THE EAST AFRICAN COMMUNITY

BILL SUPPLEMENT

No. 8 ***7th November, 2014.***

to the East African Community Gazette No. 17 of 7th November, 2014.

Printed by the Uganda Printing and Publishing Corporation, Entebbe, by Order of the East African Community.

THE EAST AFRICAN COMMUNITY

THE EAST AFRICAN COMMUNITY ELECTRONIC TRANSACTIONS BILL, 2014.

MEMORANDUM

The object of this Bill is to make provision for the use, security, facilitation and regulation of electronic communications and transactions; to encourage the use or e-Government service and to provide for related matters.

This Bill is premised on Article 103 of the Treaty for the Establishment of the East African Community, in which the Partner States, recognizing the fundamental importance of science and technology in economic development, undertook to promote cooperation in the development of science and technology in the Community through inter-alia, the promotion, development and application of information technology and new ones throughout the Community.

The Partner States therefore need to create a proper environment for all possible users and beneficiaries of ICT to educate them on the operations involving electronic transactions and in doing so, make necessary

amends to ensure security of users of ICT. It has been established that the Community needs to maximally exploit the great resource of ICTs resources, by ensuring that the businesses and institutions have access to these modern technologies.

It is on the basis of this background therefore that this Bill seeks to meet the need of exploiting electronic transactions in the modern business transactions that have become common.

The Bill creates facilitation of electronic transactions, e-Government services and the extent of liability of service providers.

HON. DR JAMES NDAHIRO,
Member, East African Legislative Assembly.

THE EAST AFRICAN COMMUNITY ELECTRONIC TRANSACTIONS BILL, 2014.

ARRANGEMENT OF CLAUSES.

PART I—PRELIMINARY

Clause.

PART II—FACILITATING ELECTRONIC TRANSACTIONS.

PART III—ELECTRONIC SIGNATURES.

THE EAST AFRICAN COMMUNITY ELECTRONIC TRANSACTIONS BILL, 2014

A Bill for an Act

ENTITLED

THE EAST AFRICAN COMMUNITY ELECTRONIC TRANSACTIONS ACT, 2014

An Act of the Community to provide for the use, security, facilitation and regulation of electronic transactions; to encourage the use of e-Government services and to provide for other related matters.

ENACTED by the East African Community and assented to by the Heads of State.

PART I—PRELIMINARY

Short title.

1. This Act may be cited as the East African Community Electronic Transactions Act, 2014 and shall come into force on such a date as the Council may, by notice published in the Gazette appoint.

Inter-pretation.

2. In this Act, unless the context otherwise requires—

"addressee", in respect of a data message, means a person who is intended by the person originating the data message to receive the data message, but not a person acting as an intermediary in respect of the data message;

"automated transaction" means an electronic transaction conducted or performed, in whole or in part, by means of a data message in which the conduct or data messages of one or both parties is not reviewed by a natural person in the ordinary course of the natural person's business or employment;

"consumer" means a natural person who enters or intends to enter into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

"Council" means the Council of Ministers established by Article 9 of the Treaty;

"data" means electronic representations of information in any form;

"data message" means data generated, sent, received or stored by electronic means and includes—

(a) a voice, where the voice is used in an automated transaction; and

(b) a stored record;

"data subject" means a natural person from whom or in respect of whom personal information has been requested, collected, collated, processed or stored;

"e-Government service" includes a public service provided by electronic means by a public body in a Partner State;

"electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction;

"electronic communication" means a communication by means of a data message;

"electronic record" means data which is recorded or stored on any medium, in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device, including a display, printout or other output of that data;

"electronic records system" includes the computer system or other similar device by or in which data is recorded or stored and the procedure for recording and storing electronic records;

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

"electronic transaction" includes the sale or purchase of goods or services whether between businesses, individuals or governments and other public or private organisations, conducted over computer mediated networks whether the payment or delivery of the goods or services is made on or off line;

"information" includes data, text, image, sound, code, computer programme, software and database;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages;

"information system services" means providing information system connections, operating facilities for information systems, providing access to information systems, transmitting or routing data messages between or among points specified by a user, and processing and storing of data at the request of the recipient of the service;

"intermediary" means a person who, on behalf of another person, whether as agent or otherwise, sends, receives or stores a particular data message or provides other services with respect to that data message;

