally undertake to indemnify the certification service provider under this section, as if they were accepting subscribers in their own right.

(3) The indemnity provided in this section shall not be disclaimed or contractually limited in scope.

58. Certification of accuracy of information given.

When obtaining information from a subscriber which is material to the issue of a certificate, the certification service provider may require the subscriber to certify the accuracy of the relevant information under oath or affirmation.

59. Duty of subscriber to keep private key secure.

By accepting a certificate issued by a certification service provider, the subscriber named in the certificate assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorised to create the subscriber's digital signature.

60. Property in private key.

A private key is the personal property of the subscriber who rightfully holds it.

61. Fiduciary duty of a certification service provider.

Where a certification service provider holds the private key corresponding to a public key listed in a certificate which it has issued, the certification service provider shall hold the private key as a fiduciary of the subscriber named in the certificate and may use that private key only with the subscriber's prior written approval, unless the subscriber expressly and in writing grants the private key to the licensed certification service provider and expressly and in writing permits the licensed certification service provider to hold the private key according to other terms.

62. Suspension of certificate by certification service provider.

(1) Unless the certification service provider and the subscriber agree otherwise, the licensed certification service provider, which issued a certificate, which is not a transactional certificate, shall suspend the certificate for a period not exceeding forty-eight hours—

(a) upon request by a person identifying himself as the subscriber named in the certificate or as a person in a position likely to know of a compromise of the security of a subscriber's private key, such as an agent, business associate, employee or member of the immediate family of the subscriber; or

(b) by order of the Controller under section 35.

(2) The certification service provider shall take reasonable measures to check the identity or agency of the person requesting suspension.

63. Suspension of certificate by Controller.

(1) Unless the certificate provides otherwise or the certificate is a transactional certificate, the Controller may suspend a certificate issued by a certification service provider for a period of forty-eight hours, if—

(a) a person identifying himself or herself as the subscriber named in the certificate or as an agent, business associate, employee or member of the immediate family of the subscriber requests suspension; and

(b) the requester represents that the certification service provider, which issued the certificate, is unavailable.

(2) The Controller may require the person requesting suspension to provide evidence, including a statement under oath or affirmation regarding his or her identity and authorisation and the unavailability of the issuing licensed certification service provider and may decline to suspend the certificate in his or her discretion.

(3) The Controller or other law enforcement agency may investigate suspensions by the Controller for possible wrongdoing by persons requesting suspension.

64. Notice of suspension.

(1) Upon suspension of a certificate by a certification service provider, the certification service provider shall publish a signed notice of the suspension in the repository specified in the certificate for publication of notice of suspension.

(2) Where one or more repositories are specified, the certification service provider shall publish signed notices of the suspension in all those repositories.

(3) Where any repository specified no longer exists or refuses to accept publication or if no such repository is recognised under section 69 the certification service provider shall also publish the notice in a recognised repository.

(4) Where a certificate is suspended by the Controller, the Controller shall give notice as required in this section for a certification service provider if the person requesting suspension pays in advance any prescribed fee required by a repository for publication of the notice of suspension.

65. Termination of suspension initiated by request.
A certification service provider shall terminate a suspension initiated by request—

(a) where the subscriber named in the suspended certificate requests termination of the suspension, only if the certification service provider has confirmed that the person requesting suspension is the subscriber or an agent of the subscriber authorised to terminate the suspension; or

(b) where the licensed certification service provider discovers and confirms that the request for the suspension was made without authorisation by the subscriber.

66. Alternate contractual procedures.
(1) The contract between a subscriber and a licensed certification service provider may limit or preclude requested suspension by the certification service provider or may provide otherwise for termination of a requested suspension.

(2) Where the contract limits or precludes suspension by the Controller when the issuing licensed certification service provider is unavailable, the limitation or preclusion shall be effective only if notice of it is published in the certificate.

67. Effect of suspension of certificate.
Nothing in this Part shall release the subscriber from the duty under section 47 to keep the private key secure while a certificate is suspended.

