ELECTRONIC TRANSACTIONS ACT*

Act 23 of 2000 – 1 August 2001
(*unless otherwise indicated*)

ARRANGEMENT OF SECTIONS

*Parts I to V, VII to IX, XI, XIII and section 41 have come into operation by virtue of Proclamation 7 of 2001.

SECTION

ELECTRONIC TRANSACTIONS ACT

PART I — PRELIMINARY

1. Short title

This Act may be cited as the Electronic Transactions Act.

2. Interpretation

In this Act—

"asymmetric cryptosystem" 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;

"authorised officer" means the person designated as such under section 25 of the Information and Communication Technologies Act;

"automated transaction" means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction;

"certificate" means a 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;

"certification authority" means a person duly authorised under this Act to issue a certificate;

"certification practice statement" means a statement issued by a certification authority to specify the practices that the certification authority employs in issuing certificates;

"Controller" means the Controller of Certification Authorities referred to in section 37;

"correspond", in relation to a private key or public key, means to belong to the same key pair;

"digital signature"—

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

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

(ii) whether the initial electronic record has been altered since the transformation was made; and

(b) includes voice recognition features, digital finger-printing or such other biotechnology features or process, as may be prescribed;

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

"electronic agent" means a computer programme or an electronic or other automated means used to initiate an action or response to electronic records or performances in whole or in part without review or action by an individual;

"electronic record" means a record created, generated, sent, communicated, received or stored by electronic means;

"electronic signature" means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record;

"ICT Authority" means the Information and Communication Technologies Authority established under the Information and Communication Technologies Act;

"information" means data, text, images, sounds, codes, computer programmes, software, databases, or the like;

"information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information;

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

"licensed certification authority" means a certification authority licensed by the Controller;

"Minister" means the Minister to whom responsibility for the subject of information technology is assigned;

"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 sector agency" includes any Ministry or Government Department, local authority or statutory body;

"record" means information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form;

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

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

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

(b) detecting error or alteration in the communication, content or storage of an electronic record since a specific point in time,

which may require the use of algorithms or codes, identifying words or numbers, encryption, answerback or acknowledgement procedures, or similar security devices;

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

"transaction" means an action or set of actions relating to the conduct of business, commercial, or public sector activities and occurring between 2 or more persons;

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

(a) are reasonably secure from intrusion or misuse;

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

(c) are reasonably suitable for performing their intended functions; and

(d) adhere to generally accepted security procedures;

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

(a) the digital signature was created using the private key corresponding to the public key listed in the certificate; and

(b) the record has not been altered since its digital signature was created.

[S. 2 amended by s. 3 of Act 7 of 2009 w.e.f. 15 July 2009.]

3. Objects of Act

The objects of this Act are to—

(a) establish the legal infrastructure necessary to implement secure electronic commerce and to remove uncertainties over writing and signature requirements;

(b) regulate electronic commerce and other electronic transactions by means of secure and reliable electronic records;

(c) provide for electronic filing of documents with public sector agencies and promote efficient delivery of public sector services by means of reliable electronic records;

(d) foster the development of electronic commerce through the use of electronic signatures;

(e) establish the authenticity and integrity of correspondence in any electronic medium;

(f) help establish uniformity or rules, regulations and standards regarding the authentication and integrity of electronic records;

(g) prevent the incidence of forged electronic records and fraud in electronic commerce and other electronic transactions; and

(h) promote public confidence in the integrity and reliability of electronic records and electronic commerce.

4. Application of Act

(1) Subject to subsections (2) and (3), this Act shall apply to electronic records and electronic signatures relating to a transaction or an automated transaction.

(2) Parts II and IV shall not apply to any enactment requiring writing or signatures in writing in—

(a) the creation or execution of a will;

(b) a negotiable instrument;

(c) a power of attorney;

(d) a contract for the sale or other disposition of immovable property, or any interest in such property;

(e) the conveyance of immovable property or the transfer of any interest in immovable property;

(f) a document of title; or

(g) such other document or instrument as may be prescribed.

(3) Any provision of Part II or IV may be varied by agreement between the parties involved in creating, generating, sending, receiving, storing or otherwise processing or using electronic records.