"Minister" means the Minister responsible for information and communications technology in a Partner State;

"originator" means a person by whom or on whose behalf, a data message is sent or generated prior to storage, other than a person acting as an intermediary in respect of that data message;

"Partner States" means the partner states of the Community provided for under Article 3 of the Treaty;

"person" includes a public body;

"public body" includes a government, a department, service or undertaking of a government, a parliament, a court, a local government administration or a local council and any committee or commission, an urban authority, a municipal council and any committee of any such council, any corporation, committee, board, commission or similar body whether corporate or incorporate established by an Act of Parliament relating to undertakings of public services or such purpose for

the benefit of the public or any section of the public to administer funds or property belonging to or granted by a government or money raised by public subscription, rates, taxes, cess or charges in pursuance of any written law and any council, board, committee or society established by an Act of Parliament for the benefit, regulation and control of any profession;

"service provider" means a certification authority which certifies public keys that are used in electronic transactions in order to guarantee the relationship between the identity and the public key;

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

"signature" includes any symbol, executed or adopted, or any methodology or procedure employed or adopted by a person with the intention of authenticating a record, including electronic or digital methods;

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

"technology neutrality" means the freedom of an individual or organisation to choose the most appropriate and suitable technology to the needs and requirements for development, acquisition, use or commercialisation without dependencies on knowledge involved as information or data;

"third party" in relation to a service provider, means a subscriber to a service provided by the service provider or any other user of the service provider's services or a user of information systems;

"transaction" includes a transaction of a commercial or non commercial nature, including providing information and e-Government services; and

"Treaty" means the Treaty for the Establishment of the East African Community.

Application.

3. (1) This Act does not apply to a—

(a) will or codicil;

(b) trust created by a will or a codicil;

(c) power of attorney;

(d) document that creates or transfers an interest in property and requires registration to be effective against third parties; and

(e) negotiable instrument, including negotiable documents of title.

(2) The Council may by statutory instrument, amend subsection (1).

(3) This Act shall not limit the operation of a law which expressly authorises, prohibits or regulates the use of electronic documents.

Object of the Act.

4. (1) The object of this Act is to provide a legal and regulatory framework to—

(a) enable and facilitate electronic communication and transactions;

(b) address the legal and operational barriers to electronic transactions;

(c) promote technology neutrality in applying legislation to electronic communications and transactions;

(d) provide legal certainty and public confidence in the use of electronic communications and transactions;

(e) promote e-Government services through electronic communications and transactions with the Government, public and statutory bodies;

(f) ensure that electronic transactions in the Community conform to the best practices by international standards;

(g) encourage investment and innovation in information communications and technology to promote electronic transactions;

(h) develops a safe, secure and effective environment for the consumer, business and the governments of the Partner States to conduct and use electronic transactions;

(i) promote the development of electronic transactions that are responsive to the needs of users and consumers;

(j) promote public confidence in the integrity and reliability of electronic records, electronic signatures and electronic commerce;

(k) reduce the cost of doing business in the Community; and

(l) foster economic and social prosperity in the Community through the information communication technology sector.

PART II—FACILITATING ELECTRONIC SIGNATURES.

Legal effect of electronic records.

5. (1) Information shall not be denied legal effect, validity or enforcement solely on the ground that it is wholly or partly in the form of an electronic record.

(2) Information incorporated into a contract that is not in the public domain is regarded as having been incorporated into a data message if the information is—

(a) referred to in a way that a reasonable person would have noticed the reference to the information or incorporation in the contract; and

(b) accessible in a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout, provided the information is reasonably capable of being reduced into electronic form by the party incorporating it.

(3) Where—

(a) an act;

(b) a document; or

(c) information,

is required to be in writing, produced, recorded or retained, it may be written, produced, recorded or retained in electronic form.

(4) For purposes of subsection (3) the requirement for a document or information to be in writing is fulfilled if the document or information is—

(a) in the form of a data message; and

(b) accessible in a manner which is usable for subsequent reference.

Use of electronic signature.

6. Where a law requires a signature or provides for consequences where a document is not signed, the requirement is fulfilled if an electronic signature is used.

Authenticity of data message.

