LAWS OF MALAYSIA

DIGITAL SIGNATURE ACT 1997 *[ACT 562]*

P.U.(A) 359/98

DIGITAL SIGNATURE REGULATIONS 1998

Publication : 1st October 1998
Date of coming into operation : 1st October 1998

ARRANGEMENT OF REGULATIONS

Preamble

IN exercise of the powers conferred by section 91 of the Digital Signature Act 1997 [Act 562], the Minister makes the following regulations:

PART I - PRELIMINARY

Regulation 1. Citation and commencement.

(1) These regulations may be cited as the **Digital Signature Regulations 1998.**

(2) These Regulations shall come into operation on 1 October 1998.

Regulation 2. Interpretation.

In these Regulations, unless the context otherwise requires -

"approved digital signature scheme" means a digital signature scheme approved under regulation 29;

"approved fee" means a fee or charge imposed by a licensed certification authority, a recognised repository and a recognised date/time stamp service under the Act and these Regulations that is approved by the Controller under regulations 40, 50 and 63 respectively;

"certified public accountant" means a public accountant registered under the Accountants Act 1967 *[Act 94]*;

"distinguished name" means a set of data that identifies a real-world entity, such as a person, in a computer-based context;

"hardware based" means in a token or smart card or other external device;

"hash function" means an algorithm mapping or translating one sequence of bits into another generally smaller set, known as the hash result, such that -

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

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

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

"hash result" means the output produced by a hash function upon processing a message;

"licensed" means to be issued with the operation stage of the licence;

"public-key algorithm" means an algorithm designed to create different signing and verification keys where the verification key can be made public and the signing key cannot in a reasonable amount of time be calculated from the verification key;

"qualified auditor" means a certified public accountant or an accredited computer security professional registered as a qualified auditor under regulation 41;

"qualified right to payment" means an award of damages against a licensed certification authority by a court having jurisdiction over the licensed certification authority in a civil action under the Act;

"recognised" means to be issued with the operation stage of the certificate of recognition;

"software based" means in the computer system or programmes;

"subliminal channel" means a channel within a digital signature that allows subliminal text to be sent within the digital signature;

"suitable guarantee" means a suitable guarantee under regulation 23.

Regulation 3. Forms.

The forms in the First Schedule are prescribed for use under these Regulations.

Regulation 4. Fees.

(1) The fees in the Second Schedule are prescribed for the purposes of these Regulations.

(2) The fees shall be paid to the Controller by such means and in such manner as the Controller may direct.

PART II - LICENSING OF CERTIFICATION AUTHORITIES

Regulation 5. Stages of licence.

(1) A licence to carry on or operate as a certification authority shall be issued in two stages, namely -

(a) the establishment stage; and

(b) the operation stage.

(2) No person shall carry on or operate, or hold himself out as carrying on or operating, as a licensed certification authority unless that person has been issued with the operation stage of the licence.

(3) A person who contravenes subregulation (2) shall be deemed to carry on or operate as a certification authority without a valid licence.

(4) The establishment stage of a licence may be issued for any period not exceeding one year.

(5) An application for a licence shall be deemed to be withdrawn and shall not be further proceeded with,

without prejudice to a fresh application being made by the applicant, if -

(a) the applicant fails to apply for the operation stage of the licence before the expiry of the period specified in subregulation (4); or

(b) on an application for the operation stage of the licence having duly been made within the period specified in subregulation (4), the applicant is not issued with the operation stage of the licence.

(6) Nothing in these Regulations shall be construed so as to require an applicant to apply for the establishment stage of a licence as a condition for applying for the operation stage of a licence if the applicant is otherwise able to satisfy the prescribed requirements to apply for the operation stage of a licence.

Regulation 6. Qualification requirements.

A person intending to carry on or operate as a certification authority shall satisfy the following requirements:

(a) it is a body corporate incorporated in Malaysia or a partnership within the meaning of the Partnership Act 1961 *[Act 135]*;

(b) it maintains a registered office in Malaysia;

(c) it has working capital reasonably sufficient, according to the requirements of the Controller, to enable it to carry on or operate as a certification authority;

(d) it files with the Controller a suitable guarantee;

(e) it uses a trustworthy system for the generation and management of key pairs and certificates;

(f) it uses an approved digital signature scheme for the generation of key pairs and for the creation and verification of digital signatures;

(g) it has an operating procedure that includes a certification practice statement, the measures to be taken to check the identity of subscribers to be listed in certificates, and the repositories and date/time stamp services to be used;

(h) it employs as operative personnel only persons who -

(i) have not been convicted within the past fifteen years of an offence involving fraud, false statement or deception; and

(ii) have demonstrated knowledge and proficiency in following the requirements of the Act and these Regulations;

(i) it complies with the licensing, standards and technical requirements under the Act and these Regulations; and

(j) it complies with such other requirements as the Controller thinks fit.

Regulation 7. Application for licence.

(1) An application for a licence shall be made in Form 1.

(2) If the applicant has more than one office, the applicant shall specify each of the offices in the application.

(3) An application under subregulation (1) shall be accompanied by -

(a) the information required under regulation 8 or 9, as the case may be;

(b) the prescribed fee; and

(c) such other information or document as the Controller may require.

(4) The Controller may, on an application for the operation stage of a licence, require the applicant to demonstrate any part of its operating procedure and may require independent testing of the software, hardware, technical components, algorithms, standards and other pertinent parameters and other equipment to be used by the applicant, at the applicant's expense, for the purpose of ascertaining its security and trustworthiness.

(5) If any information or document required under subregulation (3) is not provided by the applicant or any demonstration or test required under subregulation (4) is not complied with within the time specified in the requirement or any extension thereof granted by the Controller, the application shall be deemed to be withdrawn and shall not be further proceeded with, without prejudice to a fresh application being made by the applicant.

Regulation 8. Information required for establishment stage.

An application for the establishment stage of a licence shall contain the following information:

(a) the particulars of the applicant;

(b) the anticipated operational costs and proposed financing;

(c) details of the personnel to be employed and their qualifications, if available;

(d) the proposed operating procedure; and

(e) the services to be provided and the fees and charges to be imposed therefor.

Regulation 9. Information required for operation stage.

An application for the operation stage of a licence shall contain -

(*a*) all valid information submitted for the establishment stage;

(*b*) all new information and all the changes to the information submitted for the establishment stage, if any;

(*c*) a suitable guarantee; and

(*d*) a report from a qualified auditor certifying that the prescribed licensing, standards and technical requirements have been satisfied.

Regulation 10. Issue of licence.

(1) A licence to operate as a certification authority shall be in Form 2.

(2) The Controller shall specify the stage for which the licence is issued and the duration of the licence in the licence.

(3) The prescribed granting fee and annual operating fee for the first year of operation shall be payable to the Controller on the issuance of the operation stage of the licence.

(4) The prescribed annual operating fee for the second and subsequent years of operation shall be payable at such time as may be determined by the Controller.

Regulation 11. Implied conditions.

In every licence granted under the Act, there shall be implied on the part of the licensed certification authority that -

(*a*) the licensed certification authority shall keep and maintain working capital reasonably sufficient to carry on or operate as a certification authority;

(*b*) the licensed certification authority shall keep its operating procedures under review and shall not make any substantial changes to its operating procedures without the Controller's prior written approval;

(*c*) the licensed certification authority shall only use an approved digital signature scheme;

(*d*) the licensed certification authority shall make, keep and maintain the necessary arrangements with a recognised repository and a recognised date/time stamp service for its own use and for the use of its subscribers if it does not also provide those services;

(*e*) the licensed certification authority shall establish and maintain a secure system and infrastructure to safeguard its private key and for key distribution, key management, key storage and key disposal;

(*f*) the licensed certification authority shall establish and maintain a secure system and data base for the storage of information and documents obtained from a subscriber under the Act and these Regulations;

(*g*) the licensed certification authority shall at all times maintain the confidentiality of information and documents obtained from a subscriber under the Act and these Regulations and be subject to the directions of the subscriber in relation to the release or disclosure of such information and documents;

(*h*) the licensed certification authority shall keep and maintain the suitable guarantee as required under these Regulations;

(*i*) if the licensed certification authority intends to discontinue its operations, the licensed certification authority shall give to the subscriber of each unrevoked or unexpired certificate issued by the licensed certification authority at least ninety days written notice of such intention;

(*j*) the licensed certification authority shall keep and maintain detailed written records of its transactions as required under these Regulations;

(*k*) the licensed certification authority shall keep and maintain books of account as required under these Regulations; and

(*l*) the licensed certification authority shall comply with any directions of the Controller issued under the Act and these Regulations.