PART II — ELECTRONIC RECORDS AND SIGNATURES

5. Legal recognition of electronic records

No record or signature shall be denied legal effect, validity or enforceability solely on the ground that it is in electronic form.

6. Requirement for writing

Where an enactment requires any information or record to be in writing, that requirement shall be satisfied by an electronic record where the information contained therein is accessible so as to be usable for subsequent reference.

7. Electronic records

(1) Where an enactment requires that records, documents or information be kept, that requirement shall be satisfied where the records, documents or information are kept in the form of an electronic record in accordance with this section.

(2) An electronic record shall be kept—

(a) so that the information contained therein remains accessible so as to be usable for subsequent reference;

(b) 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) so that such information, if any, as enables the identification of the origin and destination of the electronic record and the date and time when it was sent or received, is preserved; and

(d) so that the consent of the public sector agency which has supervision over the requirement for the keeping of such records is obtained.

(3) An obligation to keep records, documents or information in accordance with subsection (2) (c) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.

(4) A person may satisfy the requirements referred to in subsection (2) by using the services of any other person.

(5) Nothing in this section shall—

(a) apply to an enactment which expressly provides for the keeping of records, documents or information in the form of an electronic record; or

(b) preclude any public sector agency from specifying additional requirements for the retention of electronic records that are subject to the supervision of the public sector agency.

8. Electronic signatures

Where any enactment requires a signature, or provides for certain consequences if a document is not signed, an electronic signature shall satisfy that requirement.

PART III — LIABILITY OF NETWORK SERVICE PROVIDERS

9. Liability of network service providers

(1) Subject to subsection (2), a network service provider shall not be subject to any civil or criminal liability in respect of third-party material in the form of an electronic record to which he merely provides access where such liability is limited to—

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

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

(2) Nothing in this section shall affect—

(a) an obligation founded on contract;

(b) the obligation of a network service provider as such under a licensing or other regulatory regime established under any enactment; or

(c) any obligation imposed under any enactment or by a Court to remove, block or deny access to any material.

(3) For the purposes of this section—

"provide access", in relation to third-party material—

(a) means provide the necessary technical means by which third-party material may be accessed; and

(b) includes the automatic and temporary storage of the third-party material for the purpose of providing access;

"third-party", in relation to a network service provider, means a person over whom the provider has no effective control.

PART IV — ELECTRONIC CONTRACTS

10. Validity of contracts

No contract shall be denied legal effect, validity or enforceability solely on the ground that an electronic record was used in its formation.

11. Declaration of intent

No declaration of intent or other similar statement between the originator and the addressee of an electronic record shall be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

12. Attribution of electronic record and signature

(1) An electronic record or electronic signature shall be attributable to a person where it was the act of that person.

(2) The act of a person referred to in subsection (1) may be shown in the manner set out in this section which includes the proper application of any security procedure to determine the person to whom the electronic record or electronic signature is attributable.

(3) An electronic record shall be deemed to be that of the originator where it was sent—

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

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

(4) Subject to subsection (5), an addressee is entitled to regard an electronic record as being that of the originator and to act on that assumption where—

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

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

(5) Subsection (4) shall not apply—

(a) from the time when the addressee has both received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly;

(b) in a case referred to in subsection (4) (b), at any time when the addressee knew or ought to have known, had it exercised reasonable care or used any agreed procedure, that the electronic record was not that of the originator; or

(c) where, in all the circumstances of the case, there are reasonable grounds for the addressee to regard the electronic record as that of the originator or to act on that assumption.

(6) Subject to subsection (7), where an electronic record is that of the originator or is deemed to be that of the originator, or where the addressee is entitled to act on that assumption, the addressee shall be entitled to regard the electronic record received as being what the originator intended to send, and to act on that assumption.

(7) The addressee shall not be entitled to regard the electronic record received as being what the originator intended to send where the addressee knew or ought to have known, had the addressee exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the electronic record as received.

(8) The addressee shall be entitled to regard each electronic record received as a separate electronic record and to act on that assumption, except to the extent that the addressee duplicates another electronic record and the addressee knew or ought to have known, had the addressee exercised reasonable care or used any agreed procedure, that the electronic record was a duplicate.