7. (1) Where a law requires information to be presented or retained in its original form, the requirement is fulfilled by a data message if—

(a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

(b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1(a), the authenticity of a data message shall be assessed—

(a) by considering whether the information has remained complete and unaltered, except for the addition of an endorsement and any change which arises in the normal course of communication, storage or display;

(b) in light of the purpose for which the information was generated; and

(c) having regard to all other relevant circumstances.

Admissibility in evidence of a data message and an electronic record.

8. (1) In legal proceedings, the rules of evidence shall not be applied so as to deny the admissibility of a data message or an electronic record—

(a) merely on the ground that it is constituted by a data message or an electronic record;

(b) if it is the best evidence that the person adducing the evidence could reasonably be expected to obtain; or

(c) merely on the ground that it is not in its original form.

(2) A person seeking to introduce a data message or an electronic record in legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

(3) Subject to subsection (2), where the best evidence rule is applicable in respect of an electronic record, the rule is fulfilled upon proof of the authenticity of the electronic records system in or by which the data was recorded or stored.

(4) When assessing the evidential weight of a data message or an electronic record, the court shall have regard to—

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the authenticity of the data message was maintained;

(c) the manner in which the originator of the data message or electronic record was identified; and

(d) any other relevant factor.

(5) The authenticity of the electronic records system in which an electronic record is recorded or stored shall, in the absence of evidence to the contrary, be presumed where—

(a) there is evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record and there are no other reasonable grounds to doubt the integrity of the electronic records system;

(b) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

(6) For the purposes of determining whether an electronic record is admissible under this section, evidence may be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or stored, with regard to the type of business or endeavours that used, recorded or stored the electronic record and the nature and purpose of the electronic record.

(7) This section does not modify the common law or a statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.

Retention of information or record.

9. (1) Where a law in a Partner State requires that a document, record or information be retained, the requirement is fulfilled by retaining the document, record or information in electronic form if—

(a) the information contained in the electronic record remains accessible and can be used for subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to accurately represent the information originally generated, sent or received;

(c) the information which is retained enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received; and

(d) the consent of the department or ministry of the Government, or the statutory corporation, which has supervision over the requirement for retaining the record, has been obtained.

(2) The obligation to retain a document, record or information in accordance with subsection (1) (c) shall not extend to information generated solely for the purpose of enabling a document, record or information to be sent or received.

(3) Subsection (1) may be fulfilled by using the services of a person other than the person who originated the document, record or information.

(4) Nothing in this section shall—

(a) affect a law which expressly provides for the retention of documents, records or information in the form of electronic records;

(b) preclude a department or ministry of a Government or a statutory corporation from specifying additional requirements for retaining electronic records that are subject to the jurisdiction of the department or ministry of the Government, or statutory corporation.

Production of document or information.

10. (1) For purposes of section 5(3), a requirement to produce a document or information is fulfilled if a person produces the document or information in electronic form if—

(a) considering all the relevant circumstances at the time the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and

(b) at the time the data message was sent, it was reasonable to expect that the information contained in the data message would be readily accessible so as to be usable for subsequent reference.

(2) For the purposes of subsection (1), the authenticity of the information contained in a document is maintained if the information has remained complete and unaltered, except for—

(a) the addition of an endorsement; or

(b) an immaterial change, which arises in the normal course of communication, storage or display.

Notarisation, acknowledgement and certification

11. (1) A requirement for a signature, statement or document to be notarised, acknowledged, verified or made under oath, is fulfilled if an advanced or secure electronic signature of a person authorised by law to sign or notarise the document is attached, incorporated or is logically associated with the electronic record.

(2) Where a person is required or permitted to provide a certified copy of a document which is in electronic form, the requirement is fulfilled if the person provides a printout certified to be a true copy of the document or information.

(3) Where a person is required or permitted to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is fulfilled if an electronic copy of the document is certified to be a true copy of the document and the certification is confirmed with an advanced electronic signature.

Other requirements.

12. (1) A requirement for multiple copies of a document to be submitted to a person at the same time is fulfilled by submitting a single data message which is capable of being reproduced by the person to whom the data message is submitted.

(2) Where a document is required to be sealed and the law does not prescribe the method or form in which it is to be the sealed, the document may be sealed by electronic means.

(3) For purposes of subsection (2) a document is sealed by electronic means if the document includes the advanced electronic signature of the person authorised to seal the document.

