THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2021

ARRANGEMENT OF SECTIONS

Single copies of this Act may be obtained from the Government Printer, P.O. Box 30136, 10101 Lusaka, Price K96.00 each.

PART IV

NATIONAL PUBLIC KEY INFRASTRUCTURE

PART V

CERTIFICATION AUTHORITY

PART VI

DUTIES OF SUBSCRIBERS

PART VII

TIME-STAMPING SERVICE PROVIDERS

PART VIII

CONSUMER PROTECTION

PART IX

DOMAIN NAME REGULATION

PART X

LIMITATION OF LIABILITY OF SERVICE PROVIDER

PART XI

ENCRYPTING COMMUNICATION

PART XII

GENERAL PROVISIONS

GOVERNMENT OF ZAMBIA

ACT

No. 4 of 2021

Date of Assent: 23rd March, 2021

An Act to provide a safe and effective environment for electronic transactions; promote secure electronic signatures; facilitate electronic filing of documents by public authorities; provide for the use, security, facilitation and regulation of electronic communications and transactions; promote legal certainty and confidence, and encourage investment and innovation in relation to electronic transactions; regulate the National Public Key Infrastructure; repeal and replace the Electronic Communications and Transactions Act, 2009; and provide for matters connected with, or incidental, to the foregoing.

[24th March, 2021

ENACTED by the Parliament of Zambia. Enactment

PART I
PRELIMINARY

1. This Act may be cited as the Electronic Communications and Transactions Act, 2021, and shall come into operation on the date appointed by the Minister by statutory instrument. Short title and commencement

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

"access" in relation to a computer system or electronic communication system, means the right to use or open the whole or any part of the computer system or electronic communication system, or to see, open, use, get or enter information in a computer system;

"advanced electronic signature" means a digital signature that is based on a certificate, that is unique to the user, capable of verification, under the sole control of the person using it and linked to the data in a manner that if the data is changed, the signature is invalidated;

"addressee" means a person who is intended by the originator to receive the electronic communication, but excludes a person acting as an intermediary in respect of that electronic communication;

"authenticity" means the assurance that a message, transaction or other exchange of information is from the author or service it purports to be from;

"Authority" has the meaning assigned to the word in the Information and Communications Technology Act, 2009;

Act No. 15 of 2009

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

"automated message system" means a preprogrammed system, or other automated system, used to initiate an action, respond to electronic communications or generate other performances in whole or in part without review or intervention by a party each time an action is initiated or a response is generated by the system;

"asymmetric crypto system" means a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key to verify the digital signature;

"caching" means the storage of data in an information system in order to speed up data transmission or processing;

"ccTLD" means a country code domain at the top level of the internet's main system signed according to the two letter codes in the International Standard ISO 3166 or any other standards as may be prescribed by the Minister;

"certificate" means a digital record issued by a certification authority for the purpose of supporting digital signatures which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;

"certificate holder" means a natural person in the case of a digital signature, and either a natural or a legal person in the case of a digital seal, to whose data the public key contained in the certificate is linked in the same certificate to whom a certificate is issued under this Act;

"certification authority" means an entity licensed under section 28 to manage and issue certificates and public keys;

"certification practice statement" means a statement issued by a certification authority specifying the practices that the certification authority employs in issuing a certificate;

"certificate revocation list" means a list of certificates that have been revoked by the issuing certification authority before their scheduled expiration date and are no longer trusted certificates;

"certification service" means a service of—

(a) issuing certificates necessary for giving digital signatures or digital seals to users;

(b) enabling the verification of digital signatures or digital seals given on the basis of certificates;

(c) implementing procedures for suspension, termination of suspension and revocation of certificates;

(d) checking the revocation status of the certificate and advising the relying party; or

(e) issuing cross-pair certificates;

"commerce business entity" means an entity that provides ecommerce services;

"communication" means oral, written, wire or electronic communication;

"Competition and Consumer Protection Commission" means the Competition and Consumer Protection Commission established by the Competition and Consumer Protection Act, 2010; Act No. 24 of 2010

"computer" means equipment or any part thereof, that perform predetermined arithmetic, logical, routing, processing or storage operations in accordance with set instructions and includes input devices, output devices, processing devices, computer data storage mediums and other equipment and devices related to, or connected with the computer system;

"computer network" means the interconnection of one or more computers or an information system through—

(a) the use of satellite, microwave, terrestrial line or other communication media; or

(b) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

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

"correspond" in relation to public key infrastructure or encryption keys, means to belong to the same key pair;

"cryptography" means the method of protecting information by transforming the information into unreadable format;

"cryptography product" means a product that makes use of cryptographic techniques in respect of data for the purpose of ensuring—

(a) that the data can be accessed only by a relevant person;

(b) the authenticity of the data;

(c) the integrity of the data; and

(d) that the source of the data can be correctly ascertained;

"cryptography provider" means any person who provides a cryptography service or product in the Republic;

"cryptography service" means a service which is provided to a seller or a recipient of a data message, or anyone storing a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring—

(a) that the data or data message can be accessed, or can be put into an intelligible form only by a certain person;

(b) that the authenticity and integrity of that data or data message is capable of being ascertained; and

(c) the integrity of the data or data message or that the source of the data or data message can be correctly ascertained.

"data" means an electronic representation of information in any form;

"data message" means data generated, sent, received or stored by electronic, optical or similar means and includes, but is not limited to electronic data interchange (EDI), voice, stored record, electronic mail, mobile communications audio and video recordings;

"digital seal" means a digital signature for use by a person authorised to use a seal under any law and may be used by more than one person or system under that person's authorisation;

"digital signature" means an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine whether the—

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

(b) initial electronic record has been altered since the transformation was made;

"domain name" means the alphanumeric designation that is registered or assigned in respect of an electronic address or other resource on the internet;

"domain name system" means a system to translate domain names into IP addresses or other resources;

"ecommerce" means a system which allows a commercial transaction to be conducted electronically on the internet or any other network using electronic, optical or similar media for information exchange;

"electronic" in relation to technology, means having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities;

"electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response;

"electronic communication" means a transfer of signs, signals, writings, images, sounds, data or intelligence of any nature transmitted in whole or in part by radio, electromagnetic, photo-electronic or photo-optic system, but does not include—

(a) direct oral communication; or

(b) any communication made through a tone only paging device;

"electronic communications system" means a radio, electromagnetic, photooptical or photoelectronic facility for the transmission of electronic communications, and any computer facility or related electronic equipment, for electronic storage of those communications;

"electronic signature" means—

(a) sound;

(b) symbol;

(c) process; or

(d) other data created or adopted by a person with the intent to sign a data message;

"electronic transaction" means a transaction, action or set of transactions of a commercial or non-commercial nature, that takes place electronically;

"hash function" means an algorithm mapping data of arbitrary size to fixed size values such that—

(a) a record yields the same hash result every time the algorithm is executed using the same record as input;

(b) it is computationally infeasible that a record can be derived or reconstituted from the hash result produced by the algorithm; and

(c) it is computationally infeasible that two or more records can be found that produce the same hash result using the algorithm;