68. Revocation on request.
(1) A licensed certification service provider shall revoke a certificate, which it issued but which is not a transactional certificate—

(a) upon receiving a request for revocation by the subscriber named in the certificate; and

(b) upon confirming that the person requesting revocation is that subscriber or is an agent of that subscriber with authority to request the revocation.

(2) A certification service provider shall confirm a request for revocation and revoke a certificate within one business day after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity of the person requesting the revocation or of the agent.

69. Revocation on subscriber's demise.

A licensed certification service provider shall revoke a certificate which it issued—

(a) upon receiving a certified copy of the subscriber's death certificate or upon confirming by other evidence that the subscriber is dead; or

(b) upon presentation of documents effecting a dissolution of the subscriber or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.

70. Revocation of unreliable certificates.

(1) A licensed certification service provider may revoke one or more certificates, which it issued if the certificates are or become unreliable regardless of whether the subscriber consents to the revocation and notwithstanding any provision to the contrary in a contract between the subscriber and the licensed certification service provider.

(2) Nothing in subsection (1) shall prevent the subscriber from seeking damages or other relief against the licensed certification service provider in the event of wrongful revocation.

71. Notice of revocation.

(1) Upon revocation of a certificate by a licensed certification service provider, the licensed certification service provider shall publish a signed notice of the revocation in the repository specified in the certificate for publication of notice of revocation.

(2) Where one or more repositories are specified, the licensed certification service provider shall publish signed notices of the revocation in all such repositories.

(3) Where any repository specified no longer exists or refuses to accept publication or if no such repository is recognised under section 69, the licensed certification service provider shall also publish the notice in a recognised repository.

72. Effect of revocation request on subscriber.

Where a subscriber has requested for the revocation of a certificate, the subscriber ceases to certify as provided in Part IV and has no further duty to keep the private key secure as required under section 59—

(a) when notice of the revocation is published as required under section 71; or

(b) where forty eight hours have lapsed after the subscriber requests for the revocation in writing, supplies to the issuing licensed certification service provider information reasonably sufficient to confirm the request and pays any prescribed fee, whichever occurs first.

73. Effect of notification on certification service provider.

Upon notification as required under section 71, a certification service provider shall be discharged of its warranties based on issue of the revoked certificate and ceases to certify as provided in sections 22 and 24 in relation to the revoked certificate.

74. Expiration of certificate.

(1) The date of expiry of a certificate shall be specified in the certificate.

(2) A certificate may be issued for a period not exceeding three years from the date of issue.

(3) When a certificate expires, the subscriber and licensed certification service provider shall cease to certify as provided under this Act and the licensed certification service provider shall be discharged of its duties based on issue in relation to the expired certificate.

(4) The expiry of a certificate shall not affect the duties and obligations of the subscriber and licensed certification service provider incurred under and in relation to the expired certificate.

75. Reliance limit.

(1) A licensed certification service provider shall, when issuing a certificate to a subscriber, specify a recommended reliance limit in the certificate.

(2) The licensed certification service provider may specify different limits in different certificates as it considers fit.

76. Liability limits for certification service providers.

Unless a licensed certification service provider waives the application of this section, a licensed certification service provider—

(a) shall not be liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the licensed certification service provider complied with the requirements of this Act;

(b) shall not be liable in excess of the amount specified in the certificate as its recommended reliance limit for either—

(i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification service provider is required to confirm; or

(ii) failure to comply with sections 31 and 32 when issuing the certificate.

77. Recognition of repositories.

(1) The Controller may recognise one or more repositories, after determining that a repository to be recognised satisfies the requirements prescribed in the regulations made under this Act.

(2) The procedure for recognition of repositories shall be as prescribed by regulations made under this Act.

(3) The Controller shall publish a list of recognised repositories in such form and manner as he or she may determine.

78. Liability of repositories.

(1) Notwithstanding any disclaimer by the repository or a contract to the contrary between the repository and a licensed certification service provider or a subscriber, a repository shall be liable for a loss incurred by a person reasonably relying on an electronic signature verified by the public key listed in a suspended or revoked certificate, if loss was incurred more than one business day after receipt by the repository of a request to publish notice of the suspension or revocation and the repository had failed to publish the notice when the person relied on the digital signature.