Regulation 12. Renewal of licence.

(1) An application for the renewal of a licence shall be made in Form 1.

(2) An application under subregulation (1) shall be accompanied by -

(*a*) the prescribed fee; and

(*b*) the annual compliance audit report for the relevant year or years.

Regulation 13. Replacement of l

icence.

(1) An application for a replacement licence shall be made in Form 3.

(2) If the Controller is satisfied as to the reasons for the loss of the licence, the Controller may issue a replacement licence in Form 2 with the words "DUPLICATE" endorsed on the licence.

Regulation 14. Amendment of licence on request.

(1) A licensed certification authority may apply to the Controller to amend -

(*a*) the particulars of the licence; or

(*b*) the conditions attached to the licence.

(2) An application under subregulation (1) shall be in writing and shall be submitted to the Controller.

(3) If the Controller approves the amendment, the Controller shall amend the licence accordingly and allow the licence to continue to have effect, as amended, until its expiry.

Regulation 15. Power to amend, etc. conditions of licence.

(1) The Controller may, during the currency of a licence, amend, vary, add to, revoke, suspend or revive any condition attached to the licence or attach new conditions to it and shall notify the licensed certification authority in writing accordingly.

(2) The Controller shall, before taking any action under subregulation (1), take into consideration -

(*a*) the estimated cost to be incurred by the licensed certification authority to comply with the varied or new conditions; and

(*b*) the nature and size of the business being carried out in the business premises.

(3) If the Controller amends, varies, adds to or attaches any condition to a licence under subregulation (1), such condition shall have no effect until the licensed certification authority is given a reasonable opportunity of being heard.

Regulation 16. Transfer or assignment of licence.

(1) A licence shall not be transferred except with the written approval of the Controller.

(2) An application for approval under subregulation (1) shall be made by the licensed certification authority in writing and shall be submitted to the Controller.

(3) An application under subregulation (1) shall be accompanied by the prescribed fee.

(4) If the licensed certification authority -

(*a*) in the case of a company, is wound up; or

(*b*) in the case of a partnership, is dissolved,

the Controller may, on application in writing, by endorsement on the licence and subject to such conditions as he thinks fit, assign the licence to a fit and proper person for the benefit of the licensed certification authority until the expiration of the licence or such earlier date as the Controller thinks fit and such person shall be deemed to be the licensed certification authority for the purposes of the Act and these Regulations.

Regulation 17. Partnerships in licence.

(1) If a licence is issued to a partnership, all the partners shall be named as licensees in the licence.

(2) If any change occurs in the partnership, the remaining partners or any of them shall, within one month of such change, inform the Controller in writing accordingly.

(3) If the Controller is satisfied that the partnership has not been dissolved and, in the case of an addition of a partner to the partnership, that the new partner is a fit and proper person, the Controller may amend the licence accordingly and allow the licence to continue to have effect, as amended, until its expiry.

(4) An amendment under subregulation (3) shall be deemed to be an amendment made under regulation 14.

(5) Every partner shall be deemed to be jointly and severally liable for the acts and omissions of the other partners unless the partner proves to the satisfaction of the court that -

(*a*) the act or omission was committed without that partner's knowledge, consent or connivance; and

(*b*) the partner took all reasonable precautions and had exercised due diligence to prevent the act or omission.

Regulation 18. Register of Licences.

(1) The Controller shall keep and maintain a Register of Licences in such form as he thinks fit.

(2) A person may inspect the Register of Licences and make copies of or take extracts from the Register.

(3) The Controller shall publish a list of licensed certification authorities in such form and manner as he may determine.

Regulation 19. Certified copy of licence.

(1) A licensed certification authority may apply in writing to the Controller for a certified copy of the licence if -

(*a*) the licence issued to the licensed certification authority is lost, destroyed or mutilated; or

(*b*) a certified copy of the licence is required for a valid reason.

(2) An application shall be accompanied by a statutory declaration or police report by the licensed certification authority to the effect that the licence issued to the licensed certification authority is lost, destroyed or mutilated or by a statement specifying the reasons for the application, as the case may be.

(3) The Controller or an officer authorised by the Controller may issue a certified copy of the licence to the applicant if the Controller or officer is satisfied that the original is lost, destroyed or mutilated or that a certified copy is required for a valid reason.

PART III - CERTIFICATION AUTHORITY DISCLOSURE RECORD

Regulation 20. Contents of certification authority disclosure record.

(1) The certification authority disclosure record of a licensed certification authority shall contain the following particulars:

(*a*) a statement that the certification authority disclosure record is provided and maintained by the Controller;

(*b*) the business name and registered address of the licensed certification authority;

(*c*) the telephone and facsimile number of the licensed certification authority, if any;

(*d*) the electronic mail or other address by which the licensed certification authority may be contacted electronically, if any;

(*e*) the distinguished name of the licensed certification authority;

(*f*) the licence number, the date and time of the issue, and the date and time of the expiry, of the licence issued to the licensed certification authority;

(*g*) the restrictions imposed on the licence issued to the licensed certification authority under section 15 of the Act, if any;

(*h*) if the revocation of a licence under section 9 of the Act has taken effect, the fact of the revocation and its effective date;

(*i*) if a licence has been surrendered under section 11 of the Act, the fact of the surrender and its effective date;

(*j*) if the licensed certification authority has no intention of renewing its licence under section 17 of the Act, a statement to that effect;

(*k*) the current public key or keys of the licensed certification authority by which its digital signatures on published certificates may be verified;

(*l*) the amount of the licensed certification authority's suitable guarantee;

(*m*) the total amount of all claims filed with the Controller for payment from the suitable guarantee filed by the licensed certification authority;

(*n*) a brief description of any limit known to the Controller and applicable to the licensed certification authority's liability or legal capacity to pay damages in tort or for breach of a duty under the Act or these Regulations, unless the limitation is specified in the Act or these Regulations;

(*o*) a statement indicating the location of the licensed certification authority's certification practice statement, the method or procedure by which it may be retrieved, its form and structure, its authorship and its date;

(*p*) the date and result of a compliance audit under section 20 of the Act;

(*q*) if a licensed certification authority is exempted from a compliance audit under section 21 of the Act, a statement to that effect;

(*r*) the repository used by the licensed certification authority;

(*s*) if a certificate containing the public key required to verify one or more certificates issued by the licensed certification authority has been revoked or is currently suspended, the date and time of its revocation or suspension;

(*t*) any event that substantially affects the licensed certification authority's ability to conduct its business or the validity of a certificate published in the repository provided by the Controller or in a recognised repository; and

(*u*) any other particulars relating to the licensed certification authority the Controller thinks fit.

(2) If the particulars required to be published in the certification authority disclosure record are within the

knowledge of the licensed certification authority concerned, whether solely or otherwise, the licensed certification authority shall, as soon as practicable, forward the particulars to the Controller.

(3) A person who contravenes subregulation (2) commits an offence and shall on conviction be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both.

(4) The Controller shall review the certification authority disclosure record on a regular basis and shall ensure that all information received is inserted into the certification authority disclosure record as soon as possible after it is received.