"hosting" means the service of storage of data or providing storage of computing resources for one self or others;

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

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

"key pair" in an asymmetric cryptosystem, means a private key and its mathematically related public key, having a property that allows the public key to verify a digital signature that the private key creates;

"National Public Key Infrastructure" means a Government deployed public key infrastructure whose root certification authority is established as the highest level certification authority of Zambia and is managed by the National Root Certification Authority as a regulatory function;

"National Root Certification Authority" means the National Root Certification Authority referred to under section 25;

"operational period" in relation to a certificate, means a period beginning on the date and time the certificate is issued by a certification authority, or a later date and time specified in the certificate and ending on the date and time the certificate expires or as stated in the certificate, unless earlier revoked or suspended;

"private certification authority" means a certification authority registered by the National Root Certification Authority to provide certification services to institutions whose information infrastructure is not critical;

"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;

"public key infrastructure" means a system comprising hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public keys;

"recovery agent" means a person or entity who provides recovery information for storage services;

"recovery information" means a parameter that may be used with an algorithm, other data or hardware, to decrypt data or communications;

"registrar" means a person who is given authority to populate a .zm domain registry;

"Registry" means a database of domain names registered under .zm;

"registrant" means the person or organisation whose application of a domain name is successful;

"registration authority" means a person or entity that is entrusted by the certification authority to register or vouch for the identity of users of a certification authority, but does not sign certificates;

"repository" means a system for storing and retrieving certificates or other information relevant to a certificate;

"secure signature creation device" means an adapted piece of software or hardware, and includes a microchip card equipped with a security chip, which is used for the storage and application of a private key;

"subscriber" means a person who is the subject named or identified in a certificate issued to that person and who holds a private key that corresponds to a public key listed in that certificate;

"timestamp" means a data unit created using a system of technical and organisational means which certifies the existence of electronic data at a given time;

"time stamping service" is the issue of a time stamp necessary to prove the official time and temporary order of a digital signature and digital seal and the creation of conditions for verification of the issued time stamp; and

"trustworthy system" means computer hardware, software and procedures that—

(a) are reasonably secure from intrusion and misuse;

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

(c) are reasonably suited to perform their intended function; and

(d) adhere to generally accepted security procedures.

Application

3. (1) This Act applies to electronic transactions, electronic communications and electronic records used in the context of commercial and noncommercial activities that include domestic and international transactions, arrangements, agreements and exchanges and storage of information and other related transactions.

(2) Except as otherwise specified, this Act shall not be construed as—

(a) requiring any person to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by, or in electronic form; or

(b) prohibiting a person from establishing requirements in respect of the manner in which that person will accept data messages.

(3) Except as otherwise specified, this Act does not limit the operation of any written law that authorises electronic payments, electronic money and value transaction services, prohibits or regulates the use of data messages, including any requirement by, or under, any law for information to be posted or displayed in a specified manner, or for any information or document to be transmitted, stored or retained by a specified method.

PART II
LEGAL REQUIREMENTS FOR DATA MESSAGES

Legal requirements for data message

4. (1) Data has legal force and effect if that data—

(a) is wholly or partly in the form of a data message; and

(b) is not contained in the data message purporting to give legal effect, but is merely referred to in that data message.

(2) Information incorporated into an agreement and that is not in the public domain shall be treated as having been incorporated into a data message if that information is—

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

(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 as long as the information is reasonably capable of being reduced to electronic form by the party incorporating it.

Writing

5. A requirement in law that a document or information shall be in writing is met if the document or information is—

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

(b) accessible and capable of being retained in a manner usable for subsequent reference.

Use of advanced electronic signature

6. (1) Where the signature of a person is required by law and that law does not specify the type of signature, that requirement in relation to a data message is met if an advanced electronic signature is used.

(2) Subject to subsection (1), an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.

Use of electronic signature

7. (1) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if—

(a) a method is used to identify the person and to indicate the person's approval of the information communicated; and

(b) having regard to the relevant circumstances at the time the method was used, the method was reliable and appropriate for the purposes for which the information was communicated.

(2) Where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement shall not be without legal effect merely on the grounds that—

(a) it is in the form of a data message; or

(b) it is not evidenced by an electronic signature but is evidenced by other means from which that person's intent or other statement may be inferred.

(3) Where an advanced electronic signature is used as a valid signature, that signature shall be treated as a valid electronic signature and to have been applied properly, unless the contrary is proved.

Determination of originality of data message

8. (1) Where a law requires information to be presented or retained in its original form, that requirement is met 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 the assessment specified under 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 integrity of any information is assessed—

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

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

(c) by having regard to other relevant circumstances.

Admissibility and evidential weight of data message

9. (1) In any legal proceedings, the rules of evidence shall not be applied so as to deny the admissibility of a data message in evidence —

(a) on the mere grounds that it is constituted by a data message; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original format provided the substance is the same.

(2) Information in the form of a data message shall be given due evidential weight.

(3) In any legal proceedings, when assessing the evidential weight of a data message, regard shall be had 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 integrity of the data message was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of, or an extract from, the data message certified to be correct by an officer in the service of that person, shall on its mere production in any civil, criminal, administrative or disciplinary proceedings under a written law, be admissible in evidence against a person and rebuttable proof of the facts contained in a record, copy, printout or extract.

Retention of information in data message

10. (1) Where a law requires information to be retained, that requirement is met by retaining the information in the form of a data message if—

(a) the information contained in the data message is accessible and usable for subsequent reference;

(b) the data message is in the form or format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) the origin and destination of that data message, and the date and time it was sent or received, may be determined.

(2) The obligation to retain information under subsection (1) does not extend to any information whose sole purpose is to enable the message to be sent or received.

Production of document or information

11. (1) Subject to section 24, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information and if—

(a) considering all the relevant circumstances at the time that 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 therein would be readily accessible and usable for subsequent reference.

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

(a) the addition of any endorsement; or

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

Notarisation, acknowledgment and certification

12. (1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement shall be met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the data message containing that notarisation, acknowledgment or verification.

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement shall be met if the person provides a printout certified to be a true reproduction of the document or information.

(3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.

Other legal requirement

13. (1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time is satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) An expression in a law, whether used as a noun or verb, including the words "document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print" or words or expressions of similar effect, shall be interpreted to include or permit that form, format or action in relation to a data message unless otherwise provided for in this Act.

(3) Where a seal is required by a written law to be affixed to a document and that written law does not prescribe the method or form by which that document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

(4) Where any law requires or permits a person to send a document or information by registered or certified post or similar service, that requirement shall be met if an electronic copy of the document or information is sent to the office of a courier service provider, is registered and sent by that courier service provider to the electronic address provided by the sender.