13. Acknowledgement of receipt

(1) Subsections (2), (3) and (4) shall apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or has agreed with the addressee that receipt of the electronic record be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given 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.

(3) Where the originator has stated that an electronic record is conditional on receipt of the acknowledgement, the electronic record shall be treated as though it had never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that an electronic record is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, where no time has been specified or agreed within a reasonable time, the originator—

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) where the acknowledgement is not received within the time specified in paragraph (a), may, upon notice to the addressee, treat the electronic record as though it has never been sent or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed, unless evidence to the contrary is adduced, that the related electronic record was received by the addressee, but that presumption does not imply that the content of the electronic record corresponds to the content of the record received.

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

(7) Except in so far as it relates to the sending or receipt of the electronic record, this Part is not intended to deal with the legal consequences that may flow either from that electronic record or from the acknowledgement of its receipt.

14. Time and place of sending and receipt

(1) Unless otherwise agreed between the originator and the addressee, an electronic record is sent when it enters an information processing system outside the control of the originator or the person who sent the electronic record on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall—

(a) where the addressee has designated an information processing system for the purpose of receiving an electronic record, occur—

(i) at the time when the electronic record enters the designated information processing system; or

(ii) where the electronic record is sent to an information processing system of the addressee that is not the designated information processing system, at the time when the electronic record is retrieved by the addressee; or

(b) where the addressee has not designated an information processing system, occur when the electronic record enters an information processing system that the addressee uses for the purpose of receiving electronic records or information of the type sent from which the addressee is able to retrieve the electronic record or information.

(3) Subsection (2) shall apply notwithstanding that the place where the information processing system is located may be different from the place where the electronic record is deemed to be received under subsection (4).

(4) Unless otherwise agreed between the originator and the addressee, an electronic record is deemed to be sent from 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.

(5) For the purposes of this section—

(a) where the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;

(b) where the originator or the addressee does not have a place of business, reference is to be made to the usual place of residence; and

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

PART V — SECURE ELECTRONIC RECORDS AND SIGNATURES

15. Secure electronic records

(1) Where a prescribed security procedure, or a commercially reasonable security procedure agreed to by the parties involved, has been properly applied to an electronic record to verify that the electronic record has not been altered since a specified point in time, the record shall be treated as a secure electronic record from such specified point in time to the time of verification.

(2) For the purposes of this section and section 16, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including—

(a) the nature of the transaction;

(b) the sophistication of the parties;

(c) the volume of similar transactions engaged in by either or all 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.

16. Secure electronic signatures

Where, in the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made—

(a) unique to the person using it;

(b) capable of identifying such person;

(c) created in a manner or using a means under the sole control of the person using it; and

(d) linked to the electronic record to which it relates in a manner such that had the record been changed, the electronic signature would be invalidated,

the signature shall be treated as a secure electronic signature.

17. Presumptions relating to secure electronic records and signatures

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

(2) In any proceedings involving a secure electronic signature, it shall be presumed, unless evidence to the contrary is adduced, that—

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

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

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

(4) For the purposes of this section—

"secure electronic record" means an electronic record treated as a secure electronic record by virtue of section 15 or 18;

"secure electronic signature" means an electronic signature treated as a secure electronic signature by virtue of section 16 or 19.

PART VI — EFFECT OF DIGITAL SIGNATURES

(Part VI came into operation on 1 December 2010.)

18. Secure electronic records with digital signatures

Where a digital signature is a secure electronic signature by virtue of section 19, the portion of an electronic record that is signed with a digital signature shall be treated as a secure electronic record.

(S. 18 came into operation on 1 December 2010.)

19. Secure digital signatures

Where any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the record, where—

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

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

(i) the certificate was issued by a licensed certification authority;

(ii) the certificate was issued by a certification authority outside Mauritius recognised for this purpose by the Controller;

(iii) the certificate was issued by a public sector agency approved by the Minister to act as a certification authority on such conditions as he may impose; or

(iv) the originator and the addressee have expressly agreed to use a digital signature as a security procedure, and the digital signature was properly verified by reference to the public key of the originator.

(S. 19 came into operation on 1 December 2010.)