(2) Unless waived, a recognised repository or the owner or operator of a recognised repository—

(a) shall not be liable for failure to record publication of a suspension or revocation, unless the repository has received notice of publication and one business day has elapsed since the notice was received;

(b) shall not be liable under subsection (1) in excess of the amount specified in the certificate as the recommended reliance limit;

(c) shall not be liable for misrepresentation in a certificate published by a certification service provider;

(d) shall not be liable for accurately recording or reporting information which a licensed certification service provider, a court or the Controller has published as required or permitted under this Act, including information about the suspension or revocation of a certificate; and

(e) shall not be liable for reporting information about a certification service provider, a certificate or a subscriber, if the information is published as required or permitted under this Act or is published by order of the Controller in the performance of his or her licensing and regulatory duties under this Act.

79. Recognition of date or time stamp services.

(1) The Controller may recognise one or more date or time stamp services, after determining that a service to be recognised satisfies the requirements prescribed in the regulations made under this Act.

(2) The procedure for recognising of date or time stamp services shall be as may be prescribed by regulations made under this Act.

(3) The Controller shall publish a list of recognised date or time stamp services in a form and manner as he may determine.

Part V—Miscellaneous

80. Prohibition against dangerous activities

(1) A certification service provider, whether licensed or not, shall not conduct its business in a manner that creates an unreasonable risk of loss to the subscribers of the certification service provider, to persons relying on certificates issued by the certification service provider or to a repository.

(2) The Controller may publish in one or more recognised repositories brief statements advising subscribers, persons relying on digital signatures and repositories about any activities of a certification service provider, whether licensed or not, which create a risk prohibited under subsection (1).

(3) The certification service provider named in a statement as creating or causing a risk may protest the publication of the statement by filing a brief written defence.

(4) On receipt of a protest made under subsection (3), the Controller shall publish a written defence together with the Controller's statement and shall immediately give the protesting certification service provider notice and a reasonable opportunity of being heard.

(5) Where, after a hearing, the Controller determines that the publication of the advisory statement was unwarranted, the Controller shall revoke the advisory statement.

(6) Where, after a hearing, the Controller determines that the advisory statement is no longer warranted, the Controller shall revoke the advisory statement.

(7) Where, after a hearing, the Controller determines that the advisory statement remains warranted, the Controller may continue or amend the advisory statement and may take further legal action to eliminate or reduce the risk prohibited under subsection (1).

(8) The Controller shall publish his decision under subsection (5), (6) or (7), as the case may be, in one or more recognised repositories.

81. Obligation of confidentiality

(1) Except for the purpose of this Act or for any prosecution for an offence under any written law or under an order of court, a person under any powers conferred under this Act, shall not obtain access to any electronic record, book, register, correspondence, information, document, other material or grant access to any other person.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding one hundred twenty currency points or imprisonment for a term not exceeding five years or both.

82. False information.

A person who knowingly makes, orally or in writing, signs or furnishes any declaration, return, certificate or other document or information required under this Act which is false or misleading in any particular way commits an offence and is liable, on conviction, to a fine not exceeding one hundred and twenty currency points or imprisonment for a term not exceeding five years or both.

83. Offences by body corporate.

(1) Where a body corporate commits an offence under this Act, a person who at the time of the commission of the offence is a director, manager, secretary or other similar officer of the body corporate or was purporting to act in that capacity or was in any manner or to any extent responsible for the management of any of the affairs of the body corporate or was assisting in such management—

(a) may be charged severally or jointly in the same proceedings with the body corporate; and

(b) where the body corporate is convicted of the offence, such a person shall be deemed to have committed an offence unless, having regard to the nature of his functions in that capacity and to all circumstances, he proves—

(i) that the offence was committed without his knowledge, consent or connivance; and

(ii) that he took all reasonable precautions and had exercised due diligence to prevent the commission of the offence.

(2) Where a person is liable under this Act to a punishment or penalty for any act, omission, neglect or default, he or she is liable to the same punishment or penalty for every such act, omission, neglect or default of any employee or agent of his or of the employee of such agent, if the act, omission, neglect or default was committed—

(a) by his employee in the course of his employment;

(b) by the agent when acting on his behalf; or

(c) by the employee of such agent in the course of his employment by such agent or otherwise on behalf of the agent.