Automated transaction

14. In an automated transaction—

(a) an agreement may be formed where an electronic agent performs an action required by law for purposes of an agreement;

(b) an agreement may be formed where the parties to a transaction or either one of them uses an electronic agent;

(c) a party using an electronic agent to form an agreement shall, subject to paragraph (d), be presumed to be bound by the terms of that agreement irrespective of whether that person reviewed the actions of the electronic agent or the terms of the agreement;

(d) a party interacting with an electronic agent to form an agreement is not bound by the terms of the agreement unless those terms are capable of being reviewed by a natural person representing that party prior to agreement formation;

*(e)*an agreement shall not be formed where a natural person interacted directly with the electronic agent of another person and made a material error during the creation of a data message and—

(i) the electronic agent did not provide that natural person with an opportunity to prevent or correct the error;

(ii) that natural person notified the other person of the error as soon as practicable after that person learnt of it;

(iii) that natural person takes reasonable steps, including steps that conform to the other person's instructions to return any performance received, or, if instructed to do so, to destroy that performance; and

(iv) that natural person has not used or received any material benefit or value from any performance received from the other person.

Dispatch of electronic record

15. Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic record occurs when it enters an information system outside the control of the originator or the agent of the originator.

Receipt of electronic record

16. The time of receipt of an electronic record shall be determined as follows:

(a) where the addressee designates an information system for the purpose of receiving electronic records, receipt occurs at the time when the electronic record enters the designated information system; or

(b) where the addressee does not designate an information system, receipt occurs when the electronic record enters an information system of the addressee through which the addressee retrieves the electronic record.

Expression of intent or other statement

17. An expression of intent or other electronic representation of an electronic record between the originator and the addressee of an electronic record is admissible in circumstances where the intent or other electronic representation is relevant at law.

Attribution of electronic records to originator

18. (1) An electronic record is considered to be that of the originator if it was sent by—

(a) the originator personally;

(b) a person who has authority to act on behalf of the originator in respect of that electronic record; or

(c) an information system programmed by or on behalf of the originator to operate automatically, unless it is proved that the information system did not properly execute the programme.

(2) An addressee is entitled to regard an electronic record as being that of the originator and to act on that assumption, if—

(a) the addressee properly applied a procedure previously agreed with the originator in order to ascertain whether the electronic record was that of the originator; or

(b) the electronic record received by the addressee resulted from the actions of a person whose relationship with the originator or with an agent of the originator enabled that person to gain access to a method used by the originator to identify an electronic record as the originator's own.

(3) Where a procedure has not been agreed to by both parties to ascertain the originator, the person who appears to be the originator shall be presumed to be the originator.

(4) The presumption under subsection (3) does not apply where

(a) the addressee has received notice from the originator that the electronic record was issued without the knowledge or consent of the originator;

(b) the addressee knew or should reasonably have known, or used any agreed procedure to know that the electronic record was not that of the originator and that the person who sent the electronic record did not have the authority of the originator to issue or send the electronic record; or

(c) the addressee knew or should reasonably have known, that the transmission resulted in an error in the electronic record as received.

Acknowledgment of receipt of electronic record

19. (1) An acknowledgment of receipt may be given through

(a) a communication by the addressee, whether automated or otherwise; or

(b) any conduct of the addressee to indicate to the originator that the electronic record has been received.

(2) An acknowledgment of receipt is not required to give legal effect to a message unless otherwise agreed by the parties.

PART III
Communication of Data Messages

Application of Part

20. This Part applies if the parties involved in the generation, sending, receipt, storage or other processing of data message have not reached an agreement on the issues provided for in the data message.

Formation and validity of agreement

21. (1) An agreement shall not be without legal effect merely because it was concluded partly or in whole by means of a data message.

(2) An agreement concluded between parties by means of a data message shall be concluded at the time when, and place where, the acceptance of the offer was received by the offeror.

Expression of intent or other statement

22. An expression of intent or other statement as between the originator and the addressee of a data message shall not be without legal effect merely on the grounds that it is—

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

(b) not evidenced by an electronic signature, but by other means from which that person's intent or other statement may be inferred.

Acceptance of electronic filing and issuing of document

23. A public body that, subject to any written law, accepts the filing of documents, or requires that a document be created or retained, issues any permit, licence or approval or provides for a manner of payment, may, despite anything to the contrary in that law—

(a) accept the filing of the document, or the creation or retention of the document in the form of a data message;

(b) issue the permit, licence or approval in the form of a data message; or

(c) make or receive payment in an electronic form or by electronic means.

Requirements for electronic filing and issuing of document

24. A public body may, where that public body performs any of the functions under section 23, specify, in the Gazette, a daily newspaper of general circulation in the Republic or any other form of the public body's electronic platform—

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

(b) in cases where a data message has to be signed, the type of electronic signature required;

(c) the manner and format in which an electronic signature shall be attached to, incorporated in or otherwise associated with, a data message;

(d) the identity of, or criteria that shall be met by a designated certification authority used by the person filing a data message;

(e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and

(f) any other requirements for data messages or payments.

PART IV

National Public Key Infrastructure

National Root Certification Authority

25. For the purposes of this Part, the Authority shall perform the functions of the National Root Certification Authority.

Functions of National Root Certification Authority

26. (1) The National Root Certification Authority shall regulate the national public key infrastructure.

(2) Without limiting the generality of subsection (1), the functions of the National Root Certification Authority are to—

(a) licence certification authorities and time stamping service providers;

(b) register cryptography service providers;

(c) monitor the conduct, systems and operations of certification authorities, time stamping service providers and cryptography service providers to ensure compliance with this Act;

(d) appoint an independent auditing firm to conduct periodic audits of a certification authority to ensure compliance with the provisions of this Act;

(e) verify the accuracy of results of the information systems audit submitted to the National Root Certification Authority;

(f) conduct inspections and audits;

(g) maintain a certificate revocation list and any other repositories;

(h) conduct research and development with regard to certification and cryptography services;

(i) issue guidelines relating to national public key infrastructure; and

(j) regulate the provision of secure signature creation devices.

Prohibition of providing certification service or time-stamping service without licence

27. (1) A person shall not provide a certification service or a timestamping service to an institution with critical information infrastructure without a 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 one million penalty units or to imprisonment for a term not exceeding ten years, or to both.

(3) A private certification authority shall not provide a certification service under this Act without notifying the Authority in the prescribed manner and form.

Licence

28. (1) A person who intends to provide a certification service or a time stamping service to an institution with critical information infrastructure, shall apply to the National Root Certification Authority for a licence in the prescribed manner and form on payment of the prescribed fee.

(2) The National Root Certification Authority shall, within sixty days of receipt of an application, under subsection (1), grant or reject the application.

(3) The National Root Certification Authority shall, in considering an application for a licence made under subsection (1) have regard to the—

(a) financial and technical capability of the applicant;

(b) the ability of an electronic signature to—

(i) uniquely be linked to the user;

(ii) identify the user;

(iii) be maintained under the sole control of the user;

(iv) be linked to the data or data message to which it relates in a manner that any subsequent change of the data or data message is detectable; and

(v) enable face to face identification of the user;

(c) the quality of the hardware and software systems;

(d) the procedures for the processing of products or services;

(e) the availability of information to third parties relying on the certification service;

(f) the regularity and extent of audits by an independent body;

(g) the applicant's ability to comply with the latest version of Request for Comments 3161 standard issued by the Internet Engineering Task Force; and

(h) any other relevant factor that may be prescribed.