(4) Where a person is required or permitted to send a document or information by registered or certified mail, that requirement is fulfilled if an electronic copy of the document or information is sent to an authorised service provider and the document, is registered by the service provider and sent to the electronic address provided by the sender.

Automated transactions.

13. (1) In an automated transaction—

(a) a contract may be formed where an electronic agent performs an action required by law in order to form a contract; or

(b) a contract may be formed by a party to the transaction using an electronic agent to enter into the contract.

(2) A party using an electronic agent to enter into a contract shall, subject to subsection (3), be bound by the terms of the contract irrespective of whether the party reviewed the actions of the electronic agent or the terms of the contract.

(3) A party interacting with an electronic agent to form a contract is not bound by the terms of the contract unless the terms are capable of being reviewed by a person representing that party before the formation of the contract.

(4) A contract shall not be formed under subsection (1) where a natural person interacts directly with the electronic agent of another party and the electronic agent makes a material error when creating a data message unless—

(a) the other party notifies the natural person of the error as soon as practicable after he or she has learnt of the error;

(b) the electronic agent provides the natural person with an opportunity to prevent or correct the error;

(c) the party takes reasonable steps, including steps that conform to the instructions of the natural person to return any performance received, or, if instructed to do so, to destroy that performance; and

(d) the party has not used or received any material benefit or value from the performance received from the natural person.

Formation and validity of contracts.

14. (1) A contract shall not be denied legal effect merely because it is concluded partly or wholly by means of a data message.

(2) A contract by means of a data message is concluded at the time when and the place where acceptance of the offer is received by the person making the offer.

Time of dispatch of data message.

15. (1) Subject to an agreement to the contrary, where a data message enters a single information system outside the control of the person originating the data message or a person who sent the message on behalf of the person originating the message, the dispatch of the message occurs when the data message enters the information system.

(2) Where a data message successively enters two or more information systems outside the control of the person originating the data message, unless otherwise agreed between the person originating the message and the addressee, the dispatch of the message occurs when the data message enters the first of the information systems.

Time of receipt of data message.

16. (1) Unless otherwise agreed between the person originating the data message and the addressee, the time of receipt of a data message is determined where the addressee designates an information system for receiving a data message, and the receipt of a data message occurs—

(a) at the time when the data message enters the designated information system; or

(b) if the data message is sent to an information system of the addressee which is not the designated information system, at the time when the data message is received by the addressee.

(2) Where the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Subsections (1) and (2) shall apply notwithstanding that the place where the information system is located is different from the place where the data message is received under section 17.

Place of dispatch or receipt.

17. (1) Unless otherwise agreed by the person originating a data message and the addressee, a data message is deemed to have been—

(a) dispatched at the place of business of the originator; and

(b) received at the place of business of the addressee.

(2) For the purposes of subsection (1) the person originating the data message or the addressee—

(a) has more than one place of business—

(i) and one of the places can more closely be associated with the transaction, the place of business which can be closely associated with the transaction is presumed to be the place of business;

(ii) the principal place of business of the person originating the data message or the addressee is presumed to be the place of business;

(b) does not have a place of business, the place where the person originating the data message or the addressee ordinarily resides is presumed to be the place of business.

Expression of interest.

18. An expression of interest may be in the form of a data message and may be without an electronic signature as long as it is possible to infer the interest of the person from the data message

Attributing a data message to person originating the message.

19. (1) A data message is attributed to the person who originated the data message if the message is sent by—

(a) the person originating the message;

(b) an agent of the person originating the message or a person who has the authority to act on behalf of the person originating the data message; or

(c) an information system which is programmed by the person originating the message or on behalf of the person originating the message to operate automatically, unless it is proved that the information system did not execute the programming properly.

(2) The addressee shall regard a data message as sent by the originator and to act on that assumption if—

(a) in order to ascertain whether the data message is sent by the person originating the message, the addressee properly applies a method previously agreed to by the person originating the message for that purpose;

(b) the data message received by the addressee resulted from the action of a person whose relationship with the originator enabled the person to gain access to a method used by the originator to identify electronic records as records of the originator; or

(c) the data message is sent by an agent of the originator.

