CONSOLIDATED TO 31 DECEMBER 2015

LAWS OF SEYCHELLES

ELECTRONIC TRANSACTIONS ACT, 2001

[20th December, 2001]

Act 8 of 2001
S.I. 38 of 2001

ARRANGEMENT OF SECTIONS

PART I – PRELIMINARY

Short title and application

1. (1) This Act may be cited as the Electronic Transactions Act, 2001.

(2) [Commencement – omitted as spent.]

(3) Nothing in this Act shall apply to the documents and transactions specified in the schedule to this Act.

Interpretation

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

"access" means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network;

"addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

"affixing digital signature" means adoption of any procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

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

"Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 26 or a foreign certifying authority recognised under section 22;

"certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

"computer" means any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;

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

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

(b) terminals or a complex consisting of two or more interconnected computers;

"computer resource" means computer, computer system, computer network, data, computer database or software;

“computer system” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, and data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

“Controller” means the Controller of Certifying Authorities appointed under section 16(1);

“data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

“digital signature” means the authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with section 3;

“Digital Signature Certificate” means a Digital Signature Certificate issued under section 34;

“electronic form” with reference to information means any information generated, sent, received or stored in any computer storage media such as magnetic, optical, computer memory or other similar devices;

“electronic record” means data, record or data generated, image or sound store, received or sent in an electronic form;

“function”, in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

“information” includes data, text, images, sound, codes, and databases;

“intermediary”, with respect to any particular electronic message, means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

“law” includes any instrument that has the force of law and any unwritten rule of law;

“key pair”, in an asymmetric crypto system, means a private key and it’s mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

“licence” means a licence granted to a Certifying Authority under section 26;

“originator” means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

“prescribed” means prescribed by regulation made under this Act;

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

“Public Authority” means a Ministry, department, division or agency of the Government or a statutory corporation or a limited liability company which is directly or ultimately under the

control of the Government or any other body which is carrying out a governmental function or service or a body or person specified by an Act;

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

"secure system" means computer hardware, software and procedure that —

(a) are reasonably secure from intrusion and misuse;

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

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

"security procedure" means the security procedure prescribed under section 15;

"subscriber" means a person in whose name the Digital Signature Certificate is issued;

"verify" in relation to a digital signature, electronic record or public key, means to determine whether —

(a) the initial electronic record was affixed with the digital signature by the use of the private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

PART II – DIGITAL SIGNATURE

Authentication of electronic records

3. (1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of an electronic record shall be effected by the use of an asymmetric crypto system and hash function. For the purposes of this subsection, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible —

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber may verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

PART III – ELECTRONIC GOVERNANCE

Legal recognition of electronic records

4. Where any law provides that information or any other matter shall be in writing then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is —

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

Legal recognition of digital signature

5. Where any law provides that information or any other matter shall be authenticated by affixing the signature or any documents should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by means of the digital signature affixed in such manner as may be prescribed.

Use of electronic records and digital signatures in Public Authorities

6. (1) Where any law provides for —

(a) the filing of any form, application or any other document with any Public Authority in a particular manner;

(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner;

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed.

(2) The Minister may, for the purposes of subsection (1), prescribe —

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fee or charge for filing, creating or issuing any electronic record under paragraph (a).

Retention of electronic records

7. (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form if —

(a) the information contained therein remains accessible so as to be usable for a 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 represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record;

Provided that this paragraph does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Sections 6, 7 not to confer right to insist document should be accepted in electronic form

8. Nothing contained in sections 6 and 7 shall confer a right upon any person to insist that any Public Authority should accept, issue, create, retain or preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

Power to make regulations in respect of digital signature

9. The Minister may, for the purposes of this Act, make regulations prescribing —

(a) the type of digital signature;

(b) the manner and format in which the digital signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the digital signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to digital signatures.

PART IV – ATTRIBUTION, ACKNOWLEDGEMENT AND DISPATCH OF ELECTRONIC RECORDS

Attribution of electronic records

10. An electronic record shall be attributed to the originator if it was sent —

(a) by the originator himself;

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

(c) by an information system programmed by or on behalf of the originator to operate automatically.

Acknowledgement of receipt

11. (1) Where the originator has not agreed with the addressee that the acknowledgement be in a particular form or by a particular method, an acknowledgement may be given by ——

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

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

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement of such electronic record by him, then unless acknowledgement has been so received, the electronic record shall be deemed not to have been sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement must be received by him and if no acknowledgement is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

Time and place of dispatch and receipt of electronic records

12. (1) Save as otherwise agreed between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely —

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records —

(i) receipt occurs at the time when the electronic record enters the designated computer resource; or

(ii)if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of subsection (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under subsection (3).