(4) The National Root Certification Authority shall, where it rejects an application for a licence, inform the applicant, in writing, giving reasons for the decision.

(5) Where the National Root Certification Authority fails to make a decision within the period specified under subsection (2), the application is considered to have been granted.

(6) The National Root Certification Authority may request for further particulars in respect of an application.

(7) Where the National Root Certification Authority requests for particulars referred to in subsection (6), the period referred to in subsection (2) shall stop running.

Certification authority

29. (1) The following entities may apply to be licensed as a certification authority under the national public key infrastructure:

(a) public companies;

(b) private limited companies; or

(c) statutory bodies.

(2) The following entities shall form part of the national public key infrastructure:

(a) Government entities; and

(b) entities providing certification services to entities whose information infrastructure has been declared as critical under the applicable written law.

Variation of licence

30. (1) A licensee may, at any time during the validity of the licence, apply to the Authority for variation of the terms and conditions of the licence or any matter relating to the licence.

(2) The National Root Certification Authority shall consider the application under subsection (1) and may grant or reject the application.

(3) The National Root Certification Authority may, on its own motion, vary the terms and conditions of a licence where—

(a) the variation is necessary in the public interest; or

(b) the variation is necessary to address the concerns of the members of the public or subscribers.

(4) The National Root Certification Authority shall, before making any variation of the terms and conditions of a licence under this section, notify the licensee—

(a) of its intention to vary the licence in the manner specified in the notice; and

(b) specifying the period, not being less than thirty days from the date of service of the notice on the licensee, within which a written representation in respect of the proposed variation may be made to the National Root Certification Authority by the licensee.

(5) Where a licence is varied under subsection (1), the National Root Certification Authority shall not refund any fees paid for with respect to the licence.

Surrender of licence

31. (1) A licensee shall, where a licensee decides not to continue providing the services relating to the licence, notify the National Root Certification Authority in writing and shall agree with the National Root Certification Authority on the terms and conditions of the surrender of the licence, with particular reference to anything done or any benefit obtained under the licence.

(2) Where a licence is surrendered under sub- section (1)—

(a) the licence shall lapse and the licensee shall cease to be entitled to any benefits arising from the licence;

(b) the licensee shall not be refunded the licence fees.

(3) Where a licence is surrendered under subsection (1), the licensee is not entitled to a refund of any fees paid with respect to the licence.

Transfer, cede or assignment of licence

32. (1) A licensee shall not cede, pledge, encumber or otherwise dispose of a licence.

(2) A licensee may transfer or assign a licence with the prior approval of the National Root Certification Authority.

(3) An application for approval to transfer or assign a licence shall be made to the National Root Certification Authority in a prescribed manner and form and the Authority may, within thirty days of receipt of the application—

(a) approve the application on terms and conditions that it may determine; or

(b) reject the application in accordance with this Act.

Suspension or cancellation of licence

33. (1) Subject to this Act, the National Root Certification Authority may suspend or cancel a licence if the holder—

(a) obtained the licence by fraud or submission of false information or statements;

(b) contravenes this Act, any other written law relating to the licence or any terms and conditions of the licence;

(c) fails to comply with a decision or guidelines issued by the National Root Certification Authority;

(d) enters into receivership or liquidation or takes an action for voluntary winding up or dissolution;

(e) enters into any scheme of arrangement, other than for the purpose of reconstruction or amalgamation, on terms and within a period that may previously have been approved in writing by the National Root Certification Authority;

(f) is the subject of any order that is made by a court or tribunal for its compulsory winding up or dissolution;

(g) has ceased to fulfil the eligibility requirements under this Act; or

(h) the suspension or cancellation is in the public interest.

(2) The National Root Certification Authority shall before suspending or cancelling the licence, give written notice to the holder thereof of its intention to suspend or cancel the licence and shall—

(a) give the reasons for the intended suspension or cancellation; and

(b) require the holder to show cause, within a period of not more than thirty days, why the licence should not be suspended or cancelled.

(3) The National Root Certification Authority shall not suspend or cancel a licence under this section where the licensee takes remedial measures to the satisfaction of the National Root Certification Authority within the period specified under subsection (2).

(4) The National Root Certification Authority shall, in making its final determination on the suspension or cancellation of the licence consider submissions made by the licensee under subsection (2).

(5) The National Root Certification Authority may suspend or cancel a licence where the holder, after being notified under subsection (2) fails to show cause or does not take remedial measures, to the satisfaction of the Authority within the time specified in the notice.

(6) The National Root Certification Authority shall, where it suspends or cancels a licence under this section, enter the suspension or revocation in the Register.

Registration of cryptography service provider

34. (1) A person who intends to provide cryptography services shall apply for registration to the National Root Certification Authority in the prescribed manner and form on payment of a prescribed fee.

(2) A person shall not provide a cryptography service without registration.

(3) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years or to both.

Recognition of foreign certification authority

35. (1) The National Root Certification Authority may, by notice in the Gazette and subject to the conditions that the National Root Certification Authority may determine, recognise a licence, accreditation or recognition granted to a foreign certification authority by a foreign country.

(2) A foreign certification authority that falsely holds out any products or services as recognised by the National Root Certification Authority under subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

Issue of certificate to subscriber

36. A certification authority may issue a certificate to a subscriber where—

(a) the certification authority has received an application from the subscriber;

(b) the certification authority has complied with its certification practice statement, including procedures regarding identification of the subscriber;

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

(d) in the case of a subscriber acting through an agent, the certification authority has verified that the subscriber has authorised the agent to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

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

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

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

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

Details of certificate

37. A certificate shall set out—

(a) the number of the certificate;

(b) the name of the certificate holder;

(c) the personal identification code or registry code of the certificate holder;

(d) the public key of the certificate holder;

(e) the period of validity of the certificate;

(f) the issuer and registry code of the issuer; and

(g) a description of the limitations on the scope of use of the certificate.

PART V
CERTIFICATION AUTHORITY

Trustworthy system

38. A certification authority shall utilise a trustworthy system in performing its services.

Disclosure and compliance with certification practice statement

39. (1) A certification authority shall disclose—

(a) its certificate that contains the public key corresponding to the private key used by that certification authority to digitally sign another certificate;

(b) a certification practice statement as prescribed;

(c) notice of the revocation or suspension of certificate; and

(d) any other fact that materially and adversely affects either the reliability of a certificate that the authority has issued or the authority's ability to carry out its obligations.

(2) In the event of an occurrence that materially and adversely affects a certification authority's trustworthy system or its certificate, the certification authority shall—

(a) use reasonable efforts to notify any person who is known or likely to be affected by that occurence.

(b) act in accordance with procedures governing such an occurrence as specified in its certification practice statement.

Audit services

40. (1) A certification authority shall conduct an information system audit annually and submit the audit report to the National Root Certification Authority.

(2) Despite subsection (1), the National Root Certification Authority may require a certification authority to conduct an information system audit as and when the Authority considers it necessary at the cost of the certification authority.

Publication of certificate revocation list

41. (1) A certification authority shall maintain a certificate revocation list.

(2) A certification authority that contravenes subsection(1) commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units.