(3) Subsection (2) shall not apply where—

(a) the addressee receives notice from the originator that the originator did not send the data message;

(b) the addressee knows or ought to have known, had he or she exercised reasonable care or used the agreed method, that the data message was not sent by the originator ;or

(c) in the circumstances it is unreasonable for the addressee to regard the data message as a message of the originator or to act on the assumption that the data message was sent by the originator.

(4) This section shall not affect the law of agency or the law on formation of contracts.

Acknowledgement of receipt of data message.

20. (1) Subject to this section, an acknowledgement of receipt of a data message is not necessary to give legal effect to the data message.

(2) Where the originator specifies that the data message is conditional on receipt of the acknowledgement, the data message is taken as not sent, until the acknowledgement is received by the originator.

(3) Where the originator specifies that the data message is conditional on receipt of an acknowledgement and the acknowledgement is not received by the originator within the time specified or agreed upon or, if no time has been specified or agreed upon, within a reasonable time, the originator may—

(a) give notice to the addressee stating that an acknowledgement has not been received and specify a reasonable time within which the acknowledgement should be received; and

(b) upon notice to the addressee, treat the data message as though it has never been sent or exercise any other rights that he or she may have in respect of the data message.

(4) Where the originator does not specify that the acknowledgement is to be given in a particular form or by a particular method, the acknowledgement may be given by—

(a) any communication from the addressee, automated or otherwise; or

(b) any conduct of the addressee which is sufficient to indicate to the originator that the addressee received the data message.

(5) Where the originator receives the acknowledgement of receipt from the addressee, unless there is evidence to the contrary it is presumed, that the addressee received the data message.

(6) The presumption in subsection (5) does not imply that the content of the electronic record corresponds to the content of the record received.

(7) Where the acknowledgement states that the related data message fulfilled the technical requirements, either agreed upon or set forth in applicable standards, it is presumed, unless evidence to the contrary is adduced, that those requirements have been met.

(8) Except in so far as it relates to sending or receiving of a data message, this section does not apply to the legal consequences that arise from the data message or from the acknowledgement of its receipt.

Variation of conditions or requirements by agreement.

21. Sections 16, 17, 18, 19 or 20 may be varied by an agreement made between the parties involved in generating, sending, storing or processing a data message.

PART III—ELECTRONIC SIGNATURES.

Compliance with a requirement for a signature.

22. (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.

Conduct of the signatory.

23. (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.

Variation by agreement.

24. 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.

Conduct of the relying party.

25. A relying party shall bear the legal consequences of its 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.

Trust worthiness.

26. 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.

Conduct of the certification service provider.

27. (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 23(1)(b);

(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 23(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).

Advanced signatures.

28. (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.

Secure electronic signature.

29. 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.

Presumptions relating to secure and advanced electronic signatures.

30. (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.

PART IV—SECURE DIGITAL SIGNATURES.

Secure digital signatures.

31. 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 authority operating in compliance with regulations made under this Act;

(ii) the certificate was issued by a certification authority 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 authority on such conditions as the regulations may specify; or

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

Satisfaction of signature requirements.

32. (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 authority;

(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.

Unreliable digital signatures.

33. (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.

Digitally signed document taken to be written document.

34. (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 authority; 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.

Digitally signed document deemed to be original document.

35. 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.

Authentication of digital signatures.

36. A certificate issued by a licensed certification authority 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 authority 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.

Presumptions in adjudicating disputes.

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

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

(i) published in a recognised repository; or

(ii) made available by the issuing licensed certification authority or by the subscriber listed in the certificate, is issued by the licensed certification authority 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 authority 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 authority—

(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.

PART V—E-GOVERNMENT SERVICES

Electronic filing and issuing of documents.

38. Where a law provides that a public body may—

(a) accept the filing of a document or requires that a document be created or retained;

(b) issue a permit, licence or an approval; or

(c) provide for the making of a payment,

the public body may—

(i) accept the document to be filed, created or retained in the form of a data message;

(ii) issue the permit, licence or approval in electronic form; or

(iii) make or receive payment by electronic means.

Specific requirements by public body.