20. Presumptions regarding certificates

It shall be presumed, unless evidence to the contrary is adduced, that any information, other than information identified as subscribed information which has not been verified, set out in a certificate issued by a licensed certification authority and accepted by the subscriber, is correct.

(S. 20 came into operation on 1 December 2010.)

21. Unreliable digital signatures

Unless otherwise provided for in any enactment or agreement, a person relying on a digitally signed electronic record shall assume the risk that the digital signature is invalid as a signature or authentication of the signed electronic record, where reliance on the digital signature is not reasonable under the circumstances having regard to—

(a) any fact which the person relying on the digitally signed electronic record knows or has notice of, including a fact set out in the certificate or incorporated in it by reference;

(b) the value or importance of the digitally signed electronic record, if known;

(c) the course of dealing between the person relying on the digitally signed electronic record and the subscriber and any available indication of reliability or unreliability other than the digital signature; and

(d) any usage of trade, particularly trade conducted by trustworthy systems or other electronic means.

(S. 21 came into operation on 1 December 2010.)

PART VII — OBLIGATIONS RELATING TO DIGITAL SIGNATURES

22. Reliance on certificates

Any person relying on a digital signature shall also rely on a valid certificate containing the public key by which the digital signature can be verified.

23. Prerequisites to publication of certificates

No person shall publish a certificate or otherwise make it available to a person known by that person to be in a position to rely on the certificate or on a digital signature that is verifiable with reference to a public key listed in the certificate, where that person knows that—

(a) the certification authority referred to in the certificate has not issued it;

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

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

PART VIII — OBLIGATIONS OF CERTIFICATION AUTHORITIES

24. Trustworthy system

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

25. Disclosure

(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, hereafter referred to as a certification authority certificate;

(b) any certification practice statement;

(c) notice of the revocation or suspension of its certification authority 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 certification authority certificate, the certification authority shall—

(a) notify any person who is known to be or foreseeably will be affected by that occurrence; or

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

26. Issuing of certificate

(1) A certification authority may only issue a certificate to a prospective subscriber where it has—

(a) received a request to that effect from the prospective subscriber; and

(b) complied with—

(i) where it has a certification practice statement, all the practices and procedures set forth in the certification practice statement including procedures regarding identification of the prospective subscriber; or

(ii) in the absence of a certification practice statement, the conditions in subsection (2).

(2) In the absence of a certification practice statement, the certification authority may only issue a certificate to a prospective subscriber where it has ascertained that—

(a) the prospective subscriber is the person to be referred to in the certificate to be issued;

(b) where the prospective subscriber is acting through an agent, the subscriber authorised the agent to have custody of the subscriber's private key and to request the issue of a certificate setting out the corresponding public key;

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

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

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

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

27. Representations on issue of certificate

(1) A certification authority shall, by the issue of a certification, represent to a person who reasonably relies on the certificate or a digital signature verifiable by the public key referred to in the certificate that the certification authority has issued the certificate in accordance with any certification practice statement incorporated by reference in the certificate or of which the relying person has notice.

(2) In the absence of any certification practice statement, the certification authority shall, subject to subsection (3), represent that—

(a) it has complied with all applicable requirements of this Act in issuing the certificate, and where it has published the certificate or otherwise made it available to a person relying on it that the subscriber referred to in the certificate has accepted it;

(b) the subscriber identified in the certificate holds the private key corresponding to the public key referred to in the certificate;

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

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

(e) it has no knowledge of any material fact which would, if it had been included in the certificate, adversely affect the reliability of the representations in paragraphs (a) to (d).

(3) Where there is a certification practice statement which has been incorporated by reference in the certificate, or of which the person relying on it has notice, subsection (2) shall apply to the extent that the representations are not inconsistent with the certification practice statement.

28. Suspension of certificate

A certification authority shall, unless it has otherwise agreed with the subscriber, immediately suspend a certificate which it has issued to the subscriber upon a request by—

(a) the subscriber referred to in the certificate; or

(b) a person duly authorised to act on behalf of the subscriber.

29. Revocation of certificate

A certification authority shall revoke a certificate upon receiving a request to the effect by the subscriber referred to in the certificate after confirming that the person making the request is the subscriber, or is an agent of the subscriber with authority to make the request.