Regulation 21. Form of certification authority disclosure record.

The Controller shall maintain the certification authority disclosure record of a licensed certification authority in such form as the Controller thinks fit.

Regulation 22. Retention of certification authority disclosure record.

The certification authority disclosure record of a licensed certification authority shall, unless the Controller otherwise directs, be retained for not less than ten years from the date of the last entry.

PART IV - SUITABLE GUARANTEES AND CLAIMS

Regulation 23. Suitable guarantee.

(1) A suitable guarantee shall satisfy the following requirements:

(*a*) it is in a form approved by the Controller;

(*b*) it is issued payable to the Controller for the benefit of persons holding qualified rights of payment against the licensed certification authority;

(*c*) it is in an amount specified in subregulation (2) or (3), as the case may be;

(*d*) it states that it is issued for the purposes of the Act and these Regulations; and

(*e*) it specifies a term of effectiveness extending at least as long as the term of the licence to be issued to the certification authority.

(2) A suitable guarantee shall be in an amount equal to or exceeding the greater of either -

(*a*) 100 per centum of the largest recommended reliance limit of a certificate to be issued by the certification authority during the term of the certification authority's licence; or

(*b*) 35 per centum of the total recommended reliance limits of all certificates issued by the licensed certification authority, which certificates have not expired or been revoked.

(3) Notwithstanding subregulation (2), the Controller may, on a request in writing by the certification authority and if the Controller thinks it is reasonable in the circumstances to do so, specify an amount that is less than the amount determined under subregulation (2) to be the suitable guarantee provided that the amount so specified shall not be less than two million ringgit.

(4) A suitable guarantee may in addition provide that the total annual liability on the guarantee to all persons making claims based on it may not exceed the face amount of the guarantee.

(5) The Controller shall hold the suitable guarantee for the period for which the licence is issued and as provided under regulation 24.

Regulation 24. Return of suitable guarantee.

(1) If a licence has expired and will not be renewed or has sooner been revoked or surrendered, the Controller shall return the suitable guarantee or the balance of the suitable guarantee, if any, as the case may be, to the certification authority concerned after all claims on it are settled or after the expiry of a period of three years after such expiry, revocation or surrender, whichever is the later.

(2) If the term of the suitable guarantee would expire in the period referred to in subregulation (1), the Controller shall require the certification authority concerned to renew or extend the term of the suitable guarantee for that period or submit a new suitable guarantee for the period.

(3) A person who contravenes the Controller's request under subregulation (2) commits an offence and shall on conviction be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both.

Regulation 25. Collection on suitable guarantee.

(1) Notwithstanding any provision in the suitable guarantee to the contrary, a person may recover from the issuer of the suitable guarantee the full amount of a qualified right to payment against the person named in the suitable guarantee, or, if there is more than one such qualified right to payment during the term of the suitable guarantee, a rateable share, up to a maximum total liability of the issuer of the suitable guarantee equal to the amount of the suitable guarantee.

(2) Claimants may recover successively on the same suitable guarantee, provided that the total liability on the suitable guarantee to all persons making qualified rights of payment during its term shall not exceed the amount of the suitable guarantee.

(3) In addition to recovering the amount of a qualified right to payment, a claimant may recover from the proceeds of the suitable guarantee, until depleted, legal fees, reasonable in amount, and court costs incurred by the claimant in collecting the claim, provided that the total liability on the suitable guarantee to all persons making qualified rights of payment or recovering legal fees or court costs during its term shall not exceed the amount of the suitable guarantee.

Regulation 26. Procedure for claim.

(1) Subject to regulation 27, a person who asserts that that person has a qualified right to payment against the issuer of a suitable guarantee shall, within thirty days of the judgment of the court on which the qualified right to payment is based, submit a written notice of the claim in Form 4 to the Controller.

(2) A notice under subregulation (1) shall be accompanied by -

(*a*) the prescribed fee; and

(*b*) such information or document as the Controller may require.

(3) If the Controller finds that the claim is in order, the Controller may order the payment and satisfaction of the claim.

(4)

Regulation 27. Claims after suitable guarantee returned.

(1) No claim to recover a qualified right to payment from the proceeds of a suitable guarantee shall be

made to the Controller under regulation 26 after the Controller has returned the suitable guarantee to the certification authority under regulation 24.

(2) Nothing in subregulation (1) shall be construed as limiting the rights of the claimant to recover a qualified right to payment from the certification authority concerned in execution of the judgment of the court by any other means.

PART V - APPROVED DIGITAL SIGNATURE SCHEME AND KEY MANAGEMENT

Regulation 28. Approved digital signature scheme to be used.

An approved digital signature scheme shall be used for the purpose of generating a key pair, or creating, using or verifying a digital signature under the Act.

Regulation 29. Approved digital signature scheme.

(1) A digital signature scheme shall be approved for the purposes of the Act and these Regulations if -

(*a*) the digital signature scheme uses a secure public-key algorithm for the generation of the key pair and a secure public-key algorithm and hash function for the creation of the digital signature;

(*b*) the digital signature scheme satisfies the technical component requirements under regulation 81; and

(*c*) the digital signature created is not capable of being modified to contain a subliminal channel.

(2) A key pair used to create and verify a digital signature shall not be used to encrypt and decrypt any messages.

Regulation 30. Storage of private keys.

(1) The data storage medium for the private key may be hardware based or software based.

(2) If the data storage medium of the private key is hardware based, the holder of the private key shall ensure that the token, smart card or other external device in which the private key is stored is kept in a secure place and in a secure manner.

(3) If the data storage medium of the private key is software based, the holder of the private key shall ensure that the computer system in which the private key is stored is reasonably secure.

(4) The personal identification numbers or other data used for the identification of the rightful holder of the private key in conjunction with the data storage medium for the private key shall be kept secret.

Regulation 31. Key length.

A licensed certification authority and a subscriber shall ensure that the key length of its key pair is adequately secure for its purposes.

Regulation 32. Prohibition against duplication of private key.

(1) No person, except the rightful holder of the private key, shall make or cause to be made any copy of a private key.

(2) A person who contravenes subregulation (1) commits an offence and shall on conviction be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Regulation 33. Disposal of key pairs.

(1) If a key pair is no longer in use or to be used, or if the private key of the key pair is compromised, the holder of the key pair shall dispose of it in a suitable manner, including by destroying it.

(2) A secure means and method shall be used for the destruction of keys.

(3) Notwithstanding subregulation (1), if the holder desires to retain a key pair that is no longer in use or to be used, or that has been compromised, the holder shall ensure that the key pair is stored by a reasonably secure method.

PART VI - REGULATION OF CERTIFICATION PRACTICE

Regulation 34. Key generation.

(1) A subscriber's key pair may be generated by -

(*a*) the subscriber; or

(*b*) the licensed certification authority for the subscriber on a written request by the subscriber and on payment of the approved fee.

(2) If the subscriber generates the key pair, the licensed certification authority shall reasonably ascertain whether the subscriber has used the prescribed technical components for the generation of the key pair and for the storage of the key pair.

(3) If the licensed certification authority generates a key pair for the subscriber, the licensed certification authority shall ensure that -

(*a*) it uses a secure protocol that incorporates adequate safeguards and security features for the distribution or transmission of the private key to the subscriber; and

(*b*) no copy of the subscriber's private key is retained or otherwise kept by the licensed certification authority.

(4) A licensed certification authority that contravenes subregulation (3) commits an offence and shall on conviction be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Regulation 35. Certification practice statement.

(1) A licensed certification authority shall issue or make available to a subscriber before or at the time the subscriber applies for a certificate from the licensed certification authority a copy of its

certification practice statement.

(2) A certification practice statement shall contain all the particulars specified in the Third Schedule.

(3) Nothing in subregulation (2) shall prevent the licensed certification authority from adopting a more comprehensive certification practice statement provided it is not inconsistent with the Act and these Regulations.