Prohibition of publication of certificate

42. A person shall not publish a certificate or otherwise make it available to another person if—

(a) that person is not the certification authority listed in that certificate;

(b) the subscriber listed in that certificate has not accepted it; or

(c) the certificate has been suspended or revoked, unless that publication is for the purpose of verifying a digital signature created prior to that suspension or revocation.

Representations on issuance of certificate

43. A certification authority by issuing a certificate, represents to any person who reasonably relies on the certificate, that—

(a) the certification authority has issued the certificate in accordance with the applicable certification practice statement incorporated by reference in the certificate, or of which the relying party has notice;

(b) the certification authority has complied with requirements under this Act for issuing of certificate, and that the subscriber listed in the certificate has accepted it;

(c) the subscriber identified in the certificate holds the private key corresponding to the public key listed in the certificate;

(d) the subscriber's public key and private key constitute a functioning key pair;

(e) information in the certificate is accurate, unless the certification authority has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed; and

(f) the certification authority has no knowledge of any material fact which if included in the certificate would adversely affect the reliability of the representations in paragaphs *(a)* to *(d)*.

Recommended reliance limits

44. (1) A certification authority shall, in issuing a certificate to a subscriber, specify a recommended reliance limit in the certificate.

(2) The certification authority may specify different reliance limits in different certificates as it considers fit.

Liability limits for certification authority

45. Subject to an agreement between a certification authority and a subscriber, a certification authority is not liable—

(a) 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 certification authority complied with the requirements of this act; or

(b) 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 certification authority is required to confirm; or

(ii) failure to comply with requirements for issuance of the certificate and representations on issuance of the certificate.

Suspension of certification authority certificate

46. A certification authority may suspend a certificate—

(a) on request by the subscriber listed in the certificate or a person duly authorised by that subscriber;

(b) by court order; or

(c) if there are reasonable grounds to believe that incorrect data has been entered in the certificate or that it is possible to use the private key corresponding to the public key contained in the certificate without the consent of the certificate holder.

Notice of suspension

47. A certification authority shall, after the suspension of a certificate under section 46 publish a signed notice of the suspension in the repository.

Revocation of Cetificate

48. A certification authority shall revoke a certificate—

(a) on receiving a request for revocation by the subscriber listed in the certificate and confirming that the person requesting the revocation is the subscriber, or is an agent of the subscriber with authority to request the revocation;

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

(c) on presentation of documents effecting a dissolution of the subscriber, or on confirming by other evidence that the subscriber has been dissolved or ceases to exist.

Revocation without subscriber's consent

49. (1) A certification authority shall revoke a certificate, regardless of whether the subscriber listed in the certificate consents, where the certification authority confirms that—

(a) a material fact represented in the certificate is false;

(b) a requirement for issuance of the certificate was not satisfied;

(c) the certification authority's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability;

(d) an individual subscriber is dead; or

(e) a subscriber has been dissolved, wound up or otherwise ceases to exist.

(2) The certification authority shall, where the certification authority revokes the certificate under subsection (1), immediately notify the subscriber listed in the revoked certificate.

Notice of revocation

50. (1) A certification authority shall, publish a signed notice of the revocation under section 48 in a repository specified in the certificate.

(2) The certification authority shall, where one or more repositories are specified, publish a signed notice of the revocation in all those repositories.

Appointment of registration authority

51. The certification authority may appoint any person as a registration authority as prescribed.

Appeals under this Part

52. A person aggrieved with the decision of a certification authority may appeal to the Authority within fourteen days of receiving the move of suspension or revocation.

PART VI
DUTIES OF SUBSCRIBERS

Generating key pair

53. (1) A subscriber shall, where the subscriber generates a key pair whose public key is to be listed in a certificate and accepted by the subscriber, generate that key pair using a trustworthy system.

(2) This section shall not apply to a subscriber who generates the key pair using a system approved by a certification authority.

Obtaining certificate

54. A subscriber shall ensure that all material representation to a certification authority for purposes of obtaining a certificate, including all information known to the subscriber and represented in the certificate, shall be accurate and complete to the best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the certification authority.

Acceptance of certificate

55. (1) A subscriber is deemed to have accepted a certificate if the subscriber—

(a) publishes or authorises the publication of the certificate

(i) to one or more persons; or

(ii) in a repository; or

(b) otherwise demonstrates approval of the certificate while knowing or having notice of its contents.

(2) A subscriber who accepts a certificate issued by a certification authority, shall certify that—

(a) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate;

(b) a representation made by the subscriber to the certification authority to the information listed in the certificate is true; and

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

Control of private key

56. (1) A subscriber identified in the certificate who accepts a certificate issued by a certification authority, shall exercise reasonable care in retaining control of the private key corresponding to the public key listed in that certificate and prevent its disclosure to a person not authorised to create that subscriber's digital signature.

(2) A subscriber shall continue to perform the duty under subsection (1) during the operational period of the certificate and during any period of suspension of the certificate.

Suspension or revocation of compromised certificate

57. A subscriber who has accepted a certificate from a certification authority shall, where the private key corresponding to the public key listed in the certificate has been compromised, request the issuing certification authority as soon as possible to suspend or revoke the certificate.

PART VII

TIME STAMPING SERVICE PROVIDERS

Time-stamping service

58. (1) A person who intends to provide a timestamping service shall ensure that the timestamp is linked to data in a manner that precludes the possibility of changing the data undetectably after obtaining the time-stamp.

(2) A timestamping service provider shall confirm the time-stamps issued by that provider when required.

(3) A timestamping service provider shall ensure that it is impossible for that timestamping service provider's systems to issue identical time stamps for a time earlier or later than the relevant point in time to which the time-stamping service is applied.

Time-stamping service provider

59. The following entities may provide a time stamping service:

(a) public company;

(b) private limited company; or

(c) State body.

Requirements for time-stamping service provider

60. (1) A timestamping service provider shall comply with the requirements established by this Act and be capable of ensuring a reliable timestamping service in accordance with this Act.

(2) A timestamping service provider shall annually conduct an information systems audit and submit the results to the Authority.

(3) Despite subsection (2), the Authority may require a timestamping service provider to conduct an information system audit as and when the Authority determines and at the cost of the time stamping service provider.

(4) A timestamping service provider shall procure insurance relating to the provider's licensed services up to a prescribed amount and in the manner prescribed.

Duties of time stamping service provider

61. A timestamping service provider shall—

(a) make correct indications of time in time stamps pursuant to the descriptions provided in guidelines issued by the Authority;

(b) maintain records of issued time- stamps;

(c) preserve documentation in order to verify issued time-stamps;

(d) ensure that it is possible to obtain and verify time stamps in the data communication network as and when required;

(e) conduct an annual information systems audit and submit the results of the audit to the authorised processor of the register of certification;

(f) publicise the conditions of compulsory insurance contracts in a data communication network where applicable; and

(g) inform the authorised processor of the register of certification of any changes to a public key used in the provision of a timestamping service.

PART VIII
CONSUMER PROTECTION

Scope of application

62. This Part is without prejudice to any other written law in force on consumer protection in relation to electronic transactions.