39. A public body may for the purposes of section 38 by notice in the *Gazette*, specify—

(a) the manner and format in which the data message shall be filed, created or retained;

(b) the manner and format in which the permit, licence or approval shall be issued;

(c) where the data message has to be signed, the type of electronic signature required;

(d) the manner and format in which the electronic signature shall be attached to or incorporated into the data message;

(e) the criteria that shall be met by an authentication service provider used by the person filing the data message or that the authentication service provider shall be a preferred authentication service provider;

(f) the appropriate control process and the procedure to ensure adequate integrity, security and confidentiality of a data message or a payment; and

(g) any other requirements in respect of the data message or payment.

(2) For the purposes of subsection (1) (e) a relevant generic service provider shall be a preferred authentication service provider.

PART VI—CONSUMER PROTECTION

Information to be provided by suppliers or sellers.

40. (1) A person offering goods or services for sale, hire or exchange through an electronic transaction shall provide to the consumers on the web site or electronic communication where the goods or services are offered, the following—

(a) the full name and legal status of the person;

(b) the physical address and telephone number of the person;

(c) the web site address or e-mail address of the person;

(d) membership of any self-regulatory or accreditation bodies to which the person belongs or subscribes and the contact details of that body;

(e) any code of conduct to which that person subscribes and how the consumer may access that code of conduct electronically;

(f) in the case of a legal person, the registration number, names of directors and place of registration;

(g) the physical address where the person may be served with documents;

(h) a description of the main characteristics of the goods or services offered by the person which is sufficient to enable a consumer to make an informed decision on the proposed electronic transaction;

(i) the full price of the goods or services, including transport costs, taxes and any other fees or costs;

(j) the manner of payment;

(k) any terms or conditions of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;

(l) the time within which the goods will be dispatched or delivered or within which the services will be rendered;

(m) the manner and period within which consumers may access and maintain a full record of the transaction;

(n) the return, exchange and refund policy of the person;

(o) any alternative dispute resolution code to which the person subscribes and how the code may be accessed electronically by the consumer;

(p) the security procedures and privacy policy of the person in respect of payment, payment information and personal information; and

(q) where appropriate, the minimum duration of the agreement in the case of agreements for the sale, hire, exchange or supply of products or services to be performed on an ongoing basis or recurrently.

(2) A person offering goods or services for sale, hire or exchange through an electronic transaction shall provide a consumer with an opportunity to—

(a) review the entire electronic transaction;

(b) correct any mistakes; and

(c) withdraw from the transaction before placing an order.

(3) Where a person offering goods or services for sale, hire or exchange through an electronic transaction fails to comply with subsection (1) or (2), a consumer may cancel the transaction within fourteen days after receiving the goods or services under the transaction.

(4) Where a transaction is cancelled under subsection (3)—

(a) the consumer shall return the goods to the person who offered the goods or, where applicable, cease using the service; and

(b) the person selling or offering the goods or services shall refund all payments made by the consumer after deducting the direct cost of returning the goods.

(5) For the purposes of subsection (4) (b) the person offering the goods or services shall use a payment system which is secure, according to the accepted technological standards at the time of the transaction.

(6) Where a person offering goods or services for sale, hire or exchange by electronic means fails to comply with subsections (4) (b) and (5) he or she is liable for the damage suffered by the consumer

(7) Subsection (3) does not apply to an electronic transaction—

(a) for financial services, including, investment services, insurance and reinsurance operations, banking services and securities;

(b) by way of an auction;

(c) for the supply of foodstuff, beverages or other goods intended for everyday consumption if they are supplied to the home, residence or workplace of the consumer;

(d) for services which began with the consumer's consent before the end of the seven-day period referred to in section 41(1);

(e) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;

(f) where the goods—

(i) are made to the specifications of the consumer;

(ii) are clearly personalised;

(iii) by reason of their nature cannot be returned; or

(iv) are likely to deteriorate or expire rapidly;

(g) where audio or video recordings or computer software is unsealed by the consumer;

(h) for the sale of newspapers, periodicals, magazines and books;

(i) for the provision of gaming and lottery services; or

(j) for the provision of accommodation, transport, catering or leisure services and where the supplier undertakes, when the transaction is concluded, to provide these services on a specific date or within a specific period.

Cancelling electronic transaction after receipt of goods or services.

41. (1) Subject to sub section (2), a consumer may cancel an electronic transaction and any related credit agreement for the supply of goods or services—

(a) within seven days after the date of receipt of the goods or services; or

(b) within seven days after the date of conclusion of the agreement.