84. Authorised officer.

An authorised officer may exercise the powers of enforcement under this Act.

85. Power to investigate.

(1) The Controller may investigate the activities of a certification service provider material to its compliance with this Act.

(2) For the purposes of subsection (1), the Controller may issue orders to a certification service provider to further its investigation and secure compliance with this Act.

(3) Further, in any case relating to the commission of an offence under this Act, any authorised officer carrying on an investigation may exercise all or any of the special powers in relation to police investigation in all cases given by the Criminal Procedure Code.

86. Search by warrant.

(1) If it appears to a Magistrate, upon written information on oath and after such inquiry as he or she considers necessary, that there is reasonable cause to believe that an offence under this Act is being or has been committed on any premises, the Magistrate may issue a warrant authorising any police officer not below the rank of Inspector or any authorised officer named in the warrant, to enter the premises at any reasonable time by day or by night, with or without assistance and if need be by force, to search for and seize—

(a) copies of any books, accounts or other documents, including computerized data, which contain or are reasonably suspected to contain information as to any offence so suspected to have been committed;

(b) any signboard, card, letter, pamphlet, leaflet, notice or other device representing or implying that the person is a licensed certification service provider; and

(c) any other document, article or item that is reasonably believed to furnish evidence of the commission of that offence.

(2) A police officer or an authorised officer conducting a search under subsection (1) may, if in his or her opinion it is reasonably necessary to do so for the purpose of investigating into the offence, search any person who is in or on those premises.

(3) A police officer or an authorised officer making a search of a person under subsection (2) may seize, detain or take possession of any book, accounts, document, computerised data, card, letter, pamphlet, leaflet, notice, device, article or item found on that person for the purpose of the investigation being carried out by that officer.

(4) A female person shall not be searched under this section except by another female person.

(5) Where, by reason of its nature, size or amount, it is not practicable to remove any book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item seized under this section, the seizing officer shall, by any means, seal that book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item in the premises or container in which it is found.

(6) A person who, without lawful authority, breaks, tampers with or damages the seal referred to in subsection (5) or removes any book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item under seal or attempts to do so commits an offence.

87. Search and seizure without warrant.

If a police officer not below the rank of Inspector in any of the circumstances referred to in section 86 has reasonable cause to believe that by reason of delay in obtaining a search warrant under that section the investigation would be adversely affected or evidence of the commission of an offence is likely to be tampered with, removed, damaged or destroyed, that officer may enter the premises and exercise in, upon and in respect of the premises all the powers referred to in section 86 in as full and ample a manner as if he or she were authorised to do so by a warrant issued under that section.

88. Access to computerised data.

(1) A police officer conducting a search under section 86 or 87 shall be given unlimited access to computerised data whether stored in a computer or otherwise.

(2) For the purposes of this section, "access" includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of computerised data.

89. List of things seized.

(1) Except as provided in subsection (2), where any book, accounts, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, device, article or item is seized under section 86 or 87, the seizing officer shall prepare a list of the things seized and immediately deliver a copy of the list signed by him or her to the occupier of the premises which have been searched or to his or her agent or servant, at those premises.

(2) Where the premises are unoccupied, the seizing officer shall post a list of things seized conspicuously on the premises and leave a copy with the local authorities.

90. Obstruction of authorised officer.

A person who obstructs, impedes, assaults or interferes in any way with any authorised officer in the performance of his functions under this Act commits an offence.

91. Additional powers.

An authorised officer may, for the purposes of the execution of this Act, to do all or any of the following—

(a) require the production of records, accounts, computerised data and documents kept by a licensed certification service provider and to inspect, examine and copy any of them;

(b) require the production of any identification document from a person in relation to any case or offence under this Act;

(c) make such inquiry as may be necessary to ascertain whether the provisions of this Act have been complied with.

92. General penalty.

(1) A person who commits an offence under this Act for which no penalty is expressly provided is liable, on conviction, to a fine not exceeding seventy two currency points or to imprisonment for a term not exceeding three years or both and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding two currency points for each day the offence continues.