30. Revocation without subscriber's consent

(1) A certification authority shall, without the consent of the subscriber, revoke a certificate where—

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

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

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

(d) an individual subscriber is dead; or

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

(2) The certification authority shall immediately notify the subscriber referred to in the revoked certificate of any revocation under subsection (1) (a), (b) or (c).

31. Notice of suspension

(1) A certification authority shall, upon the suspension of a certificate, forthwith publish a notice of the suspension in the repository specified in the certificate for the purpose.

(2) Where more than one repository is specified, the certification authority shall publish notices of the suspension in every repository.

32. Notice of revocation

(1) The certification authority shall, upon revocation of a certificate, forthwith publish a notice of the revocation in the repository specified in the certificate for the purpose.

(2) Where more than one repository is specified, the certification authority shall publish notices of the revocation in every repository.

PART IX — OBLIGATIONS OF SUBSCRIBERS

33. Generating key pair

(1) Subject to subsection (2), where a subscriber generates a key pair of which the public key is to be set out in a certificate and accepted by the subscriber, the subscriber shall generate the key pair using a trustworthy system.

(2) Subsection (1) shall not apply to a subscriber who generates a key pair using a system approved by a certification authority.

34. Acceptance of certificate

(1) A subscriber shall be deemed to have accepted a certificate where he—

(a) publishes or authorises the publication of the certificate—

(i) to any other person; or

(ii) in a repository; or

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

(2) A subscriber referred to in a certificate shall, by accepting a certificate, certify to any person who may rely on the information contained in the certificate that—

(a) he rightfully holds the private key corresponding to the public key referred to in the certificate;

(b) every representation made by him to the certification authority which is material to the information set out in the certificate are true; and

(c) all information in the certificate that is within his knowledge is true.

35. Control of private key

(1) A subscriber identified in a certificate shall, on accepting a certificate—

(a) exercise reasonable care to retain control of the private key corresponding to the public key referred to in the certificate; and

(b) prevent its disclosure.

(2) Subsection (1) shall continue to apply during—

(a) the operational period of the certificate; and

(b) any period of suspension of the certificate.

36. Initiating suspension or revocation

Where the private key corresponding to the public key referred to in a certificate has been compromised or otherwise becomes unreliable, a subscriber who has accepted the certificate shall forthwith request the relevant certification authority to suspend or revoke the certificate.

PART X — REGULATION OF CERTIFICATION AUTHORITIES

(Part X came into operation on 1 December 2010.)

37. Controller of Certification Authorities

(1) There shall be for the purposes of this Act a Controller of Certification Authorities.

(2) For the purposes of the Act, the ICT Authority shall be the Controller and may be assisted by such of its officers and other members of its staff as may be necessary.

(3) The Controller shall maintain a publicly accessible database containing a certification authority disclosure record for each licensed certification authority which shall contain such particulars as may be prescribed.

(4) In the application of this Act to certificates issued by the Controller and to digital signatures verified by reference to those certificates, the Controller shall be deemed to be a licensed certification authority.

[S. 37 amended by s. 4 of Act No. 7 of 2009 w.e.f. 1 December 2010.]

(S. 37 came into operation on 1 December 2010.)

38. Recommended reliance limit

(1) A licensed certification authority shall, where it issues a certificate to a subscriber, specify a recommended reliance limit in the certificate.

(2) The licensed certification authority may specify different limits in different certificates.

(S. 38 came into operation on 1 December 2010.)

39. Liability limits for licensed certification authorities

A licensed certification authority shall not be liable—

(a) for any loss caused by reliance on a false or forged digital signature of a subscriber, where it has acted in compliance with the requirements of this Act relating thereto;

(b) in excess of the amount specified in the certificate as its recommended reliance limit for—

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

(ii) failure to comply with sections 26 and 27 in issuing the certificate.

(S. 39 came into operation on 1 December 2010.)