(5) For the purpose of this section —

(a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

PART V – SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

Secure electronic record

13. Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Secure digital signature

14. If by application of a security procedure agreed to by the parties concerned it can be verified that a digital signature, at the time it was affixed, was —

(a) unique to the subscriber affixing it;

(b) capable of identifying such subscriber; and

(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated,

then such digital signature shall be deemed to be a secure digital signature.

Security procedure

15. The Minister shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure is used, including —

(a) the nature of the transaction;

(b) the level of sophistication of the parties with reference to their technological capacity;

(c) the volume of similar transactions engaged in by other parties;

(d) the availability of alternatives offered to but rejected by any party;

(e) the cost of alternative procedures; and

(f) the procedures in general use for similar types of transactions or communications.

PART VI – REGULATION OF CERTIFYING AUTHORITIES

Appointment of Controller and other officers

16. (1) The Minister may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and such number of Deputy Controllers and Assistant Controllers as the Minister deems fit.

(2) The Controller shall discharge the functions of the Controller under this Act subject to the general control and directions of the Minister.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

Functions of Controller

17. The Controller may perform all or any of the following functions, namely —

(a) exercising supervision over the activities of the Certifying Authorities;

(b) laying down the standards to be maintained by the Certifying Authorities;

(c) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(d) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(e) specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect to a Digital Signature Certificate and the public key;

(f) specifying the form and content of a Digital Signature Certificate and the public key;

(g) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(h) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(i) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and the regulation of such system;

(j) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(k) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(l) laying down the duties of the Certifying Authorities;

(m) maintaining a data-base containing a disclosure record in respect of every Certifying Authority containing such particulars as may be specified by regulations, which record shall be accessible to the public.

Controller to act as repository

18. (1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall —

(a) make use of hardware and procedures that are secure from intrusion and misuse;

(b) observe such other standards as may be prescribed to ensure that the secrecy and security of digital signatures are assured.

(3) The Controller shall maintain a computerised data base of all public keys in such a manner that the data base and the public keys are available to any member of the public.

Power to delegate

19. The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any other officer to exercise any of the powers of the Controller under this Part

Power to investigate contraventions

20. The Controller or any officer authorised by him in that behalf may investigate any contravention of the provisions of this Act or regulations made thereunder.

Access to computers and data

21. (1) The Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of subsection (1), the Controller or any person authorised by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data, apparatus or material, to provide the Controller or the person authorised with such reasonable technical and other assistance as he may consider necessary.

Recognition of foreign Certifying Authorities

22. (1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may, with the previous approval of the Minister and by notification in the Official Gazette, recognise any foreign Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under subsection (1), the Digital Signature Certificates issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under subsection (1), for

reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

Licence to issue Digital Signature Certificates

23. (1) Subject to the provisions of subsection (2), any person may make an application to the Controller for a licence to issue Digital Signature Certificates.

(2) No licence shall be granted unless the applicant fulfils such requirements with respect to qualifications, expertise, manpower, financial resources and other infrastructure facilities as may be prescribed by regulations.

(3) A licence granted under this section shall —

(a) be valid for such period as may be prescribed;

(b) not be transferable or heritable;

(c) be subject to such terms and conditions as may be prescribed.

Application for licence

24. (1) Every application for a licence shall be in prescribed form.

(2) Every such application shall be accompanied by —

(a) a certification practice statement;

(b) a statement outlining the procedures with respect to identification of the applicant;

(c) proof of payment of such fee as may be prescribed;

(d) such other documents as may be prescribed.

Renewal of licence

25. An application for renewal of a licence shall be–

(a) in the prescribed form; and

(b) accompanied by such fee as may be prescribed, and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence:

Provided that an application for renewal of licence made after the expiry of the licence may be entertained on payment of such late fee as may be prescribed.

Procedure for grant or rejection of licence

26. The Controller may, on receipt of an application under section 23(1), after considering the documents accompanying the application and such other matters as he deems fit, grant the licence or reject the application:

Provided that no application shall be rejected under this section unless the applicant has been

given a reasonable opportunity of presenting his case.

Revocation of licence

27. (1) The Controller may, if he is satisfied after making such inquiry as he may think fit that a Certifying Authority has —

(a) made in, or in relation to, the application for the issue or renewal of the licence, a statement which is incorrect or false in a material particular;

(b) failed to comply with the terms and conditions subject to which the licence was granted;

(c) failed to maintain standards prescribed under section 18(2)(b);

(d) has contravened any provisions of this Act or any regulation made thereunder,

revoke the licence after giving the Certifying Authority a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any grounds for revoking a licence under subsection (1), by order suspend such licence pending the completion of any inquiry ordered by him:

Provided that, no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose licence has been suspended shall issue any Digital Signature Certificate during the period of suspension.