(2) For the purposes of this section, "this Act" does not include the regulations made under this Act.

93. Institution and conduct of prosecution.

(1) A prosecution under this Act shall not be instituted except by or with the consent of the Director of Public Prosecution, but a person charged with such an offence may be arrested or a warrant for his or her arrest issued and executed and the person may be detained or released on police bond, not withstanding that the consent of the Director of Public Prosecution to the institution of a prosecution for the offence has not yet been obtained, but no further or other proceedings shall be taken until that consent has been obtained.

(2) An officer of the Controller duly authorised in writing by the Director of Public Prosecutions may conduct the prosecution for any offence under this Act.

94. Jurisdiction to try offences.

Notwithstanding any written law to the contrary, a Magistrate Grade I shall have jurisdiction to try an offence under this Act and to impose the full punishment for the offence.

95. Protection of officers.

An action or prosecution shall not be brought, instituted or maintained in a court against the Controller or any officer duly authorised under this Act for or on account of or in respect of any act ordered or done for the purpose of carrying into effect this Act.

96. Limitation on disclaiming or limiting application of Act.

Unless it is expressly provided for under this Act, a person shall not disclaim or contractually limit the application of this Act.

97. Regulations.

(1) The Minister may on the recommendation of the Controller make regulations for all or any of the following purposes—

(a) prescribing the qualification requirements for certification service providers;

(b) prescribing the manner of applying for licences and certificates under this Act, the particulars to be supplied by an applicant, the manner of licensing and certification, the fees payable there for, the conditions or restrictions to be imposed and the form of licences and certificates;

(c) regulating the operations of licensed certification service provider;

(d) prescribing the requirements for the content, form and sources of information in certification service provider disclosure records, the updating and timeliness of such information and other practices and policies relating to certification service provider disclosure records;

(e) prescribing the form of certification practice statements;

(f) prescribing the qualification requirements for auditors and the procedure for audits;

(g) prescribing the requirements for repositories and the procedure for recognition of repositories;

(h) prescribing the requirements for date and time stamp services and the procedure for recognition of date and time stamp services;

(i) prescribing the procedure for the review of software for use in creating digital signatures and of the applicable standards in relation to digital signatures and certification practice and for the publication of reports on such software and standards;

(j) prescribing the forms for the purposes of this Act;

(k) prescribing the fees and charges payable under this Act and the manner for collecting and disbursing the fees and charges;

(l) providing for such other matters as are contemplated by or necessary for giving full effect to, the provisions of this Act and for their due administration.

(2) Regulations made under subsection (1) may prescribe any act in contravention of the regulations to be an offence and may prescribe in relation to the offence, penalties not exceeding a fine of seventy two currency points or imprisonment for three years or both.

98. Compensation.

Where a person is convicted under this Act, the court shall in addition to the punishment provided therein, order such person to pay by way of compensation to the aggrieved party, such sum as is in the opinion of the court just, having regard to the loss suffered by the aggrieved party; and such order shall be a decree under the provisions of the Civil Procedure Act, and shall be executed in the manner provided under that Act.

99. Power of Minister to amend the Schedule.

The Minister may, with the approval of Cabinet, by statutory instrument, amend the Schedule to this Act.

100. Savings and transitional provisions.

(1) A certification service provider that has been carrying on or operating as a certification service provider before the commencement of this Act shall, not later than three months from the commencement, obtain a licence under this Act.

(2) Where a certification service provider referred to in subsection (1) fails to obtain a licence after the period prescribed in subsection (1), it shall be taken to be an unlicensed certification service provider and the provisions of this Act shall apply to it and a certificate issued by it accordingly.

(3) Where a certification service provider referred to in subsection (1) has obtained a licence in accordance with this Act within the period prescribed in subsection (1), all certificates issued by that certification service provider before the commencement of this Act, to the extent that they are not inconsistent with this Act, shall be taken to have been issued under this Act and shall have effect accordingly.

SCHEDULE

Section 2

CURRENCY POINT

One currency point is equivalent to twenty thousand shillings.