PART XI — PUBLIC SECTOR USE OF ELECTRONIC RECORDS AND SIGNATURES

40. Acceptance of electronic filing and issue of documents

(1) A public sector agency which pursuant to any enactment—

(a) accepts the filing of documents, or requires that documents be created, kept or issued;

(b) issues any notice, claim, licence, permit, authorisation or approval;

(c) provides for any payment and the method and manner of such payment; or

(d) has to keep records,

may, notwithstanding anything to the contrary in the enactment—

(i) accept the filing of such documents, or the creation or keeping of such documents in electronic form;

(ii) issue such notice, claim, licence, permit, authorisation or approval in electronic form;

(iii) make and receive such payment in electronic form; or

(iv) convert written records into electronic records.

(2) Where a public sector agency decides to perform any of the functions referred to in subsection (1) (i), (ii) or (iii), it may specify—

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

(b) where the electronic records have to be signed, the type of electronic signature required including, where applicable, a requirement that the sender uses a digital signature or other electronic signature;

(c) the manner and format in which the signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any certification authority used by the person filing or issuing the document;

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

(e) any other required attributes for electronic records or payments that are currently specified for corresponding paper documents.

[S. 40 amended by s. 9 of Act 27 of 2012 w.e.f. 22 December 2012.]

PART XII — ADMINISTRATION

41. Confidentiality

(1) No person who has, pursuant to any power conferred under this Part, obtained access to an electronic record, book, register, correspondence, information, document or other material shall disclose such electronic record, book, register, correspondence, information, document or other material to any other person except for the purposes of this Act or pursuant to an order made by the Judge in Chambers.

(2) The Judge shall not make an order of disclosure under subsection (1) unless he is satisfied that—

(a) the applicant is acting in the discharge of his duties;

(b) the information is material to any judicial proceedings; or

(c) the disclosure is otherwise necessary in all the circumstances.

42. Authorised officer

(1) The Controller may in writing delegate any of his powers under this Part to an authorised officer.

(2) In exercising any of the powers of enforcement under this Act, an authorised officer shall, on demand, produce to the person against whom he is acting the authority issued to him by the Controller.

(S. 42 came into operation on 1 December 2010.)

[S. 42 amended by s. 5 of Act No. 7 of 2009 w.e.f. 1 December 2010.]

43. Directions by Controller

The Controller may, for the purposes of ensuring compliance with this Act, by notice in writing, direct a certification authority to take such measures or cease such activities as may be necessary.

(S. 43 came into operation on 1 December 2010.)

44. Production of documents and data

The Controller or an authorised officer may—

(a) require the production of records, accounts, data and documents kept by a certification authority and inspect, examine and take copies of any of them;

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

(c) make such inquiry as may be necessary to ascertain whether this Act has been complied with; and

(d) retain, for such period as he considers necessary, any record, account, data or document specified in paragraph (a) or (b).

(S. 44 came into operation on 1 December 2010.)

45. Power of access to computers and data

(1) Subject to subsection (2), the Controller or an authorised officer may, at all reasonable times, enter any business premises or place where any business is carried on or anything is done in connection with the business and—

(a) (i) have access to and inspect and check the operation of any computer system and any associated apparatus or material which he has reasonable cause to suspect is or has been in use;

(ii) use or cause to be used any such computer system to search any data contained in or available to such computer system; or

(b) require—

(i) the person by whom or on whose behalf the Controller or authorised officer has reasonable cause to suspect the computer system is or has been so used; or

(ii) any person having charge of, or otherwise concerned with the operation of, the computer system, apparatus or material, to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph (a).

(2) Subsection (1) shall not apply to any person who carries on any banking business regulated by the Banking Act or the Bank of Mauritius Act.

(S. 45 came into operation on 1 December 2010.)

46. Warrant to search and seize

(1) Subject to subsection (2), where the Controller has reasonable ground to believe that an offence has been, is being or is likely to be committed under this Act, he may apply to a District Magistrate for the issue of a warrant to an authorised officer to—

(a) enter and search any business premises or place where any business is carried on or anything is done in connection with the business;

(b) inspect or examine any equipment, apparatus, material, record, document or other information, whether kept on computer or otherwise, found therein; and

(c) seize any such equipment, apparatus, material, record, document or other information, where such seizure is necessary for any examination or investigation.

(2) Subsection (1) shall not apply to any person referred to in section 45 (2).