Notice of suspension or revocation of licence

28. (1) Where the licence of a Certifying Authority is suspended or revoked, the Controller shall publish a notice of such suspension or revocation, as the case may be, in the data-base maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish the notice of such suspension or revocation, as the case may be, in all such repositories.

Certifying Authority to follow certain procedures

29. Every Certifying Authority shall —

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services;

(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(d) observe such other standards as may be prescribed.

Certifying Authority to ensure compliance with the Act, etc

30. Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of that person's employment or engagement, with the provisions of this Act and regulations made thereunder.

Display of licence

31. Every Certifying Authority shall display its licence in a conspicuous place at the premises in which it carries on its business.

Surrender of licence

32. Every Certifying Authority whose licence is suspended or revoked shall, immediately after such suspension or revocation, surrender the licence to the Controller:

Disclosure

33. (1) Every Certifying Authority shall disclose in the manner specified by regulations —

(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate which that Certifying Authority has issued, or the Certifying Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then the Certifying Authority shall —

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in the certification practice statement to deal with such event or situation.

PART VII – DIGITAL SIGNATURE CERTIFICATES

Certifying Authority to issue Digital Signature Certificate

34. (1) Any person may make an application to any Certifying Authority for the issue of a Digital Signature Certificate.

(2) Every such application shall be accompanied by such fee as may be prescribed.

(3) Every such application shall be accompanied by a certification practice statement or, where there is no such statement, a statement containing such particulars as may be prescribed.

(4) On receipt of an application under subsection (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under subsection (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or, for reasons to be recorded in writing, reject the application:

Provided that, no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

(5) No Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that —

(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key which is capable of creating a digital signature;

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

Representations upon issuance of Digital Signature Certificate

35. A Certifying Authority while issuing a Digital Signature Certificate shall certify that —

(a) it has complied with the provisions of this Act and regulations made thereunder;

(b) it has published the Digital Signature Certificate or otherwise made it available to persons relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate;

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

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact which, if it had been included in the Digital Signature Certificate, would adversely affect the reliability of the representations made under paragraphs (a) to (d).

Suspension of Digital Signature Certificate

36. (1) Subject to the provisions of subsection (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate —

(a) on receipt of a request to that effect from –

(i) the subscriber listed in the Digital Signature Certificate; or

(ii) any person duly authorised to act on behalf of that subscriber;

(b) if it is of opinion that the Digital Signature Certificate should be suspended in the public interest.

(2) A Digital Signature should not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) The Certifying Authority shall communicate any suspension of a Digital Signature Certificate under this section to the subscriber.

Revocation of Digital Signature Certificate

37. (1) A Certifying Authority shall revoke a Digital Signature Certificate issued by it —

(a) where the subscriber or any other person authorised by the subscriber so requests; or

(b) upon the death of the subscriber; or

(c) where the subscriber is a firm or a company, upon the dissolution of the firm or winding up of the company as the case may be.

(2)Subject to the provisions of subsection (3), a Certifying Authority may revoke a Digital Signature Certificate issued by it at any time if it is of opinion that —

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the reliability of the Digital Signature Certificate;

(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, it has been dissolved, wound-up or otherwise has ceased to exit.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) The Certifying Authority shall communicate any revocation of a Digital Signature Certificate under this section to the subscriber.

Notice of suspension or revocation

38. Where a Digital Signature Certificate is suspended or revoked under section 36 or section 37, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository or repositories specified in the Digital Signature Certificate for publication of such notice.

PART VIII – DUTIES OF SUBSCRIBERS

Generating key pair

39. Where any Digital Signature Certificate, the public key of which corresponds to the private

key of the subscriber which is to be listed in the Digital Signature Certificate has been accepted by the subscriber, then the subscriber shall generate the key pair by applying the security procedure.

Acceptance of Digital Signature Certificate

40. (1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate —

(a) to one or more persons;

(b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that —

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificates are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true

Control of private key

41. (1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in the Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then the subscriber shall communicate the same without any delay to the Certifying Authority.

PART IX – OFFENCES

Tampering with computer source document

42. Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be guilty of an offence and liable on conviction to imprisonment for three years and a fine of R20, 000. For the purposes of this section, "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Penalty for failure to furnish information, return etc

43. If any person who is required, under this Act or any regulation made thereunder to —

(a) furnish any document, return or report to Controller or to the Certifying Authority

fails to furnish the same, he shall be guilty of an offence and shall on conviction be liable to a fine not exceeding R10,000 for each such failure;

(b) file any return or furnish any information, book or other document within the time specified therefor in the regulations fails to file the return or furnish the same within the time specified therefor in the regulations, he shall be guilty of an offence and liable on conviction to a fine not exceeding R1000 for every day during which such failure continues;

(c) maintain books of account or records, fails to maintain the same, he shall be liable to a fine not exceeding R10,000.