(4) The certification practice statement shall be in such form as the Controller may determine.

Regulation 36. Duty of instruction.

(1) A licensed certification authority shall instruct an applicant for a certificate concerning -

(*a*) the measures necessary to contribute to secure digital signatures and their reliable verification;

(*b*) which technical components fulfill the requirements of regulation 81; and

(*c*) the attribution of digital signatures created with the subscriber's private key.

(2) A licensed certification authority shall inform the applicant that data with digital signatures may need to be re-signed before the security value of an available digital signature decreases with time.

(3) If data are re-signed under subregulation (2), the new digital signature shall include the earlier digital signature or signatures and shall bear a time-stamp.

Regulation 37. Application for certificate.

(1) An application for a certificate shall be made in writing to the licensed certification authority.

(2) An application under subregulation (1) shall contain the following particulars:

(*a*) the name and address of the subscriber;

(*b*) the telephone and facsimile number of the subscriber, if any;

(*c*) the electronic mail or other address by which the subscriber may be contacted electronically, if any;

(*d*) the distinguished name of the subscriber;

(*e*) any pseudonym to be used to preserve the anonymity of the subscriber;

(*f*) the public key corresponding to the subscriber's private key, if the subscriber generates his own key pair;

(*g*) an identifier of the algorithms with which the subscriber's public key is intended to be used, if the subscriber generates his own key pair;

(*h*) a statement of the period for which the certificate is required;

(*i*) a statement of any limitations on the authority of the subscriber who is to be the signer;

(*j*) the recommended reliance limit required for the certificate; and

(*k*) either the distinguished name of the repository designated for publication of notice of revocation or suspension of the certificate, or a specification of the method by which notice of revocation or

suspension of the certificate is to be given.

(3) An application under subregulation (1) shall be accompanied by -

(*a*) the approved fee; and

(*b*) such other information or document as the licensed certification authority may require.

(4) The licensed certification authority may, at its discretion, refuse to allow a subscriber to use a pseudonym.

Regulation 38. Issue of certificate.

(1) On receipt of an application under regulation 37, the licensed certification authority shall consider the application.

(2) If the licensed certification authority is satisfied as to the identity of the subscriber, the licensed certification authority may issue a certificate to the subscriber, with or without conditions, or refuse the certificate.

(3) A certificate issued by a licensed certification authority under subregulation (2) shall contain or incorporate by reference the following particulars:

(*a*) a statement that the type of the certificate is in accordance with this regulation;

(*b*) the licence number, the date and time of the issue, and the date and time of the expiry, of its licence;

(*c*) the serial number of the certificate, that must be unique among the certificates issued by the licensed certification authority;

(*d*) a statement whether the certificate is a transactional certificate;

(*e*) the name by which the subscriber is generally known or the pseudonym to be used;

(*f*) the distinguished name of the subscriber;

(*g*) the public key corresponding to the subscriber's private key;

(*h*) an identifier of the algorithms with which the subscriber's public key is intended to be used;

(*i*) the date and time on which the certificate is issued and accepted;

(*j*) the date and time on which the certificate expires;

(*k*) the distinguished name of the licensed certification authority issuing the certificate;

(*l*) an identifier of the algorithm or algorithms used to sign the certificate, in the form generally accepted in the subscriber's industry;

(*m*) the recommended reliance limit of the certificate;

(*n*) either the distinguished name of the repository designated for publication of notice of revocation or suspension of the certificate, or a specification of the method by which notice of revocation or suspension of the certificate is to be given; and

(*o*) a statement indicating the location of the licensed certification authority's certification practice statement, the method or procedure by which it may be retrieved, its form and structure, its

authorship and its date.

(4) A certificate issued by a licensed certification authority under subregulation (2) may, at the option of the subscriber and the licensed certification authority, contain or incorporate by reference all or any of the following particulars:

(*a*) one or more additional, secondary public keys;

(*b*) identifiers or usage indicators related to public keys;

(*c*) references incorporating any applicable certification practice statements;

(*d*) any other available documents material to the certificate, the issuing licensed certification authority or the accepting subscriber.

(5) The data in a certificate shall be in such form as the Controller may determine.

(6) A certificate shall be digitally signed by the issuing licensed certification authority.

(7) The licensed certification authority shall keep and maintain a Register of Certificates containing a list of the certificates issued by it in such form as the Controller may determine.

(8) If the licensed certification authority refuses a certificate under subregulation (2), the licensed certification authority shall immediately notify the applicant in writing and shall immediately refund the approved fee.

(9) The licensed certification authority may classify the certificates issued by it according to designated levels of trust and may issue certificates according to such classification.

Regulation 39. Certificate Revocation List.

(1) A licensed certification authority shall keep and maintain a Certificate Revocation List that shall contain a list of all certificates revoked by the licensed certification authority together with the date and time of revocation.

(2) A Certificate Revocation List shall be digitally signed by the licensed certification authority.

(3) The licensed certification authority shall publish the Certificate Revocation List in at least one recognised repository.

(4) The licensed certification authority shall keep the Certificate Revocation List under constant review and shall enter all relevant information as soon as possible after it is received or determined but no later than the end of the business day on which it is received or determined.

(5) The licensed certification authority shall publish an up-dated Certificate Revocation List at least once in every twenty-four hours.

Regulation 40. Chargeable fees.

A licensed certification authority may impose such fees and charges for its services as may be approved by the Controller.

Regulation 41. Qualification and registration of auditors.

(1) A certified public accountant or an accredited computer security professional intending to act as a compliance auditor under section 20 of the Act shall satisfy the following requirements:

(*a*) holds such accreditation or qualification as the Controller may determine;

(*b*) has at least two years experience in trusted computer information systems, trusted telecommunications networking environments and professional audit techniques;

(*c*) has at least two years experience in digital signature technology, standards and practices; and

(*d*) demonstrates knowledge of the requirements of the Act and these Regulations that satisfies the Controller.

(2) A certified public accountant or an accredited computer security professional intending to act as a compliance auditor under section 20 of the Act shall apply in writing to the Controller to be registered as a qualified auditor.

(3) If the Controller is satisfied that the requirements under subregulation (1) have been complied with, the Controller may register the applicant as a qualified auditor.

(4) A qualified auditor registered with the Controller under these Regulations shall not operate as or in any way participate in the operation of or be concerned in a certification authority, a repository or a date/time stamp service.

(5) The Controller shall keep and maintain a Register of Qualified Auditors in such form as he thinks fit.

(6) A person may inspect the Register of Qualified Auditors and make copies of or take extracts from the Register.

Regulation 42. Procedure for annual compliance audit.

(1) The qualified auditor shall give the licensed certification authority at least seven days written notice before the qualified auditor carries out the annual compliance audit.

(2) The licensed certification authority shall make available any information, document or personnel as may be required by the qualified auditor.

(3) Based on the information gathered in the audit, the qualified auditor shall categorise the licensed certification authority's compliance as one of the following:

(*a*) full compliance, if the licensed certification authority appears to comply with all the requirements of the Act and these Regulations;

(*b*) substantial compliance, if the licensed certification authority appears generally to comply with the requirements of the Act and these Regulations but one or more instances of non-compliance or of inability to demonstrate compliance were found in the audited sample, that were likely to be inconsequential;

(*c*) partial compliance, if the licensed certification authority appears to comply with some of the requirements of the Act and these Regulations but was found not to have complied with or not to be able to demonstrate compliance with one or more important safeguards; or

(*d*) non-compliance, if the licensed certification authority

(i) complies with few or none of the requirements of the Act or these Regulations;

(ii) fails to keep adequate records to demonstrate compliance with more than a few requirements; or

(iii) refused to submit to an audit.

Regulation 43. Auditor's report.

(1) The qualified auditor shall within fourteen days from the completion of a compliance audit under regulation 42 submit a written report to the Controller.