(3) Any equipment, apparatus, material, record, document or other information seized under subsection (1) (c) shall be returned to the person from whom they were seized when no longer required.

(S. 42 came into operation on 1 December 2010.)

46A. Police assistance

The Controller or an authorised officer may, for the purposes of this Act, make use of the services of a police officer who shall assist the Controller or authorised officer, as the case may be.

[S. 46A inserted by s. 6 of Act No. 7 of 2009 w.e.f. 1 December 2010.]

(S. 46A came into operation on 1 December 2010.)

PART XIII — MISCELLANEOUS

47. Offences

(1) Any person who, knowingly and with intent to defraud, creates, publishes or otherwise makes available a certificate in breach of section 23, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years.

(2) Any person who knowingly misrepresents to a certification authority his identity or authorisation for the purpose of requesting for a certificate or for suspension or revocation of a certificate, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years.

(3) Any subscriber who, for the purposes of obtaining a certificate—

(a) makes any inaccurate or incomplete statement;

(b) gives any incorrect or false information; or

(c) makes any material misrepresentation,

to a certification authority shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 12 months.

(4) Any person who contravenes section 41 shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 12 months.

(5) Any person who fails to comply with any direction under section 43 shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 12 months.

(6) Any person who obstructs the lawful exercise of the powers of the Controller or any authorised officer under section 45 (1) (a) or who fails to comply with a request under section 45 (1) (b) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 12 months.

(7) Any person who obstructs, impedes, assaults or interferes with the Controller or any authorised officer in the performance of his functions under this Act shall commit an offence.

(8) Any person who otherwise contravenes any other provision of this Act shall commit an offence.

(9) Any person who commits an offence in respect of which no penalty is provided shall, on conviction, be liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 6 months.

48. Consent of Director of Public Prosecutions

No prosecution in respect of an offence under this Act shall be instituted except with the consent of the Director of Public Prosecutions.

49. Jurisdiction

Notwithstanding any other enactment, the Intermediate Court shall have jurisdiction to try an offence under this Act and may impose any penalty provided in this Act including forfeiture.

50. Regulations

(1) The Minister may make such regulations as he thinks fit for the purposes of this Act.

(2) Regulations made under subsection (1) may provide for—

(a) the regulating and licensing of certification authorities;

(b) the securing of digital signatures and electronic signatures;

(c) applications for licences or renewal of licences of certification authorities and their authorised representatives and matters incidental thereto;

(d) the activities of certification authorities including the manner, method and place of soliciting business, the conduct of such solicitation and the prohibition of such solicitation of members of the public by certification authorities which are not licensed;

(e) the standards to be maintained by certification authorities;

(f) the appropriate standards with respect to the qualifications, experience and training of applicants for any licence or their employees;

(g) the conditions for the conduct of any of its activities and for certification practice statement by a certification authority;

(h) the content and distribution of written, printed, electronic or visual material and advertisements that may be distributed or used by a person in respect of a digital certificate or key;

(i) the form and content of a digital certificate or key;

(j) the particulars to be recorded in, or in respect of, accounts kept by certification authorities;

(k) the appointment and remuneration of an auditor appointed and for the costs of an audit;

(l) the establishment and regulation of any electronic system by a certification authority, whether by itself or in conjunction with other certification authorities, and for the imposition and variation of such requirements, conditions or restrictions as may be imposed by the Controller;

(m) the manner in which a holder of a licence conducts its dealings with its customers, conflicts of interest involving the holder of a licence and its customers, and the duties of a holder of a licence to its customers with respect to digital certificates;

(n) the recognition of a certification authority outside Mauritius that satisfies the requirements—

(i) for the recommended reliance limit, specified in a certificate issued by the certification authority; and

(ii) referred to in section 19;

(o) ensuring the quality of repositories and the services they provide including provisions for the standards, licensing or accreditation of repositories;

(p) giving effect to the obligations of Mauritius under any international treaty, convention or agreement save and to the extent that these regulations are not inconsistent with this Act;

(q) the levying of fees and for the taking of charges.

(3) Any regulations made under this section may provide that any person who contravenes them shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 6 months.

51. – 53. —