LAWS OF BRUNEI

CHAPTER 196
ELECTRONIC TRANSACTIONS ACT

S 93/00

REVISED EDITION 2008

B.L.R.O. 4/2008

LAWS OF BRUNEI

REVISED EDITION 2007

CHAPTER 197

ELECTRONIC TRANSACTIONS

ARRANGEMENT OF SECTIONS

Section

PART III

LIABILITY OF NETWORK SERVICE PROVIDERS

PART IV

ELECTRONIC CONTRACTS

PART V

SECURE ELECTRONIC RECORDS AND SIGNATURES

PART VI

EFFECT OF DIGITAL SIGNATURES

PART VII

GENERAL DUTIES RELATING TO DIGITAL SIGNATURES

PART VIII

DUTIES OF CERTIFICATION AUTHORITIES

PART IX

DUTIES OF SUBSCRIBERS

ELECTRONIC TRANSACTIONS ACT

An Act to make provision for the security and use of electronic transactions and for connected purposes

Commencement (except Part X): 1st May 2001
[S 40/01]

PART I

PRELIMINARY

Citation.

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

(2) The Minister may, with the approval of His Majesty the Sultan and Yang Di-Pertuan, by notification in the *Gazette*, appoint different dates for the commencement of different provisions of this Act and for different purposes of the same provision.

Interpretation.

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

"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;

"certification authority" means a person who or an organisation that issues 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 appointed under section 41(1) and includes a Deputy or an Assistant Controller of Certification Authorities appointed under section 41(2);

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

"data message" means information generated, sent, received or stored by electronic, optical or similar means, including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

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

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

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

"electronic record" means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another;

"electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record;

"hash function" means an algorithm mapping or translating one sequence of bits into another, generally smaller, set (the hash result) such that —

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

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

(c) it is computationally infeasible that 2 records can be found that produce the same hash result using the algorithm;

"information" includes data, text, images, sound, codes, computer programs, software and databases;

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

"key pair", in an asymmetric cryptosystem, 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 pursuant to regulations made under section 42;

"Minister" means the Minister of Finance;

"operational period of a certificate" begins on the date and time the certificate is issued by a certification authority (or on any later date and time stated in the certificate), and ends on the date and time it expires as stated in the certificate or when it is earlier revoked or suspended;

"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;

"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;

"revoke a certificate" means to permanently end the operational period of a certificate from a specified time;

"rule of law" includes a written law;

"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;

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

"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;

"suspend a certificate" means to temporarily suspend the operational period of a certificate from a specified time;

"transaction" includes a transaction of a non-commercial nature;

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

(a) are reasonably secure from intrusion and misuse;

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

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

(d) adhere to generally accepted security procedures;

"valid certificate" means a certificate that a certification authority has issued and which the subscriber listed in it has accepted;

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

(a) that 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.

Purposes and construction.

3. (1) This Act shall be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes —

(a) to facilitate electronic communications by means of reliable electronic records;

(b) to facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

(c) to facilitate electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of reliable electronic records;

(d) to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;

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

(f) to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

(2) In the interpretation of this Act, regard is to be had to its international origin and the need to promote uniformity in its application and the observance of good faith.

(3) Questions concerning matters governed by this Act which are not expressly settled in it are to be settled in conformity with the general principles on which this Act is based.

Application.

4. (1) Parts II or IV shall not apply to any rule of law requiring writing or signatures in any of the following matters —

(a) the creation of any legal instrument or document under any written law relating to Islamic law;

(b) the creation or execution of a will under any written law relating wills;

(c) negotiable instruments;

(d) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts;

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

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

(g) documents of title relating to immovable property.

(2) The Minister may, with the approval of His Majesty the Sultan and Yang Di-Pertuan, by order in the *Gazette* modify the provisions of subsection (1) by adding, deleting or amending any class of transactions or matters mentioned therein.

Variation by agreement.

5. As between parties involved in generating, sending, receiving, storing or otherwise processing electronic records, any provision of Parts II or IV may be varied by agreement.

PART II

ELECTRONIC RECORDS AND SIGNATURES GENERALLY

Legal recognition of electronic records.

6. For the avoidance of doubt, it is hereby declared that information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

Requirement for writing.