Power of the Controller to give directions

44. (1) The Controller may, by order, direct a Certifying Authority to take such measures or cease carrying on such activities as specified in the order to ensure compliance with the provisions of this Act or any regulations made thereunder.

(2) Any person who fails to comply with any order under subsection (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for three years and to a fine not exceeding R20,000.

Supreme Court may order interception

45. (1) If the Supreme Court is satisfied on application being made that it is necessary or expedient so to do in the interest of the sovereignty or the security of the Republic, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognisable offence, the Court may, for reasons to be recorded in writing by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person in charge of the computer resources shall, when called upon by any agency which has been directed under subsection (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in subsection (2) shall be guilty of an offence and liable to imprisonment for seven years.

Protected system

46. (1) The Controller may, by notification in the Official Gazette, declare that any computer, computer system or computer network is a protected system.

(2) The Controller may, by order in writing, authorise the persons who may access a protected system notified under subsection (1).

(3) Any person who secures access or attempts to secure access to a protected system without being authorised under this section shall be guilty of an offence and liable to imprisonment for two years and to a fine of R10,000.

Penalty for misrepresentation

47. Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may

be, shall be guilty of an offence and liable to imprisonment for two years and to a fine of R10,000.

Penalty for breach of confidentiality and privacy

48. Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of the powers conferred under this Act or regulations made thereunder, secures access to any electronic record, book, register, correspondence, information, document or other material and without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be guilty of an offence and liable to imprisonment for five years and to a fine of R10,000.

Penalty for publishing Digital Signature Certificate false in certain particulars

49. (1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that —

(a) the Certifying Authority listed it the certificate has not issued it; or

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

(c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of subsection (1) shall be guilty of an offence and liable on conviction to imprisonment for two years and to a fine of R10,000.

Publication for fraudulent purpose

50. Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be guilty of an offence and liable on conviction to imprisonment for two years and to a fine of R10,000 or to both such imprisonment and fine.

Act to apply to offences outside Seychelles

51. (1) Subject to the provisions of subsection (2), the provisions of this Act shall apply also to any offence committed outside Seychelles by any person irrespective of the person's nationality.

(2) For the purposes of subsection (1), this Act shall apply to an offence committed outside Seychelles by any person if the act or conduct constituting the offence involves a computer, computer system or computer network located in Seychelles.

Forfeiture

52. Any computer, computer system, floppies, compact discs, tape drives or any other accessories related thereto, in respect of which any provision of the Act or regulations made thereunder has been contravened, shall be liable to forfeiture:

Provided that where it is established to the satisfaction of the Court that the person in whose possession, power or control any such computer, computer system, floppies, compact discs, tape drives or any other accessories relating thereto are found is not responsible for the contravention of

the provisions of this Act or regulations made thereunder, the Court may, instead of making an order for forfeiture of such computer, computer system, floppies, compact discs, tape drives or any other accessories related thereto, make such order authorised by this Act against the person contravening the provisions of this Act or regulations made thereunder, as it may think fit.

PART X – MISCELLANEOUS

Network service providers not liable in certain cases

53. For the removal of doubt, it is hereby declared that no person providing service as a network service provider shall be liable under this Act or regulations made thereunder for any third party information or data made available by him if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

Protection of action taken in good faith

54. No suit, prosecution or other legal proceeding shall lie against the Government, the Controller or any person acting on behalf of the Controller for anything which is in good faith done or intended to be done in pursuance of this Act or any regulation made thereunder.

Constitution of Advisory Committee

55. (1) The Minister shall appoint an Advisory Committee for the purpose of this Act.

(2) The Advisory Committee shall consist of a Chairman and such number of other official members and other members representing the interests principally affected or having special knowledge of the subject matter, as the Minister may deem fit.

(3) The Advisory Committee shall advise the Minister –

(a) either generally or as regards any matter that may be referred to it by the Minister for advice;

(b) in framing regulations under this Act;

(4) There shall be paid to the members of the Advisory Committee such travelling and other allowances as the Minister may determine.

Power of Minister to make regulations

56. (1) The Minister may, after consultation with the Controller and the Advisory Committee, make regulations to carry out the purposes of this Act.

(2) The Minister may, by regulation, amend the Schedule to this Act.

SCHEDULE

Section 1(3)

(a) A negotiable instrument as defined in section 3 of the Bills of Exchange Act;

(b) A power-of-attorney referred to in section 70 of the Lands Registration Act;

(c) A will referred to in Article 971 of the Civil Code of Seychelles;

(d) Any contract for the sale or conveyance of immovable property;

(e) Any such class of documents or transactions as may be prescribed.

NO SUBSIDIARY LEGISLATION