(2) The auditor's report shall contain -

(*a*) the date of the audit;

(*b*) a list of the information or documents studied or of the personnel interviewed;

(*c*) the extent of compliance with the Act and these Regulations;

(*d*) the results of the audit;

(*e*) the categorisation of the licensed certification authority; and

(*f*) such other information as the qualified auditor thinks fit.

Regulation 44. Additional compliance audits.

(1) In addition to the annual compliance audit required under section 20 of the Act, the qualified auditor may carry out additional and unscheduled audits on a licensed certification authority.

(2) No notice shall be required to be given of an audit under subregulation (1).

Regulation 45. Offence to obstruct or interfere with compliance audit.

A person who obstructs or interferes with a compliance audit under regulation 42 or 44 commits an offence and shall on conviction be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both.

Regulation 46. Consequence of failing annual compliance audit.

(1) The Controller shall consider the results of the annual compliance audit when considering an application to renew a licence under regulation 12.

(2) A finding of non-compliance under regulation 42 shall be a ground for the revocation of a licence under section 9 of the Act or for the refusal to renew a licence under section 17 of the Act.

PART VIII - REPOSITORIES

Regulation 47. Stages of certificate of recognition for repositories.

(1) A certificate of recognition for a repository shall be issued in two stages, namely -

(*a*) the establishment stage; and

(*b*) the operation stage.

(2) No person shall carry on or operate, or hold himself out as carrying on or operating, as a recognised repository unless that person has been issued with the operation stage of the certificate of recognition.

(3) A person who contravenes subregulation (2) commits an offence and shall on conviction be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

(4) The establishment stage of a certificate of recognition may be issued for any period not exceeding one year.

(5) An application for a certificate of recognition shall be deemed to be withdrawn and shall not be further proceeded with, without prejudice to a fresh application being made by the applicant, if -

(*a*) the applicant fails to apply for the operation stage of the certificate of recognition before the expiry of the period specified in subregulation (4); or

(*b*) an application for the operation stage of the certificate of recognition having duly been made within the period specified in subregulation (4), the applicant is not issued with the operation stage of the certificate of recognition.

(6) Nothing in these Regulations shall be construed so as to require an applicant to apply for the establishment stage of a certificate of recognition as a condition for applying for the operation stage of a certificate of recognition if the applicant is otherwise able to satisfy the prescribed requirements to apply for the operation stage of a certificate of recognition.

Regulation 48. Qualification requirements for recognition.

A person intending to carry on or operate as a repository shall satisfy the following requirements:

(*a*) it is a body corporate incorporated in Malaysia or a partnership within the meaning of the Partnership Act 1961;

(*b*) it maintains a registered office in Malaysia;

(*c*) it has working capital reasonably sufficient, according to the requirements of the Controller, to enable it to conduct business as a repository;

(*d*) it employs as operative personnel only persons who -

(i) have not been convicted within the past fifteen years of an offence involving fraud, false statement or deception; and

(ii) have demonstrated knowledge and proficiency in following the requirements of the Act and these Regulations;

(*e*) the repository includes a data base that is capable of containing -

(i) certification authority disclosure records for licensed certification authorities;

(ii) certificates to be published in the repository;

(iii) notices of suspended or revoked certificates to be published by a licensed certification authority or any person suspending or revoking certificates;

(iv) notices of termination of suspension of certificates to be published by a licensed certification authority or any person suspending certificates;

(v) advisory statements, written defences thereto and decisions made by the Controller

thereon to be published by the Controller under the Act and these Regulations; and

(vi) such other information as the Controller thinks fit;

(*f*) it operates by means of a trustworthy system;

(*g*) the repository contains no significant amount of information that the Controller finds is known or likely to be untrue, inaccurate or not reasonably reliable;

(*h*) the repository contains certificates published by certification authorities that are required to conform to rules of practice that are similar to or more stringent than the requirements of the Act and these Regulations;

(*i*) it keeps and maintains an archive of certificates that have been suspended or revoked, or that have expired, within at least the preceding ten years;

(*j*) it complies with the certification, standards and technical requirements under the Act and these Regulations; and

(*k*) it complies with such other requirements as the Controller thinks fit.

Regulation 49. Functions of recognised repository.

(1) A recognised repository shall -

(*a*) maintain a publicly accessible data base for the purposes of publishing the information required to be published under the Act and these Regulations;

(*b*) publish the certification authority disclosure records for licensed certification authorities as the Controller may require;

(*c*) publish such advisory statements, written defences thereto and decisions by the Controller thereon and such other information as the Controller may require;

(*d*) publish such information as a licensed certification authority may require; and

(*e*) publish such other information as the recognised repository deems fit.

(2) A recognised repository shall publish all information received and requested to be published not later than one business day after receipt of the request and information.

(3) If for any reason the recognised repository is unable to comply with the time limit specified in subregulation (2), the recognised repository shall immediately upon receipt of the request and information notify the requester in writing of that fact.

(4) A person who contravenes subregulation (3) commits an offence and shall on conviction be liable to a fine not exceeding twenty thousand ringgit or to imprisonment for a term not exceeding six months or to both.

Regulation 50. Chargeable fees.

A recognised repository may impose such fees and charges for its services as may be approved by the Controller.

Regulation 51. Application for certificate of recognition.

(1) An application for the recognition of the repository shall be made to the Controller in Form 1.

(2) An application under subregulation (1) shall be accompanied by -

(*a*) the information required under regulation 52 or 53, as the case may be;

(*b*) the prescribed fee; and

(*c*) such other information or document as the Controller may require.

(3) The Controller may, on an application for the operation stage of a certificate of recognition, require the applicant to demonstrate any part of its operating procedure and may require independent testing of the software, hardware, technical components, algorithms, standards and other pertinent parameters and other equipment to be used by the applicant, at the applicant's expense, for the purpose of ascertaining its security and trustworthiness.

(4) If any information or document required under subregulation (2) is not provided by the applicant or any demonstration or test required under subregulation (3) is not complied with within the time specified in the requirement or any extension thereof granted by the Controller, the application shall be deemed to be withdrawn and shall not be further proceeded with, without prejudice to a fresh application being made by the applicant.

Regulation 52. Information required for establishment stage.

An application for the establishment stage of a certificate of recognition shall contain the following information:

(*a*) the particulars of the applicant;

(*b*) the anticipated operational costs and proposed financing;

(*c*) details of the personnel to be employed and their qualifications, if available;

(*d*) the proposed operating procedure; and

(*e*) the services to be provided and the fees and charges to be imposed therefor.

Regulation 53. Information required for operation stage.

An application for the operation stage of a certificate of recognition shall contain -

(*a*) all valid information submitted for the establishment stage;

(*b*) all new information and all the changes to the information submitted for the establishment stage, if any; and

(*c*) a report from a qualified auditor certifying that the prescribed certification, standards and technical requirements have been satisfied.

Regulation 54. Issue and renewal of certificate of recognition.

(1) On receipt of an application under regulation 51, the Controller shall consider the application.

(2) If the Controller is satisfied as to the qualification and suitability of the repository, the Controller

may issue a certificate of recognition in Form 5, with or without conditions, or may refuse the certificate of recognition.

(3) The Controller shall specify the stage for which the certificate of recognition is issued, the duration of the certificate of recognition and its serial number in the certificate of recognition.

(4) If the Controller refuses a certificate of recognition under subregulation (2), the Controller shall immediately notify the applicant in writing of his refusal.

(5) The decision of the Controller under subregulation (4) shall be final and shall not be questioned in any court.

(6) The prescribed granting fee and annual operating fee for the first year of operation shall be payable to the Controller on the issuance of the operation stage of the certificate of recognition.

(7) The prescribed annual operating fee for the second and subsequent years of operation shall be payable at such time as may be determined by the Controller.

(8) A certificate of recognition shall be renewable on application.