7. Where any rule of law requires information to be written in writing to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule of law if the information contained therein is accessible so as to be usable for subsequent reference.

Electronic signatures.

8. (1) Where any rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.

Retention of electronic records.

9. (1) Where any rule of law requires that certain documents, records or information be retained, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied —

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

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

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

(d) the consent of the department or ministry of the Government, organ of State, or the statutory corporation which has supervision over the requirement for the retention of such records has been obtained.

(2) An obligation to retain documents, records or information in accordance with subsection (1)*(c)* shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in subsections (1)*(a)* to *(d)* are complied with.

(4) Nothing in this section shall —

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

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

PART III

LIABILITY OF NETWORK SERVICE PROVIDERS

Liability of network service providers.

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

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

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

(2) Nothing in this section shall affect —

(a) any obligation founded on contract;

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

(c) any obligation imposed under any written law or by a court to remove, block or deny access to any material.

(3) For the purposes of this section —

"providing access", in relation to third-party material, means the provision of the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access;

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

PART IV

ELECTRONIC CONTRACTS

Formation and validity.

11. (1) For the avoidance of doubt, it is hereby declared that in the context of the formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic records.

(2) Where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose.

Effectiveness between parties.

12. As between the originator and the addressee of an electronic record, a declaration of intent or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

Attribution.

13. (1) An electronic record is that of the originator if it was sent by the originator himself.

(2) As between the originator and the addressee, an electronic record is deemed to be that of the originator if 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 system programmed by or on behalf of the originator to operate automatically.

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

(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 electronic records as its own.

(4) Subsection (3) 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 within subsection (3)*(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) if in all the circumstances of the case, it is unconscionable for the addressee to regard the electronic record as that of the originator or to act on that assumption.

(5) Where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the electronic record received as being what the originator intended to send, and to act on that assumption.

(6) The addressee is not so entitled when the addressee knew or should 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.

(7) The addressee is 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 should have known, had the addressee exercised reasonable care or used any agreed procedure, that the electronic record was a duplicate.

(8) Nothing in this section shall affect the law of agency or the law on the formation of contracts.

Acknowledgement of receipt.

14. (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 the 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 the 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, if 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) if 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 meets 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.

Time and place of dispatch and receipt.

15. (1) Unless otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters an information system outside the control of the originator or the 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 is determined as follows —

(a) if the addressee has designated an information system for the purpose of receiving electronic records, receipt occurs —

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

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

(b) if the addressee has not designated such an information system, receipt occurs when the electronic record enters an information system of the addressee.

(3) Subsection (2) shall apply notwithstanding that the place where the information 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 dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business.

(5) For the purposes of this section —

(a) if 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) if 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 constituted.

(6) This section shall not apply to such circumstances as the Minister may by regulations prescribe.

PART V

SECURE ELECTRONIC RECORDS AND SIGNATURES

Secure electronic record.

16. (1) If 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, such 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 of section 17, 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.

Secure electronic signature.

17. If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that all 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 if the record was changed the electronic signature would be invalidated,

such signature shall be treated as a secure electronic signature.

Presumptions relating to secure electronic records and signatures.

18. (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 with 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 sections 16 or 19;

"secure electronic signature" means an electronic signature treated as a secure electronic signature by virtue of sections 17 or 20.

PART VI

EFFECT OF DIGITAL SIGNATURES

Secure electronic record with digital signature.

19. The portion of an electronic record that is signed with a digital signature shall be treated as a secure electronic record if the digital signature is a secure electronic signature by virtue of section 20.

Secure digital signature.

20. When 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 if —

(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 because —

(i) the certificate was issued by a licensed certification authority operating in compliance with the regulations made under section 42;

(ii) the certificate was issued by a certification authority outside Brunei Darussalam recognised for this purpose by the Controller pursuant to requirements made under section 43;

(iii) the certificate was issued by a department or ministry of the Government, an organ of State or a statutory body or corporation approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or

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

Presumptions regarding certificates.

21. It shall be presumed, unless evidence to the contrary is adduced, that the information listed in a certificate issued by a licensed certification authority is correct, except for information identified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.

Unreliable digital signatures.