Information to be provided by supplier

63. (1) A supplier offering goods or services for sale, hire or exchange by way of an electronic transaction shall, where applicable, make the following information available to consumers on the website, application or other electronic media platform, where the goods or services are offered:

(a) the supplier's full name and legal status;

(b) the supplier's physical address and telephone number;

(c) the supplier's website address and email address;

(d) membership to any selfregulatory or accreditation body to which that supplier belongs or subscribes and the contact details of that body;

(e) any code of conduct to which that supplier subscribes and how that code of conduct may be accessed electronically by the consumer;

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

(g) the physical address where that supplier will receive legal service of documents;

(h) a description of the main characteristics of the goods or services offered by that supplier to enable a consumer 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 for the goods or services;

(k) any terms 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 can access and maintain a full record of the transaction;

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

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

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

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

(r) the rights of consumers in terms of section 65 where applicable;

(s) health and safety information; and

(t) any other information as maybe prescribed.

(2) A supplier 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 finally placing any order.

(3) Despite subsection (2), if a supplier fails to comply with the provisions of subsection (1) or (2), the consumer may cancel the transaction within fourteen days of receiving the goods or services under the transaction.

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

(a) the consumer shall return the goods to the supplier or, where applicable, cease using the services performed;

(b) the supplier shall refund all payments made by the consumer for goods or services where applicable minus the direct cost of returning the goods; and

(c) the consumer shall return the goods to the supplier in a condition as may be prescribed by the Minister.

(5) A supplier shall utilise a payment system that is sufficiently secure in accordance with accepted technological standards at the time of the transaction and the type of transaction concerned.

(6) A supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5).

(7) A person who contravenes provisions of subsection (1) commits an offence.

(8) A supplier referred to under subsection (1) shall register with the Authority in the prescribed manner and form.

Online market

64. (1) A person may market a product or service by means of electronic communication.

(2) A person marketing by means of electronic communication shall provide the addressee with

(a) the person's identity and contact details including its registered office and place of business, email, contact and customer service number;

(b) a valid and operational optout facility from receiving similar communications in future;

(c) the identifying particulars of the source from which the originator obtained the addressee's personal information; and

(d) applicable privacy and other user policies.

Unsolicited goods, services or communications

65. (1) A person may send one unsolicited commercial communication to a consumer.

(2) A person shall only send a commercial communications to an address where the optin requirement is met.

(3) The optin requirement is met where the addressee consents to the receipt of commercial communication and where—

(a) the addressee's email address, phone number and other personal information was collected by the originator of the message in the course of a sale or negotiations for a sale;

(b) the originator only sends promotional messages relating to its "similar products and services" to the addressee;

(c) the personal information and address was collected by the originator, the originator offered the addressee the opportunity to optout, free of charge except for the cost of transmission, and the addressee declined to opt-out; and

(d) the opportunity to optout is provided by the originator to the addressee with every subsequent message.

(4) A person shall not send a commercial communication on goods or services unless—

(a) the consumer consents to the communication;

(b) at the beginning of the communication, the sender discloses the identity of the sender and its purpose; and

(c) that communication gives an optout option to reject further communication.

(4) A contract is not formed where an addressee does not respond to commercial communication.

(5) An originator who fails to provide the recipient with an operational optout facility under subsections (2)(c) and (d) commits and offence.

(6) An originator who sends unsolicited commercial communications to an addressee who has opted-out from receiving any further electronic communications from the originator through the originator's optout facility, commits an offence.

(7) A person who advertises or who knowingly has goods or services advertised in contravention of this section commits an offence.

(8) A person convicted of an offence under this section is liable on conviction to a fine not exceeding five thousand penalty units or imprisonment for a term not exceeding five years, or to both.

Cooling-off period

66. (1) A consumer may cancel, without giving any reason and without incurring any penalty, a transaction and a related credit agreement for the supply of

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

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

(2) Where a consumer cancels a transaction under subsection (1), the only charge that may be levied on the consumer is the direct cost of returning the goods.

(3) If payment for the goods or services has been effected prior to a consumer exercising the right under subsection (1), the supplier shall give the consumer a full refund of the payment, which refund shall be made within thirty days of the date of cancellation.

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

(5) Subsection (1) does not apply to an electronic transaction—

(a) for a financial service, including an investment service, insurance and reinsurance operation, banking service or operation relating to dealings in securities;

(b) by way of an auction;

(c) for the supply of food stuffs, beverages or other goods intended for everyday consumption supplied to a home, residence or workplace of a consumer;

(d) for services which have been performed in full with the consumer's consent before the end of the sevenday period specified under subsection (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 consumer's specifications;

(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 were unsealed, streamed or downloaded by the consumer;

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

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

(j) any other goods or services as the Minister may prescribe.

Performance

67. (1) A supplier shall execute an order within thirty days from the date on which the supplier received the order, unless the parties have agreed otherwise.

(2) Where a supplier fails to execute an order within thirty days or within the agreed period, the consumer may cancel the agreement on giving seven days' written notice.

(3) Where a supplier is unable to perform under the agreement on the grounds that the goods or services ordered are unavailable, the supplier shall immediately notify the consumer of this fact and refund any payments immediately.

Application of foreign law

68. The protection provided to consumers in this Part applies irrespective of the legal system applicable to the agreement in question.

Non-exclusion

69. A provision in an agreement which excludes a right provided for in this Part is void to the extent of the exclusion.

Complaints to Authority

70. (1) A consumer may lodge a complaint with the Authority in respect of any non-compliance with the provisions of this Part by a supplier.

(2) The Authority may investigate and determine any complaint in accordance with this Act and any other applicable written law.

(3) The Authority shall, in managing consumer complaints, have the power to—

(a) carry out market surveys to determine consumer demand and consumption trends;

(b) conduct quality of experience survey;

(c) monitor the information and communications technology sector for possible infringements of consumer rights not being reported to the Authority;

(d) hear a complaint and make a determination including the award of compensation in relation to the complaint;

(e) refer any complaints to a suitable body with appropriate recommendations; and

(f) implement mitigating strategies in instances where, there is a reoccurrence of similar complaints.

Directives, code of conduct and guidelines

71. (1) The Authority may issue—

(a) directives to address special circumstances, for children and vulnerable consumers;

(b) a code of conduct for licensees on consumer related matters; or

(c) guidelines on consumer related matters.

(2) The Authority shall collaborate with the Competition and Consumer Protection Commission on matters related to unfair trading.

PART IX
DOMAIN NAME REGULATION

Regulation of domain name

72. (1) The Authority shall—

(a) administer and manage the .zm domain name space;

(b) comply with international best practice in the administration of the .zm domain name space;

(c) licence and regulate registrars; and

(d) publish guidelines on–

(i) the general administration and management of the .zm domain name space; and

(ii) the requirements and procedures for domain name registration.

(2) The Authority shall enhance public awareness on the economic and commercial benefits of domain name registration.

(3) The Authority, in relation to domain name regulation—

(a) may conduct investigations that it may consider necessary;

(b) shall conduct research into, and keep abreast of, developments in the Republic and elsewhere on the domain name system; and

(c) shall continually survey and evaluate the extent to which the .zm domain name space meets the needs of the citizens of the Republic.