(2) A consumer who returns goods after cancelling an electronic transaction under subsection (1) shall not be charged for the returning of the goods other than the direct cost of returning the goods.

(3) Where payment for the goods or services has been effected before a consumer exercises the right to cancel the transaction under subsection (1), the consumer is entitled to a full refund of money paid within thirty days of the date of the cancellation.

(4) This section shall not be construed as prejudicing the rights of a consumer which are provided for in any other law.

PART VI—CONSUMER PROTECTION.

Unsolicited goods, services or communications.

42. (1) A person who sends an unsolicited commercial communication to a consumer, shall provide—

(a) the consumer with the option to cancel his or her subscription to the mailing list of that person; and

(b) where the consumer requests, the particulars to identify the source from which that person obtained the personal information of the consumer.

Performance of electronic transaction.

43. (1) Where a person makes an order for goods or services by electronic means, unless otherwise agreed by the parties, the supplier shall execute the order within thirty days.

(2) Where the supplier fails to execute the order within thirty days or within the agreed period, the consumer may cancel the order after giving written notice of seven days.

(3) Where the supplier is not able to supply the goods or services, on the ground that the goods or services ordered are not available, he or she shall notify the consumer as soon as practicable and refund any payment made in respect of the goods or services within thirty days.

Invalidity of provisions excluding consumer rights.

44. A provision in an agreement, which excludes any rights provided for in this Part, is void.

PART VII—LIMITATION OF LIABILITY OF SERVICE PROVIDERS

Liability of a service provider.

45. (1) A service provider shall not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access if the liability is founded on—

(a) the making, publication, dissemination or distribution of the material or a statement made in the material; or

(b) the infringement of any rights subsisting in or in relation to the material.

(2) This section shall not affect—

(a) an obligation in a contract;

(b) the obligation of a network service provider under a licencing or regulatory framework which is established by law; or

(c) an obligation which is imposed by law or a court to remove, block or deny access to any material.

(3) For the purposes of this section, "provides access" in relation to third-party material, means providing the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access.

Information location tools.

46. Where a service provider refers or links users to a web page containing an infringing data message or infringing activity, the service provider is not liable for damage incurred by the user if the service provider—

(a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user;

(b) is not aware of the facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;

(c) does not receive a financial benefit directly attributable to the infringing activity; or

(d) removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to the data message infringes the rights of the user.

Notification of infringing data message or activity.

47. (1), A person who complains that a data message or an activity relating to the data message is unlawful shall notify the service provider or his or her designated agent in writing and the notification shall include—

(a) the full name and address of the person complaining;

(b) the written or electronic signature of the person complaining;

(c) the right that has allegedly been infringed;

(d) a description of the material or activity which is alleged to be the subject of infringing activity;

(e) the remedial action required to be taken by the service provider in respect of the complaint;

(f) telephone and electronic contact details of the person complaining;

(g) a declaration that the person complaining is acting in good faith; and

(h) a declaration that the information in the notification is correct to his or her knowledge.

(2) A person who knowingly makes a false statement on the notification in subsection (1) is liable to the service provider for the loss or damage suffered by the service provider.

Service provider not obliged to monitor data.

48. (1) For the purposes of complying with this Part, a service provider is not obliged to—

(a) monitor the data which the service provider transmits or stores; or

(b) actively seek for facts or circumstances indicating an unlawful activity.

(2) The Council may by statutory instrument, prescribe the procedure for service providers to—

(a) inform the competent public authorities of any alleged illegal activities undertaken or information provided by recipients of their service; and

(b) communicate information enabling the identification of a recipient of the service provided by the service provider, at the request of a competent authority.

Penalties

49. (1) A person who contravenes section 42 (1) commits an offence and is liable, on conviction to a fine not exceeding ten thousand dollars or to imprisonment not exceeding three years or both.

(2) A person who sends an unsolicited commercial communication to a person who has advised the sender that he or she should not send the communication, commits an offence and is liable on conviction, to a fine not exceeding ten thousand dollars or imprisonment not exceeding three years or both.

Regulations

50. The Council may, by statutory instrument make regulations for any—

(a) matter which is required to be prescribed;

(b) administrative or procedural matter which is necessary to give effect to this Act; or

(c) matter which is necessary and expedient to give effect to this Act.