22. Unless otherwise provided by any rule of law or by contract, a person relying on a digitally signed electronic record assumes the risk that the digital signature is invalid as a signature or authentication of the signed electronic record, if reliance on the digital signature is not reasonable under the circumstances having regard to the following factors —

(a) facts which the person relying on the digitally signed electronic record knows or has notice of, including all facts listed in the certificate or incorporated in it by reference;

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

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

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

PART VII

GENERAL DUTIES RELATING TO DIGITAL SIGNATURES

Reliance on certificates forseeable.

23. It is foreseeable that persons relying on a digital signature will also rely on a valid certificate containing the public key by which the digital signature can be verified.

Prerequisites to publication of certificate.

24. No person shall publish a certificate or otherwise make it available to a person known by that first-mentioned 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, if that first-mentioned person knows that —

(a) the certification authority listed 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 such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

Publication for fraudulent purpose.

25. Any person who knowingly creates, publishes or otherwise makes available a certificate for any fraudulent or unlawful purpose shall be guilty of an offence and be liable on conviction to a fine not exceeding $20,000, imprisonment for a term not exceeding 2 years or both.

False or unauthorised request.

26. 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 be guilty of an offence and be liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 6 months or both.

PART VIII

DUTIES OF CERTIFICATION AUTHORITIES

Trustworthy system.

27. A certification authority must utilise trustworthy systems in performing its services.

Disclosure.

28. (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 (referred to in this section as a certification authority certificate);

(b) any relevant 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 perform its services.

(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) use reasonable efforts to 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.

Issuing of certificate.

29. (1) A certification authority may issue a certificate to a prospective subscriber only after the certification authority —

(a) has received a request for issuance from the prospective subscriber; and

(b) has —

(i) if it has a certification practice statement, complied with all of the practices and procedures set forth in such certification practice statement including procedures regarding identification of the perspective subscriber; or

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

(2) In the absence of a certification practice statement, the certification authority shall confirm by itself or through an authorised agent that —

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

(b) if the prospective subscriber is acting through one or more agents, the subscriber authorised the agent to have custody of the subscriber's private key and to request issuance of a certificate listing 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 listed in the certificate;

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

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

Representations upon issuance of certificate.

30. (1) By issuing a certificate, a certification authority represents, to any person who reasonably relies on the certificate or a digital signature verifiable by the public key listed in the certificate, that the certification authority has issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the certificate, or of which the relying person has notice.

(2) In the absence of such certification practice statement, the certification authority represents that it has confirmed that —

(a) the certification authority has complied with all applicable requirements of this Act in issuing the certificate, and if the certification authority has published the certificate or otherwise made it available to such relying person, that the subscriber listed in the certificate has accepted it;

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

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

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

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

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

Suspension of certificate.

31. Unless the certification authority and the subscriber agree otherwise, the certification authority that issued a certificate shall suspend the certificate as soon as possible after receiving a request by a person whom the certification authority believes to be —

(a) the subscriber named in the certificate;

(b) a person duly authorised to act for that subscriber; or

(c) a person acting on behalf of that subscriber, who is unavailable.

Revocation of certificate.

32. A certification authority shall revoke a certificate that is issued after —

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

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

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

Revocation without subscriber's consent.

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

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

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

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

(d) an individual subscriber is dead; or

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

(2) Upon effecting such a revocation, other than under subsections (1)*(a)* or *(e)*, the certification authority shall immediately notify the subscriber named in the revoked certificate.

Notice of suspension.

34. (1) Immediately upon suspension of a certificate by a certification authority, the certification authority shall publish a signed notice of the suspension in the repository specified in the certificate for publication of notice of suspension.

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

Notice of revocation.

35. (1) Immediately upon revocation of a certificate by a certification authority, the certification authority shall publish a signed notice of the revocation in the repository specified in the certificate for publication of notice of revocation.

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

PART IX

DUTIES OF SUBSCRIBERS

Generating key pair.

36. (1) If the subscriber generates the key pair whose public key is to be listed in a certificate issued by a certification authority and accepted by the subscriber, the subscriber shall generate that key pair using a trustworthy system.

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

Obtaining certificate.

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

Acceptance of certificate.