(4) The Authority may, and shall when so requested by the Minister, make recommendations to the Minister in relation to policy on any matter relating to the .zm domain name space.

(5) The Authority shall continually evaluate the effectiveness and the management of the .zm domain name space.

(6) The Authority may—

(a) liaise, consult and cooperate with any person or other authority; and

(b) appoint experts and other consultants on conditions that the Authority may determine.

(7) The Authority may delegate any of its functions under this Part to a person or institution that the Authority may determine.

(8) The Authority shall, in relation to the .zm domain name space existing prior to the commencement of this Act, uphold the vested rights and interests of parties involved in the management and administration of the .zm domain name space at the date of its establishment.

(9) Despite subsection (8)—

(a) the parties shall be granted a period of six months during which they may continue to operate in respect of their existing delegated sub domains; and

(b) after the expiry of the sixmonth period, the parties shall apply to be licensed registrars and registries as provided for in this Part.

Licensing of registers and registries

73. (1) A person shall not update a registry or administer a licensing of second level domain unless the person is licensed to do so by the Authority.

(2) A person who intends to update a registry or administer a licensing of a second level domain as a registrar or registry shall apply to the Authority in the prescribed manner on payment of the prescribed fee.

(3) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

Regulations regarding registrars, etc.

74. The Minister may, in consultation with the Authority, by statutory instrument, make regulations to provide for—

(a) the requirements which registrars shall meet in order to be licensed, including standards relating to operational accuracy, stability, robustness and efficiency;

(b) the circumstances and manner in which registrations may be assigned, transferred, registered, renewed, refused, or revoked by the registry;

(c) the pricing policy;

(d) the provisions for the restoration of a domain name registration and penalties for late payments;

(e) the terms of the domain name registration agreement which registrars shall adopt and use in registering domain names, including issues in respect of privacy, consumer protection and alternative dispute resolution;

(f) the processes and procedures to avoid unfair and anticompetitive practices, including bias to, or preferential treatment of actual or prospective registrants, registries or registrars, protocols or products;

(g) the requirements to ensure that each domain name contains an administrative and technical contact;

(h) the creation of new subdomains;

(i) licensing fees;

(j) the procedures for ensuring the monitoring of compliance with the provisions of this Act, including regular .zm domain name space technical audits; and

(k) any other matter relating to the .zm domain name space as may be necessary to achieve the objectives of this Part.

PART X
LIMITATION OF LIABILITY OF SERVICE PROVIDER

Definition

75. In this Part, "service provider" means a person providing an information system service.

No liability for mere conduit

76. (1) A service provider is not liable for providing access to, or for operating facilities for, information systems or transmitting, routing or storage of data messages through an information system under the service provider's control, as long as the service provider

(a) does not initiate the transmission;

(b) does not select the addressee;

(c) performs the functions in an automatic, technical manner without selection of the data; and

(d) does not modify the data contained in the transmission.

(2) The acts of transmission, routing and provision of access under subsection (1), include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place

(a) for the sole purpose of carrying out the transmission in the information system;

(b) in a manner that makes it inaccessible to any person other than anticipated recipients; and

(c) for a period no longer than is reasonably necessary for the transmission.

Caching

77. A service provider that transmits data provided by a recipient of the service through an information system under the service provider's control shall not be liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing that data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider—

(a) does not modify the data;

(b) complies with conditions on access to the data; and

(c) removes or disables access to the data stored on receiving a takedown notice under section 81.

(2) Despite this section, a court may order a service provider to terminate or prevent any unlawful activities under this Act or any other law.

Hyperlink provider

78. An internet service provider who enables the access to information provided by a third person by providing an electronic hyperlink shall not be liable for the information where—

(a) the internet service provider expeditiously removes or disables access to the information after receiving an order from any court to remove the link; or

(b) the internet service provider, on obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a public authority, expeditiously informs the relevant authority to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.

Hosting

79. (1) A service provider that provides a hosting service , is not liable for damages arising from data stored at the request of the recipient of the service, as long as 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 recipient or a third party;

(b) is not aware of facts or circumstances from which the

infringing activity or the infringing nature of the data message is apparent; and

(c) on receipt of a takedown notification referred to in section 99, acts expeditiously to remove or to disable access to the data.

(2) The limitations on liability established by this section do not apply to a service provider unless the service provider has designated an agent to receive notifications of infringement and has provided through the service provider's services, including the websites in locations accessible to the public, the name, address, phone number and email address of the agent.

(3) Subsection (1) does not apply where the recipient of the service is acting under the authority or the control of the service provider.

Order by court to terminate illegal activity

80. Despite other provisions of this Act, a court may order a service provider to terminate or prevent any unlawful activities under this Act or any other written law.

Use of information location tools by service provider

81. (1) A service provider is not liable for any damage incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, and where 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 that person;

(b) is not aware of 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; and

(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 that data message, infringes the rights of a person.

Take-down notification

82. (1) A recipient of a service or any person whose rights have been affected may, through a take-down notification, in writing, notify the service provider of—

(a) any data or activity infringing the rights of the recipient or of a third party;

(b) any unlawful material or activity; or

(c) any other matter conducted or provided contrary to the provisions of this Act.

(2) Where a service provider receives a takedown notification under subsection (1), the service provider shall, as soon as practicable, take down the infringing data, activity or material.

(3) A dispute regarding a takedown notification may be referred to the Authority for determination.

(4) A takedown notification to a service provider or that service provider's designated agent shall include—

(a) the full names and address of the complainant;

(b) a signature of the complainant;

(c) the right that has allegedly been infringed;

(d) an identification of the material or activity that is claimed to be the subject of unlawful activity;

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

(f) the telephonic and electronic contact details, if any, of the complainant;

(g) a statement that the complainant is acting in good faith; and

(h) a statement by the complainant that the information in the take down notification is, based on the complainant's knowledge, true and correct.

(5) A person who lodges a false takedown notification with a service provider commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

No general obligation on service provider to monitor unlawful activities

83. (1) Subject to the other provisions of this Part, a service provider is not under any obligation to—

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

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

(2) The Minister may, on the advice of the Authority, by statutory instrument, prescribe procedures for service providers to—

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

(b) communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

Savings

84. This Part does not affect—

(a) the obligation of a service provider acting under a licensing or other regulatory system established by, or under, any written law;

(b) any obligation imposed by any written law or by a court, to remove, block or deny access to any data message; or

Cap. 1

(c) any right to limitation of liability based on the Constitution.

PART XI
ENCRYPTING COMMUNICATION

Use of encrypted communication

85. A person providing an encryption service shall use an encryption, regardless of encryption algorithm selected, encryption key length chosen, or implementation technique or medium used, in the manner provided for under this Act.

No limitation on encryption function

86. Nothing in this Act shall be construed as requiring the use by a person of any form of encryption that—

(a) limits or affects the ability of the person to use encryption without a key escrow function; or

(b) limits or affects the ability of the person who uses encryption with a key escrow function not to use a key holder.