(9) An application for the renewal of a certificate of recognition shall be made in Form 1.

(10) An application under subregulation (9) shall be accompanied by -

Regulation 55. Revocation of certificate of recognition.

(1) The Controller may revoke a certificate of recognition issued under regulation 54 -

(*a*) if the Controller finds that the recognised repository no longer satisfies the requirements specified under regulation 48; or

(*b*) if the validity period of the certificate of recognition has expired.

(2) A revocation under paragraph (1)(*b*) shall be without prejudice to a fresh application for a certificate of recognition being made by the repository.

Regulation 56. Surrender of certificate of recognition.

(1) A recognised repository may surrender its certificate of recognition by forwarding it to the Controller with a written notice of its surrender.

(2) The surrender shall take effect on the date the Controller receives the certificate of recognition and the notice under subregulation (1), or if a later date is specified in the notice, on that date.

(3) On receipt of a notice of surrender under subregulation (1), the Controller shall immediately cause such surrender to be published in such form and manner as he may determine.

(4) A recognised repository intending to surrender its certificate of recognition shall, not less than ninety days before the date the surrender is intended to take effect, notify all its clients in writing of its intention.

(5) A recognised repository that contravenes subregulation (4) commits an offence and shall on conviction be liable to a fine not exceeding ten thousand ringgit or to imprisonment for a term not exceeding three months or to both.

Regulation 57. Register of Recognised Repositories.

(1) The Controller shall keep and maintain a Register of Recognised Repositories in such form as he thinks fit.

(2) A person may inspect the Register of Recognised Repositories and make copies of or take extracts from

the Register.

PART IX - DATE/TIME STAMP SERVICES

Regulation 58. Use of time-stamps.

A time-stamp by a recognised date/time stamp service shall be appended or attached to a message, digital signature or other document if -

(*a*) a time-stamp is required under any written law; or

(*b*) a particular time may be significant with regard to the use of digitally signed data.

Regulation 59. Effect of time-stamp by recognised date/time stamp service.

(1) The date and time time-stamped on a document and digitally signed by a recognised date/time stamp service shall, unless it is expressly provided otherwise, be deemed to be the date and time at which the document is signed or executed.

(2) The date and time time-stamped on a document and digitally signed by a recognised date/time stamp service shall be admissable in evidence in all legal proceedings without further proof.

(2) Regulation 60. Stages of certificate of recognition for date/time stamp services.

(3)

(1) A certificate of recognition for a date/time stamp service shall be issued in two stages, namely -

(*a*) the establishment stage; and

(*b*) the operation stage.

(2) No person shall carry on or operate, or hold himself out as carrying on or operating, as a recognised date/time stamp service unless that person has been issued with the operation stage of the certificate of recognition.

(3) A person who contravenes subregulation (2) commits an offence and shall on conviction be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

(4) The establishment stage of a certificate of recognition may be issued for any period not exceeding one year.

(5) An application for a certificate of recognition shall be deemed to be withdrawn and shall not be further proceeded with, without prejudice to a fresh application being made by the applicant, if -

(*a*) the applicant fails to apply for the operation stage of the certificate of recognition before the expiry of the period specified in subregulation (4); or

(*b*) on an application for the operation stage of a certificate of recognition having duly been made within the period specified in subregulation (4), the applicant is not issued with the operation stage of the certificate of recognition.

(6) Nothing in these Regulations shall be construed so as to require an applicant to apply for the establishment stage of a certificate of recognition as a condition for applying for the operation stage of a certificate of recognition if the applicant is otherwise able to satisfy the prescribed requirements to apply for the operation stage of a certificate of recognition.

Regulation 61. Qualification requirements for recognition.

A person intending to carry on or operate as a date/time stamp service shall satisfy the following requirements:

(*a*) it is a body corporate incorporated in Malaysia or a partnership within the meaning of the Partnership Act 1961;

(*b*) it maintains a registered office in Malaysia;

(*c*) it has working capital reasonably sufficient, according to the requirements of the Controller, to enable it to conduct business as a date/time stamp service;

(*d*) it employs as operative personnel only persons who -

(i) have not been convicted within the past fifteen years of an offence involving fraud, false statement or deception; and

(ii) have demonstrated knowledge and proficiency in following the requirements of the Act and these Regulations;

(*e*) it operates by means of a trustworthy system;

(*f*) it uses a reasonably secure and tamper-proof mechanism as it's time-stamping device;

(*g*) it keeps and maintains an archive of documents that have been time-stamped, irrespective that the contents of the document itself are not disclosed, within at least the preceding ten years;

(*h*) it complies with the certification, standards and technical requirements under the Act and these Regulations; and

(*i*) it complies with such other requirements as the Controller thinks fit.

Regulation 62. Functions of recognised date/time stamp service.

(1) A recognised date/time stamp service shall -

(*a*) on receipt of a document for time-stamping, immediately time-stamp the date and time of its receipt on the document and digitally sign the time-stamp; and

(*b*) at the end of each business day cause to be published in at least one recognised repository all documents time-stamped by it in that day.

(2) For the purposes of paragraph (1)(*b*), only the hash result of the document shall be published.

(3) The date and time time-stamped on the document shall be the date and time at which the document is received by the recognised date/time stamp service.

(4) If for any reason the recognised date/time stamp service is unable to comply with the time limit specified in subregulation (1), the recognised date/ time stamp service shall immediately upon receipt of the document and the request for a time-stamp notify the requester in writing of that fact.

(5) A person who contravenes subregulation (4) commits an offence and shall on conviction be liable to a fine not exceeding twenty thousand ringgit or to imprisonment for a term not exceeding six months or to both.

Regulation 63. Chargeable fees.

A recognised date/time stamp service may impose such fees and charges for its services as may be approved by the Controller.

Regulation 64. Application for certificate of recognition.

(1) An application for the recognition of the date/time stamp service shall be made to the Controller in Form 1.

(2) An application under subregulation (1) shall be accompanied by -

(*a*) the information required under regulation 65 or 66, as the case may be;

(*b*) the prescribed fee; and

(*c*) such other information or document as the Controller may require.

(3) The Controller may, on an application for the operation stage of a certificate of recognition, require the applicant to demonstrate any part of its operating procedure and may require independent testing of the software, hardware, technical components, algorithms, standards and other pertinent parameters and other equipment to be used by the applicant, at the applicant's expense, for l the purpose of ascertaining its security and trustworthiness.

(4) If any information or document required under subregulation (2) is not provided by the applicant or any demonstration or test required under subregulation (3) is not complied with within the time specified in the requirement or any extension thereof granted by the Controller, the application shall be deemed to be withdrawn and shall not be further proceeded with, without prejudice to a fresh application being made by the applicant.

Regulation 65. Information required for establishment stage.

An application for the establishment stage of a certificate of recognition shall contain the following information:

(*a*) the particulars of the applicant;

(*b*) the anticipated operational costs and proposed financing;

(*c*) details of the personnel to be employed and their qualifications, if available;

(*d*) the proposed operating procedure; and

(*e*) the services to be provided and the fees and charges to be imposed therefor.

Regulation 66. Information required for operation stage.

An application for the operation stage of a certificate of recognition shall contain -

(*a*) all valid information submitted for the establishment stage;

(*b*) all new information and all the changes to the information submitted for the establishment stage, if any; and

(*c*) a report from a qualified auditor certifying that the prescribed certification, standards and technical requirements have been satisfied.

-

Regulation 67. Issue and renewal of certificate of recognition.

(1) On receipt of an application under regulation 64, the Controller shall consider the application.

(2) If the Controller is satisfied as to the qualification and suitability of the date/time stamp service, the Controller may issue a certificate of recognition in Form 5, with or without conditions, or may refuse the certificate of recognition.

(3) The Controller shall specify the stage for which the certificate of recognition is issued, the duration of the certificate of recognition and its serial number in the certificate of recognition.

(4) If the Controller refuses a certificate of recognition under subregulation (2), the Controller shall immediately notify the applicant in writing of his refusal.

(5) The decision of the Controller under subregulation (4) shall be final and shall not be questioned in any court.

(6) The prescribed granting fee and annual operating fee for the first year of operation shall be payable to the Controller on the issuance of the operation stage of the certificate of recognition.

(7) The prescribed annual operating fee for the second and subsequent years of operation shall be payable at such time as may be determined by the Controller.

(8) A certificate of recognition shall be renewable on application.

(9) An application for the renewal of a certificate of recognition shall be made in Form 1.

(10) An application under subregulation (9) shall be accompanied by -

Regulation 68. Revocation of certificate of recognition.

(1) The Controller may revoke a certificate of recognition issued under regulation 67 -

(*a*) if the Controller finds that the recognised date/time stamp service no longer satisfies the requirements specified under regulation 61; or

(*b*) if the validity period of the certificate of recognition has expired.

(2) A revocation under paragraph (1)(*b*) shall be without prejudice to a fresh application for a certificate of recognition being made by the date/time stamp service.

Regulation 69. Surrender of certificate of recognition.

(1) A recognised date/time stamp service may surrender its certificate of recognition by forwarding it to the Controller with a written notice of its surrender.

(2) The surrender shall take effect on the date the Controller receives the certificate of recognition and the notice under subregulation (1), or if a later date is specified in the notice, on that date.

(3) On receipt of a notice of surrender under subregulation (1), the Controller shall immediately cause such surrender to be published in such form and manner as he may determine.

(4) A recognised date/time stamp service intending to surrender its certificate of recognition shall, not less than ninety days before the date the surrender is intended to take effect, notify all its clients in writing of its

intention.

(5) A recognised date/time stamp service that contravenes subregulation (4) commits an offence and shall on conviction be liable to a fine not exceeding ten thousand ringgit or to imprisonment for a term not exceeding three months or to both.

Regulation 70. Register of Recognised Date/Time Stamp Services.
(1) The Controller shall keep and maintain a Register of Recognised Date/ Time Stamp Services in such form as he thinks fit.

(2) A person may inspect the Register of Recognised Date/Time Stamp Services and make copies of or take extracts from the Register.

PART X - RECOGNITION OF FOREIGN CERTIFICATION AUTHORITIES

Regulation 71. Criteria for recognition of foreign certification authorities.

(1) A foreign certification authority shall satisfy the following requirements to qualify for recognition under section 19 of the Act:

(*a*) it shall be licensed or otherwise authorised by the relevant governmental entity in that country to carry on or operate as a certification authority in that country;

(*b*) the certificate issued by the foreign certification authority demonstrates a level of security equal to or more stringent than the level of security of a certificate issued by a licensed certification authority of Malaysia;

(*c*) it has established a local agent for service of process in Malaysia;

(*d*) it complies with the standards and technical requirements under the Act and these Regulations; and

(*e*) it complies with such other requirements as the Controller thinks fit.

(2) In addition, a foreign certification authority shall only be eligible for recognition under section 19 of the Act if an international treaty, agreement or convention concerning the recognition of its certificates has been concluded to which Malaysia is a party.

(3) Notwithstanding subregulation (1), the Controller may, if the Controller thinks fit to do so, and with the approval of the Minister, grant recognition to a foreign certification authority if it is unable to comply with the requirements of paragraph (1)(*a*) on the ground that the country concerned does not require a licence or other governmental authority to carry on certification practice in that country but it otherwise satisfies the requirements of paragraphs (1)(*b*), (*c*), (*d*) and (*e*) and subregulation (2).

Regulation 72. Application for recognition.

(1) An application for the recognition of a foreign certification authority shall be made to the Controller in writing.

(2) An application under subregulation (1) shall be accompanied by -

(*a*) proof that the requirements under regulation 71 have been satisfied, including a report from a qualified auditor certifying that the prescribed standards and technical requirements have been satisfied;

(*b*) the prescribed fee; and

(*c*) such other information or document as the Controller may require.

Regulation 73. Grant of recognition

(1) On receipt of an application under regulation 72, the Controller shall consider the application.

(2) If the Controller is satisfied as to the qualification and suitability of the foreign certification authority, the Controller may recognise the foreign certification authority, with or without conditions, or may refuse the recognition.

(3) If the Controller refuses to recognise a foreign certification authority under subregulation (2), the Controller shall immediately notify the applicant in writing of his refusal.

(4) The decision of the Controller under subregulation (3) shall be final and shall not be questioned in any court.

Regulation 74. Revocation of recognition.

(1) The Controller may revoke the recognition granted under regulation 73 -

(*a*) if the Controller finds that the recognised foreign certification authority no longer satisfies the requirements specified under regulation 71; or

(*b*) if the recognised foreign certification authority applies for a revocation of the recognition under regulation 75.

(2) A revocation of recognition under subregulation (1) shall be by order published in the *Gazette*.

(3) A revocation under paragraph (1)(*b*) shall be without prejudice to a fresh application for recognition being made by the foreign certification authority.

Regulation 75. Application for revocation of recognition.

(1) A recognised foreign certification authority may apply to the Controller in writing for the revocation of its recognition.

(2) A recognised foreign certification authority intending to apply for the revocation of its recognition shall, not less than ninety days before the date the application is made, notify all its clients in writing of its intention.

(3) A recognised foreign certification authority that contravenes subregulation (2) commits an offence and shall on conviction be liable to a fine not exceeding ten thousand ringgit or to imprisonment for a term not exceeding three months or to both.

Regulation 76. Register of Recognised Foreign Certification Authorities.

(1) The Controller shall keep and maintain a Register of Recognised Foreign Certification Authorities in such form as he thinks fit.

(2) A person may inspect the Register of Recognised Foreign Certification Authorities and make copies of or take extracts from the Register.

(3) The Controller shall publish a list of recognised foreign certification authorities in such form and manner as he may determine.

PART XI - GENERAL

Regulation 77. Multiple services allowed.

Nothing in these Regulations shall be construed as requiring the operation as a certification authority or repository or date/time stamp service to be carried out by different persons if the person intending to operate as a certification authority, repository or date/time stamp service or any combination of such services is otherwise able to satisfy the requirements of the Act and these Regulations.

Regulation 78. Record-keeping.

(1) A licensed certification authority shall keep and maintain detailed written records documenting -

(*a*) the security measures taken to comply with the Act and these Regulations;

(*b*) if the licensed certification authority generates a key pair for a subscriber, the relevant time at which and the manner in which the private key is distributed or transmitted to the subscriber;

(*c*) the relevant time at which and the manner in which a certificate is issued and distributed or transmitted to the subscriber;

(*d*) the certificates issued by it in such a way that the data and its unfalsified condition may be verified at any time; and

(*e*) all other measures taken to comply with the Act and these Regulations.

(2) The records required under subregulation (1) shall include evidence demonstrating that the licensed certification authority has -

(*a*) confirmed the identification of the person named in a certificate that the licensed certification authority has issued;

(*b*) confirmed the identification of the person requesting revocation of each certificate that the licensed certification authority has revoked;

(*c*) confirmed all other facts listed as confirmed in a certificate that the licensed certification authority has issued; and

(*d*) complied with the Act and these Regulations in issuing, publishing, suspending and revoking a certificate.

(3) A licensed certification authority may require a subscriber or the agent of a subscriber to submit documentation and other evidence reasonably sufficient to enable the licensed certification authority to comply with this regulation.

(4) A recognised repository and a recognised date/time stamp service shall keep and maintain detailed written records documenting -

(*a*) the security measures; and

(*b*) all other measures,

taken to comply with the Act and these Regulations.

(5) Records kept in digital form shall be digitally signed.

Regulation 79. Books of account.

(1) A licensed certification authority, a recognised repository and a recognised date/time stamp service shall keep and maintain books of account in the manner determined by the Controller.

(2) Books of account shall be kept in either the national language or the English language.

Regulation 80. Retention and custody of records.

(1) A licensed certification authority, a recognised repository and a recognised date/time stamp service shall, unless the Controller otherwise directs, retain -

(*a*) the records required under regulation 78;

(*b*) the books of account required under regulation 79; and

(*c*) in the case of a licensed certification authority, all its records of the issuance, acceptance and any suspension or revocation of a certificate,

for not less than ten years from the date of the last entry or the date of issue, as the case may be.

(2) All the records referred to in subregulation (1) shall be retained in the custody of the licensed certification authority, recognised repository or recognised date/time stamp service, as the case may be, generating the records unless the licensed certification authority, recognised repository or recognised date/time stamp service, as the case may be, -

(*a*) contracts with another person for the record retention as required under this regulation; or

(*b*) surrenders the records to the Controller upon ceasing to act as a certification authority, repository or date/time stamp service, as the case may be.

(3) A licensed certification authority, a recognised repository and a recognised date/time stamp service shall keep its records in a secure place and in a secure manner.

Regulation 81. Technical components.

(1) The technical components required for the purposes of the Act and these Regulations shall be the technical components specified in the Fourth Schedule.

(2) The technical components referred to in subregulation (1) shall be sufficiently examined under the state of the art and the fulfillment of the requirements shall be verified by the Controller in writing.

(3) If the technical components are placed in circulation or legally manufactured in accordance with the requirements under the Act and these Regulations and which guarantee the same level of security, it may be assumed that the requirements referred to in subregulation (1) regarding technical security are fulfilled.

(4) In individual cases and when there is a good reason, the Controller may require a demonstration that the requirements referred to in subregulation (1) have been fulfilled.

(5) Any security-relevant changes in technical components shall be apparent to the user.

(6) The technical components used for the purposes of the Act and these Regulations shall be protected from unauthorised access and unauthorised modification.

(7) The Controller shall keep and maintain a catalogue of suitable security measures that shall be taken into account in the design of the technical components.

(8) For the purposes of these Regulations, the expressions "unauthorised access" and "unauthorised modification" shall have the meaning assigned to them under the Computer Crimes Act 1997 [*Act 563*].

Regulation 82. Data protection.

(1) A licensed certification authority, a recognised repository and a recognised date/time stamp service shall collect personal data only directly from the affected person and only in so far as it is necessary for the purposes of the Act and these Regulations.

(2) Data from a third party, may only be collected if the person affected gives that person's prior written consent.

(3) Data collected under the Act and these Regulations shall only be used for the purposes of the Act and these Regulations unless -

(*a*) it is permitted by written law to be used for other purposes; or

(*b*) the person affected has given that person's written consent for the data to be used for other purposes.

(4) If a subscriber uses a pseudonym with the approval of the licensed certification authority, the licensed certification authority shall transmit data concerning the subscriber's identity on the request of the proper authorities in so far as it is necessary to prosecute offences or to protect against threats to public safety or public order.

(5) If information is transmitted under subregulation (4), such information shall be documented by the relevant authority.

Regulation 83. Review of software, etc.

(1) The Controller shall keep the suitability of software, hardware, technical components, algorithms, standards and other pertinent parameters relating to the generation of digital signature key pairs, the hashing of the data to be digitally signed and the creation and verification of digital signatures under review, and may periodically publish reports of the reviews.

(2) The period of suitability of the software, hardware, technical components, algorithms, standards and other pertinent parameters reviewed under subregulation (1) shall be specified in the report.

(3) Suitability shall be considered present if throughout a specified period, being not less than six years after the time of assessment, any detectable forging of digital signatures or manipulation of digitally signed data can be ruled out with near certainty by means in accordance with current scientific and technological standards and taking relevant international standards into account.

(4) The reports referred to in subregulation (1) may be made available to the public on payment of the prescribed fee.

Regulation 84. Directives and administrative orders.

(1) The Controller may issue directives and other administrative orders to licensed certification authorities, subscribers, recognised repositories, recognised date/time stamp services and qualified auditors in relation to the implementation and enforcement of the Act and these Regulations as the Controller considers necessary.

(2) A person who contravenes a directive or order issued under subregulation (1) commits an offence and shall on conviction be liable to a fine not exceeding ten thousand ringgit or to imprisonment for a term not exceeding three months or to both.

Regulation 85. Guidelines.

The Controller may issue guidelines to licensed certification authorities, subscribers, recognised repositories, recognised date/time stamp services and qualified auditors in respect of -

(*a*) what constitutes or satisfies the requirements for a trustworthy system;

(*b*) suitable security measures;

(*c*) the determination of recommended reliance limits;

(*d*) qualified auditors and audits required under the Act and these Regulations; and

(*e*) such other matters as the Controller thinks fit.

THIRD SCHEDULE [Subregulation 35(2)] - PARTICULARS TO BE INCORPORATED IN CERTIFICATION PRACTICE STATEMENT

1. A statement as to the purpose and effect of the Certification Practice Statement.

2. A statement advising the potential subscriber to ensure that before the potential subscriber applies for, uses or relies upon a certificate issued by the licensed certification authority -

(*a*) the licensed certification authority has provided sufficient information to the potential subscriber to become familiar with -

(i) digital signatures and certificates;

(ii) the application, requirements and effect of the Digital Signature Act 1997 and the regulations made under the Act as well as the directives, orders and guidelines issued under the Act;

(iii) the rights, duties and liabilities of the licensed certification authority;

(iv) the rights, duties and liabilities of the subscriber; and

(v) the rights and duties of a recipient of the subscriber's digital signature; and

(*b*) the licensed certification authority has informed the potential subscriber of any restrictions or limitations on its licence.

3. A statement of the services provided by the licensed certification authority and the fees and charges therefor.

4. A statement with regard to the operating procedure of the licensed certification authority, in particular in relation to the application for and the issue, suspension and revocation of, certificates.

5. A statement with regard to the different classes of certificates available and that the potential subscriber

must decide which class of certificate is right for the subscriber's needs.

6. A statement with regard to the determination of the recommended reliance limit for a certificate and that the potential subscriber must decide the amount of the recommended reliance limit that is right for the subscriber's needs.

7. A statement with regard to the procedure for claims against the licensed certification authority.

8. A statement with regard to the protection and use of data obtained from the potential subscriber.

9. A statement advising the potential subscriber in respect of the generation of key pairs and the need to keep the private key secure from compromise and in a trustworthy manner and that software and hardware used must satisfy the technical components prescribed under the Digital Signature Act 1997.

10. A statement advising the potential subscriber that before communicating any certificate to another person, or otherwise inducing their use or reliance on it, the subscriber must accept the certificate, and that upon such acceptance, certain representations by the subscriber will be implied.

11. A statement advising the potential subscriber to immediately notify the licensed certification authority of the compromise of the subscriber's private key.

12. A statement advising the potential subscriber that if the subscriber is the recipient of a digital signature or certificate, the subscriber, as recipient, is responsible for deciding whether to rely on it, and that before making that determination, the subscriber should check the repository of the licensed certification authority issuing the certificate or certifying the public key listed in the certificate to confirm that the certificate is valid and not revoked or suspended. Then the subscriber should use the certificate the subscriber received to verify that the digital signature received was created during the operational period of the certificate by the private key corresponding to the public key listed in the certificate, and that the message associated with the digital signature received has not been altered.

13. A statement advising the potential subscriber that data with digital signatures may need to be re-signed before the security value of an available digital signature decreases with time.

14. A statement advising the potential subscriber that if a time-stamp is required under any written law or if a particular time may be significant with regard to the use of digitally signed data, a time-stamp by a recognised date/time stamp service should be appended or attached to the message or digital signature or other document.