38. (1) A subscriber shall be deemed to have accepted a certificate if he —

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

(i) to one or more persons; or

(ii) in a repository; or

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

(2) By accepting a certificate issued by himself or a certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that —

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

(b) all representations made by the subscriber to the certification authority and material to the information listed in the certificate are true; and

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

Control of private key.

39. (1) By accepting a certificate issued by a certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in such certificate and prevent its disclosure to a person not authorised to create the subscriber's digital signature.

(2) Such duty shall continue during the operational period of the certificate and during any period of suspension of the certificate.

Initiating suspension or revocation.

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

*PART X

REGULATION OF CERTIFICATION AUTHORITIES

Appointment of Controller and other officers.

41. (1) The Minister shall be the Controller of Certification Authorities for the purposes of this Act.

(2) The Minister may appoint such number of Deputy and Assistant Controllers of Certification Authorities and officers as he considers necessary to exercise and perform all or any of the powers and duties of the Controller under this Act or any regulations made thereunder.

(3) The Controller, the Deputy and Assistant Controllers and officers appointed under subsection (2) shall exercise, discharge and perform the powers, duties and functions conferred on the Controller under this Act or any regulations made thereunder, subject to such directions as may be issued by the Minister.

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

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

Regulation of certification authorities.

42. (1) The Minister may, with the approval of His Majesty the Sultan and Yang Di-Pertuan, make regulations for the regulation and licensing of certification authorities and to define when a digital signature qualifies as a secure electronic signature.

(2) Without prejudice to the generality of subsection (1), the Minister may make regulations for or with respect to —

* Part X has not commenced (S 40/01).

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

(b) 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 from members of the public by certification authorities which are not licensed;

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

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

(e) prescribing the conditions for the conduct of business by a certification authority;

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

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

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

(i) providing for the appointment and remuneration of an auditor appointed under the regulations and for the costs of an audit carried out under the regulations;

(j) providing for 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 the Controller may think fit;

(k) 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;

(l) prescribing any forms for the purposes of the regulations; and

(m) prescribing fees to be paid in respect of any matter or thing required for the purposes of this Act and the regulations.

(3) Regulations made under this section may provide that a contravention of a specified provisions shall be an offence and may provide for penalties for a fine not exceeding $50,000, imprisonment for a term not exceeding one year or both.

Recognition of foreign certification authorities.

43. The Minister may, by order published in the *Gazette,* recognise certification authorities outside Brunei Darussalam that satisfy the prescribed requirements for any of the following purposes —

(a) the recommended reliance limit, if any, specified in a certificate issued by the certification authority;

(b) the presumption referred to in sections 20*(b)*(ii) and 21.

Recommended reliance limit.

44. (1) A licensed certification authority shall, in issuing 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 as it considers fit.

Liability limits for licensed certification authorities.

45. Unless a licensed certification authority waives the application of this section, a licensed certification authority —

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

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

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

ii) failure to comply with sections 29 and 30 in issuing the certificate.

Regulation of repositories.

46. The Minister may, with the approval of His Majesty the Sultan and Yang Di-Pertuan, make regulations for the purpose of ensuring the quality of repositories and the services they provide, including provisions for the standards, licensing or accreditation of repositories.

PART XI

GOVERNMENT USE OF ELECTRONIC RECORDS AND SIGNATURES

Acceptance of electronic filing and issue of documents.

47. (1) Any department or ministry of the Government, organ of State or statutory body that, pursuant to any written law —

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

(b) issues any permit, licence or approval; or

(c) provides for the method and manner of payment,

may, notwithstanding anything to the contrary in such written law —

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

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

(iii) make such payment in electronic form.

(2) In any case where a department or ministry of the Government, organ of State or statutory body decides to perform any of the functions in subsections (1)(i), (ii) or (iii), it may specify —

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

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

(c) the manner and format in which such 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 the document;

(d) control processes and procedures as 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.

(3) Nothing in this Act shall by itself compel any department or ministry of the Government, organ of State or statutory body to accept or issue any document in the form of electronic records.

PART XII

GENERAL

Obligation of confidentiality.

48. (1) Except for the purposes of this Act or for any prosecution for an offence under any written law or pursuant to any order of court, no person who has, pursuant to any powers conferred under this Part, obtained access to any 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.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and be liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding one year or both.

Offences by bodies corporate.

49. Where an offence under this Act or any regulations made thereunder committed by a body corporate is proved to have committed with the consent or connivance of, or to be attributable to any act or default on the part of, any director, manager, secretary or other similar officer of that body corporate, or of any person purporting to act in any such capacity, he, as well as the body corporate, shall also be guilty of that offence and be liable to be proceeded against and punished accordingly.

Authorised officers or employees.

50. (1) The Controller may in writing authorise any officer or employee to exercise any of the powers of the Controller under this Part.

(2) Any such officer or employee shall be deemed to be a public servant for the purposes of the Penal Code (Chapter 22).

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

Controller may give directions for compliance.

51. (1) The Controller may by notice in writing direct a certification authority or any officer or employee thereof to take such measures or stop carrying on such activities as are specified in the notice if they are necessary to ensure compliance with the provisions of this Act or any regulations made thereunder.

(2) Any person who fails to comply with any direction specified in a notice issued under subsection (1) shall be guilty of an offence and be liable on conviction to a fine not exceeding $50,000, imprisonment for a term not exceeding one year or both.

Power to investigate.

52. (1) The Controller or an authorised officer or employee may investigate the activities of a certification authority in relation to its compliance with this Act and any regulations made thereunder.

(2) For the purposes of subsection (1), the Controller may in writing issue an order to a certification authority to further its investigation or to secure compliance with this Act or any regulations made thereunder.

Access to computers and data.

53. (1) The Controller or an authorised officer or employee shall —

(a) be entitled at any time to —

(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 in connection with any offence under this Act;

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

(b) be entitled to require —

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

(ii) any person having charge of, or otherwise concerned with the operation of, the computer, apparatus or material,

to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph *(a)*.

(2) Any person who obstructs the lawful exercise of the powers under subsection (1)*(a)* or who fails to comply with a request under subsection (1)*(b)* is guilty of an offence and liable on conviction to a fine not exceeding $20,000, imprisonment for a term not exceeding one year or both.

Obstruction of authorised officer or employee.

54. Any person who obstructs, impedes, assaults or interferes with the Controller or any authorised officer or employee in the performance of his functions under this Act shall be guilty of an offence.

Production of documents, data etc.

55. The Controller or an authorised officer or employee shall, for the purposes of the execution of this Act, have power to do all or any of the following —

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

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

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

General penalties.

56. Any person guilty of an offence under this Act or any regulations made thereunder for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding $20,000, imprisonment for a term not exceeding 6 months or both.

Sanction of Public Prosecutor.

57. No prosecution in respect of any offence under this Act or any regulations made thereunder shall be instituted except by or with the sanction of the Public Prosecutor.

Jurisdiction of courts.

58. A Court of a Magistrate shall have jurisdiction to hear and determine all offences under this Act and any regulations made thereunder and, notwithstanding anything to the contrary in any other written law, shall have power to impose the full penalty or punishment in respect of any such offence.

Composition of offences.

59. (1) The Controller may, in his discretion, compound any offence under this Act or any regulations made thereunder which is prescribed as

being an offence which may be compounded by collecting from any person reasonably suspected of having committed that offence a sum not exceeding $5,000.

(2) The Minister may, with the approval of His Majesty the Sultan and Yang Di-Pertuan, make regulations prescribing the offences which may be compounded under this Act.

Power to exempt.

60. Notwithstanding anything contained in this Act or in any other written law, the Minister may exempt, subject to such terms and conditions as he thinks fit, any person or classes of person from all or any of the provisions of this Act or any regulations made thereunder.

Regulations.

61. (1) The Minister may, with the approval of His Majesty the Sultan and Yang Di-Pertuan, make regulations to prescribe anything which is required to be prescribed under this Act and generally for the carrying out of the provisions of this Act.

(2) Any regulations made under this Act may make different provision for different cases or classes of case and for different purposes of the same provision.

Available from
The Attorney General's Chambers
The Law Building, Jalan Tutong
Bandar Seri Begawan BA1910
Brunei Darussalam

Printed by
The Government Printing Department
Brunei Darussalam

$10.00

ELECTRONIC TRANSACTIONS ACT
CHAPTER 196
2008 Edition