Prohibition of unauthorised decryption or release of decryption key

87. (1) Unless otherwise provided in this Act, a person shall not release a decryption key or decrypt any data without authorisation.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, in the case of—

(a) an advanced electronic signature private key, to imprisonment for a minimum term of ten years and a maximum period not exceeding twentyfive years without the option of a fine;

(b) any other electronic signature, to imprisonment for a term not exceeding ten years without the option of a fine.

(3) A key holder may release a decryption key or decrypt any data or communication—

(a) with the approval of the person whose key is held or managed by the key holder or the owner of the data or communication;

(b) where the release of the decryption key or decryption of the data or communication is necessary or incidental to the provision of encryption services or to the holding or management of the key by the key holder; or

(c) to assist a law enforcement officer pursuant to an interception order issued by a court to access transactional records or stored data.

(4) A law enforcement officer to whom a key is released under subsection (3) shall use the key in the manner and for the purpose and duration provided for under an interception and communications court order authorising the release and use and shall not exceed the duration of the electronic surveillance for which the key is released.

(5) A law enforcement officer to whom a decryption key is released shall, on or before the completion of the authorised release period, destroy the decryption key.

Prohibition of disclosure of record or other information by key holder

88. (1) A key holder shall not disclose a record or any other personal information relating to an owner of a key held or managed by the key holder except—

(a) with the consent of the owner; or

(b) to a law enforcement officer pursuant to a court order.

(2) A recovery agent shall not disclose to any person the use of any stored recovery information, any decrypted data or communication or other assistance provided to a law enforcement officer in the performance of functions under this Act.

(3) A person who contravenes subsection (1) or (2) commits an offence and is liable, on conviction, to imprisonment for a term of not less than fifteen years but not exceeding twentyfive years without an option of a fine.

(4) A recovery agent may decrypt any data or communication in the recovery agent's possession, custody or control, where the applicable law otherwise requires the recovery agent to provide the data or communication to a law enforcement officer in plain text or other form readily understood by the law enforcement officer—

(a) using or disclosing plain text in the recovery agent's possession, custody or control;

(b) using or disclosing recovery information that is not stored recovery information held by the recovery agent under the circumstances described in this Act; or

(c) using stored recovery information in the recovery agent's possession, custody or control.

Obstruction of law enforcement officer

89. A person who uses an encryption to obstruct or impede a law enforcement officer or in any manner interferes with the performance by the law enforcement officer of any functions under this Act commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

Prohibition of disclosure or use of stored recovery information Act No. of 2020

90. (1) A recovery agent shall implement technical and organisational measures to comply with the Data Protection Act, 2020 and shall not—

(a) disclose stored recovery information; or

(b) use stored recovery information to decrypt any data or communication.

(2) A person shall not access any stored recovery information from a recovery agent without authorisation.

(3) A recovery agent may disclose stored recovery information or use stored recovery information to decrypt any data or communication with the consent of the person who stored the recovery information or the agent of that person or pursuant to a court order.

Immunity of recovery agents

91. A cause of action shall not lie in any court against a recovery agent for providing information, facilities or assistance to a law enforcement officer in accordance with the terms of a court order.

PART XII

General Provisions

Appeals

92. (1) A person aggrieved by a decision of the Authority may, within thirty days of the decision, appeal to the Minister.

(2) The Minister may, in considering an appeal, set aside, vary or uphold the Authority's decision and shall, in writing, communicate the decision to the appellant.

(3) A person aggrieved by a decision of the Minister may, appeal to the High Court.

(4) A licensee or service provider aggrieved with a decision of the Authority may within, thirty days of the decision, appeal to the Tribunal established under the Information and Communications Technologies Act, 2009.

Act No. 15 of 2009

(5) A licensee or service provider aggrieved with a decision of the Tribunal shall appeal to the High Court.

Register

93. (1) The Authority shall establish and maintain a Register under this Act in which the Authority shall enter names and other details relating to—

(a) licensed and private certification authorities;

(b) timestamping service providers;

(c) cryptography service providers;

(d) applications rejected by the Authority and the reasons thereof; and

(e) any other information that the Authority considers necessary for purposes of this Act.

(2) The Register under subsection (1), shall be kept at a place that the Authority may determine, and shall be open for inspection by the public during normal working hours.

Offence by body corporate or unincorporate body

94. Where an offence under this Act is committed by a body corporate or unincorporated body, with the knowledge, consent or connivance of the director, manager, shareholder or partner, that director, manager, shareholder or partner of the body corporate or unincorporated body commits an offence and is liable, on conviction, to the penalty specified for that offence.

General penalty

95. A person who commits an offence under this Act for which no penalty is provided is liable, on conviction—

(a) in the case of an individual, to a penalty not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both; or

(b) in the case of a body corporate or un incorporate body to a penalty not exceeding one million penalty units.

Evidence obtained by unlawful interception not admissible in criminal proceedings

96. Despite any other written law, evidence which is obtained by means of an interception effected in contravention of this Act, is not admissible in any criminal proceedings except with the leave of the court, and in granting or refusing such leave, the court shall have regard, among other things, to the circumstances in which it was obtained, the potential effect of its admission or exclusion on issues of national security and the unfairness to the accused person that may be occasioned by its admission or exclusion.

Guidelines

97. (1) The Authority shall issue guidelines and publish them on electronic platforms, in a daily newspaper of general circulation in the Republic and in the Gazette, and the guidelines shall not take effect until they are so published.

(2) The guidelines issued by the authority under this Act shall bind all persons regulated under this act.

(3) A person who contravenes or fails to comply with a provision of a guideline or decision issued by the authority under this Act, commits an offence and is liable, on conviction, for each such breach, to a fine not exceeding fifty thousand penalty unit or to imprisonment for a period not exceeding six months, or to both, and forty thousand penalty units for each day of continued default.

Supervision of compliance with Act

98. The Authority shall supervise the compliance with the provisions of this Act.

Regulations

99. The Minister may, on the recommendation of the Authority, by statutory instrument, make regulations prescribing matters which by this Act are required or permitted to be prescribed.

Extraterritorial application of offences

100. (1) Subject to subsection (2), this Act shall have effect in relation to any person, whatever the person's nationality or citizenship, outside as well as within the Republic, where an offence under this Act is committed by a person in any place outside the Republic, the person shall be dealt with as if the offence had been committed within the Republic.

(2) For purposes of subsection (1), this Act shall apply to the offence where the—

(a) accused was in the Republic at the material time;

(b) computer, program or data was in the Republic at the material time; or

(c) damage occurred within the Republic whether or not paragraph (a) or (b) applies.

Act to bind Republic

101. This Act binds the Republic.

Repeal of Act No. 21 of 2009

102. (1) The Electronic Communications and Transactions Act, 2009 is repealed.

(2) Despite subsection (1), any legal proceedings commenced or pending under the repealed Act shall continue as if instituted under this Act.

This printed impression has been carefully compared by me with the Bill which has passed the National Assembly, and found by me to be a true and correctly printed copy of the said Bill.

Signed.....

Speaker/Deputy Speaker/

Clerk of the National Assembly

Date of Authentication: