Electronic Transactions (Certification Authority) Regulations 2010

Table of Contents

No. S 650

ELECTRONIC TRANSACTIONS ACT 2010
(ACT 16 OF 2010)

ELECTRONIC TRANSACTIONS (CERTIFICATION AUTHORITY) REGULATIONS 2010

In exercise of the powers conferred by sections 22, 36 and 38 of the Electronic Transactions Act 2010, RAdm (NS) Lui Tuck Yew, Senior Minister of State, charged

with the responsibility of the Minister for Information, Communications and the Arts, hereby makes the following Regulations:

PART I

PRELIMINARY

Citation and commencement

1. These Regulations may be cited as the Electronic Transactions (Certification Authority) Regulations 2010 and shall come into operation on 1st November 2010.

Definitions

2. In these Regulations, unless the context otherwise requires —

"accreditation" means accreditation granted under these Regulations;

"accredited certification authority" means a certification authority that is accredited under these Regulations;

"accreditation mark" means an accreditation mark as set out in the Schedule;

"subscriber identity verification method" means the method used to verify and authenticate the identity of a subscriber;

"trusted person" means any person who has —

(*a*) direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or these Regulations in respect of a certification authority; or

(*b*) duties directly involving the issuance, renewal, suspension, revocation of certificates (including the identification of any person requesting a certificate from an accredited certification authority), creation of private keys or administration of a certification authority's computing facilities.

PART II

ACCREDITATION OF CERTIFICATION AUTHORITIES

Application to be accredited certification authority

3.—(1) Every application to be an accredited certification authority shall be made in such form and manner as the Controller may, from time to time, determine and shall be

supported by —

(*a*) the certification practice statement of the certification authority;

(*b*) an audit report prepared in accordance with regulations 23 and 34 for compliance with the Compliance Audit Checklist published on the Controller's Internet website; and

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

(2) Upon submitting an application for accreditation, the applicant shall pay to the Controller an application fee of $1,000.

(3) The Controller shall, in such form as the Controller may determine, notify the applicant as to whether his application is successful.

(4) Upon notification that his application is successful, the applicant shall pay to the Controller an accreditation fee of $1,000 and, subject to regulation 5, the Controller shall grant accreditation to the applicant as an accredited certification authority upon such payment.

(5) The accreditation shall be subject to such conditions or restrictions as the Controller may, from time to time, determine.

(6) The accreditation shall be valid for a period of 2 years unless cancelled or suspended under the Act or these Regulations.

(7) The Controller shall not refund any fee paid under this regulation if the application is unsuccessful, withdrawn or discontinued, or if the accreditation is cancelled or suspended.

Renewal of accreditation

4.—(1) Regulation 3 (with the exception of paragraph (2) thereof) shall apply, with the necessary modifications, to an application for renewal of accreditation under this regulation as it applies to an application for accreditation under regulation 3.

(2) The Controller may allow applications for renewal of accreditation to be submitted in the form of electronic records subject to such requirements as the Controller may impose.

(3) If an accredited certification authority intends to renew its accreditation, the certification authority shall submit an application for the renewal of its accreditation not later than 3 months before the expiry of its accreditation.

(4) If an application for renewal is made later than the time prescribed in paragraph (3), the application shall be deemed to be an application under regulation 3

and the application fee prescribed in regulation 3(2) shall be payable.

(5) If the certification authority does not intend to renew its accreditation, the certification authority shall —

(*a*) inform the Controller in writing not later than 3 months before the expiry of the accreditation;

(*b*) inform all its subscribers in writing not later than 2 months before the expiry of the accreditation; and

(*c*) advertise such intention in such daily newspapers and in such manner as the Controller may determine, not later than 2 months before the expiry of the accreditation.

PART III

REFUSAL, CANCELLATION AND SUSPENSION OF ACCREDITATION

Refusal to grant or renew accreditation

5.—(1) The Controller may refuse to grant or renew an accreditation if —

(*a*) the applicant has not complied with any requirement in the Act or these Regulations;

(*b*) the applicant has not provided the Controller with such information relating to it or any person employed by or associated with it for the purposes of its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require;

(*c*) the applicant or its substantial shareholder is in the course of being wound up or liquidated;

(*d*) a receiver or a receiver and manager has been appointed to the applicant or its substantial shareholder;

(*e*) the applicant or its substantial shareholder has, whether in Singapore or elsewhere, entered into a compromise or scheme of arrangement with its creditors, being a compromise or scheme of arrangement that is still in operation;

(*f*) the applicant or its substantial shareholder or any trusted person has been convicted, whether in Singapore or elsewhere, of an offence the conviction for which involved a finding that it or he acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these Regulations;

(*g*) the Controller is not satisfied as to the qualifications or experience of the trusted person who is to perform duties in connection with the accreditation of the applicant;

(*h*) the applicant fails to satisfy the Controller that it is a fit and proper person to be accredited or that all its trusted persons and substantial shareholders are fit and proper persons;

(*i*) the Controller has reason to believe that the applicant may not be able to act in the best interest of its subscribers, customers or participants having regard to the reputation, character, financial integrity and reliability of the applicant or any of its substantial shareholders or trusted persons;

(*j*) the Controller is not satisfied as to the financial standing of the applicant or its substantial shareholder;

(*k*) the Controller is not satisfied as to the record of past performance or expertise of the applicant or its trusted person having regard to the nature of the business which the applicant may carry on in connection with the accreditation;

(*l*) there are other circumstances which are likely to lead to the improper conduct of business by, or reflect discredit on the method of conducting the business of, the applicant or its substantial shareholder or any of the trusted persons; or

(*m*) the Controller is of the opinion that it is in the interest of the public to do so.

(2) In paragraph (1), "substantial shareholder", in relation to an applicant which is a company, has the same meaning as in the Companies Act (Cap. 50).

Cancellation or suspension of accreditation

6.—(1) An accreditation shall be deemed to be cancelled if the certification authority is wound up.

(2) The Controller may cancel or suspend the accreditation of a certification authority —

(*a*) on any ground on which the Controller may refuse to grant an accreditation under regulation 5;

(*b*) if any information furnished in support of the application for the accreditation was false, misleading or inaccurate;

(*c*) if the certification authority fails to undergo or pass an audit required under regulation 34;

(*d*) if the certification authority fails to comply with a direction of the Controller made under section 23 of the Act;

(*e*) if the certification authority is being or will be wound up;

(*f*) if the certification authority has entered into any composition or arrangement with its creditors;

(*g*) if the certification authority fails to carry on business for which it was accredited;

(*h*) if the Controller has reason to believe that the certification authority or its trusted person has not performed its or his duties efficiently, honestly or fairly; or

(*i*) if the certification authority fails to comply with any condition or restriction applicable in respect of the accreditation.

(3) The Controller may cancel the accreditation of a certification authority at the request of that certification authority.

(4) The Controller shall not cancel the accreditation under paragraph (2) without first giving the certification authority an opportunity of being heard.

Inquiry into allegations of misconduct, etc.

7.—(1) The Controller may inquire into any allegation that a certification authority, its officers or employees, is or has been guilty of any misconduct or is no longer fit to continue to remain accredited by reason of any other circumstances which have led, or are likely to lead, to the improper conduct of business by it or to reflect discredit on the method of conducting business.

(2) If, after inquiring into an allegation under paragraph (1), the Controller is of the opinion that the allegation is proved, the Controller may if he thinks fit —

(*a*) cancel the accreditation of the certification authority;

(*b*) suspend the accreditation of the certification authority for such period, or until the happening of such event, as the Controller may determine; or

(*c*) reprimand the certification authority.

(3) The Controller shall, at the hearing of an inquiry into an allegation under paragraph (1) against a certification authority, give the certification authority an

opportunity of being heard.

(4) Where the Controller is satisfied, after making an inquiry into an allegation under paragraph (1), that the allegation has been made in bad faith or that it is otherwise frivolous or vexatious, the Controller may, by order in writing, require the person who made the allegation to pay any costs and expenses involved in the inquiry.

(5) The Controller may issue directions to the certification authority for compliance under section 23 of the Act as a result of making the inquiry.

(6) For the purposes of this regulation, "misconduct" means —

(*a*) any failure to comply with the requirements of the Act or these Regulations or the certification practice statement of the certification authority concerned; and

(*b*) any act or omission relating to the conduct of business of the certification authority concerned which is or is likely to be prejudicial to public interest.

Effect of cancellation or suspension of accreditation

8.—(1) A certification authority whose accreditation is cancelled or suspended under regulation 6 or 7 shall, for the purposes of the Act and these Regulations, be deemed not to be accredited from the date that the Controller cancels or suspends the accreditation, as the case may be.

(2) The cancellation or suspension of the accreditation of a certification authority shall not operate so as to —

(*a*) avoid or affect any agreement, transaction or arrangement entered into by the certification authority, whether the agreement, transaction or arrangement was entered into before or after the cancellation or suspension of the accreditation; or

(*b*) affect any right, obligation or liability arising under any such agreement, transaction or arrangement.

Appeal to Minister

9.—(1) Where the Controller —

(*a*) refuses to grant or renew an accreditation under regulation 5;

(*b*) cancels or suspends an accreditation under regulation 6; or

(*c*) cancels or suspends an accreditation, or reprimands a certification authority, under regulation 7,

any person who is aggrieved by the decision of the Controller may, within 14 days after he is notified of the decision, appeal to the Minister and the decision of the Minister shall be final.

(2) If an appeal is made against a decision made by the Controller, the Controller may, if he thinks fit, defer the execution of the decision until the appeal has been decided by the Minister or the appeal is withdrawn.

(3) In considering whether to defer the execution of the decision, the Controller shall have regard to whether the deferment is prejudicial to the interests of any subscriber of the certification authority or any other party who may be adversely affected.

(4) If an appeal is made to the Minister, a copy of the appeal shall be lodged with the Controller.

PART IV

ACCREDITATION REQUIREMENTS

Business structure

10. An applicant for accreditation must be a company operating in Singapore at the time of the application and throughout the period when it is an accredited certification authority.

Personnel

11.—(1) An applicant for accreditation shall, at the time of the application and throughout the period when it is an accredited certification authority, take reasonable measures to ensure that every trusted person —

(*a*) is a fit and proper person to carry out the duties assigned to him;

(*b*) is not an undischarged bankrupt in Singapore or elsewhere, and has not made any composition or arrangement with his creditors; and

(*c*) has not been convicted, whether in Singapore or elsewhere, of —

(i) an offence the conviction for which involved a finding that he acted fraudulently or dishonestly; or

(ii) an offence under the Act or these Regulations.

(2) Notwithstanding paragraph (1)(*c*), the Controller may allow the applicant or accredited certification authority to have a trusted person who has been convicted of an

offence referred to in that paragraph, if the Controller is satisfied that —

(*a*) the trusted person is now a fit and proper person to carry out his duties; and

(*b*) 10 years have elapsed from —

(i) the date of conviction; or

(ii) the date of release from imprisonment if he was sentenced to a term of imprisonment,

whichever is the later.

(3) Every trusted person must —

(*a*) have a good knowledge of the Act and these Regulations;

(*b*) be trained in the certification authority's certification practice statement; and

(*c*) possess the relevant technical qualifications, expertise and experience to effectively carry out his duties.

Certification practice statement

12. An accredited certification authority must have and comply with a certification practice statement approved by the Controller.

PART V

CONDUCT OF BUSINESS BY ACCREDITED CERTIFICATION AUTHORITIES

Trustworthy record keeping and archival

13.—(1) An accredited certification authority may keep its records in the form of paper documents, electronic records or any other form approved by the Controller.

(2) Such records shall be indexed, stored, preserved and reproduced so as to be accurate, complete, legible and accessible to the Controller, an auditor or an authorised officer.

Trustworthy transaction logs

14.—(1) Every accredited certification authority shall make and keep in a trustworthy manner the records relating to —

(*a*) activities in issuance, renewal, suspension and revocation of certificates

(including the process of identification of any person requesting a certificate from an accredited certification authority);

(*b*) the process of generating subscribers' (where applicable) or the accredited certification authority's own key pairs;

(*c*) the administration of an accredited certification authority's computing facilities; and

(*d*) such critical related activity of an accredited certification authority as may be determined by the Controller.

(2) Every accredited certification authority shall archive all certificates issued by it and maintain mechanisms to access such certificates for a period of not less than 7 years.

(3) Every accredited certification authority shall retain all records required to be kept under paragraph (1) and all logs of the creation of the archive of certificates referred to in paragraph (2) for a period of not less than 7 years.

Types of certificates

15.—(1) Subject to the approval of the Controller, an accredited certification authority may issue certificates of the following different levels of assurance:

(*a*) certificates which shall be considered as trustworthy certificates for the purposes of regulation 3(*b*)(i) of the Third Schedule to the Act; and

(*b*) certificates which shall not be considered as trustworthy certificates for the purposes of regulation 3(*b*)(i) of the Third Schedule to the Act.

(2) The accredited certification authority must associate a distinct certification practice statement approved by the Controller for each type of certificate issued.

(3) The accredited certification authority must draw the attention of subscribers and relying parties to the effect of using and relying on certificates that are not considered trustworthy certificates for the purposes of regulation 3(*b*)(i) of the Third Schedule to the Act.

Issuance of certificates

16.—(1) In addition to the requirements specified in paragraph 14 of the Third Schedule to the Act, every accredited certification authority shall comply with the requirements in this regulation in relation to the issuance of certificates.

(2) The certificate must contain or incorporate by reference such information as is sufficient to locate or identify one or more repositories in which notification of the

suspension or revocation of the certificate will be listed if the certificate is suspended or revoked.

(3) The practices and procedures set forth in the certification practice statement of an accredited certification authority shall contain conditions with standards higher than those conditions specified in regulation 14(2) of the Third Schedule to the Act.

(4) The subscriber identity verification method employed for issuance of certificates must be specified in the certification practice statement and is subject to the approval of the Controller during the application for accreditation.

(5) Where a certificate is issued to a person (referred to in this regulation as the new certificate) on the basis of another valid certificate held by the same person (referred to in this regulation as the originating certificate) and subsequently the originating certificate has been suspended or revoked, the certification authority that issued the new certificate must conduct investigations to determine whether it is necessary to suspend or revoke the new certificate.

(6) The accredited certification authority must provide a reasonable opportunity for the subscriber to verify the contents of the certificate before it is accepted.

(7) If the subscriber accepts the issued certificate, the accredited certification authority shall publish a signed copy of the certificate in a repository referred to in paragraph (2).

(8) Notwithstanding paragraph (7), the accredited certification authority may contractually agree with the subscriber not to publish the certificate.

(9) If the subscriber does not accept the certificate, the accredited certification authority shall not publish it.

(10) Once the certificate has been issued by the accredited certification authority and accepted by the subscriber, the accredited certification authority shall notify the subscriber within a reasonable time of any fact known to the accredited certification authority that significantly affects the validity or reliability of the certificate.

(11) The date and time of all transactions in relation to the issuance of a certificate must be logged and kept in a trustworthy manner.

Renewal of certificates

17.—(1) Regulation 16 shall apply to the renewal of certificates as it applies to the issuance of certificates.

(2) The subscriber identity verification method shall be that specified in the certification practice statement as approved by the Controller.

(3) The date and time of all transactions in relation to the renewal of a certificate must be logged and kept in a trustworthy manner.

Suspension of certificates

18.—(1) This regulation shall apply only to every accredited certification authority which allows subscribers to request for suspension of certificates.

(2) Every accredited certification authority may provide for immediate revocation instead of suspension if the subscriber has agreed in writing.

(3) Upon receiving a request for suspension of a certificate under paragraph 16 of the Third Schedule to the Act, the accredited certification authority shall ensure that the certificate is suspended and notice of the suspension published in the repository in accordance with paragraph 19 of the Third Schedule to the Act.

(4) An accredited certification authority may suspend a certificate that it has issued if the accredited certification authority has reasonable grounds to believe that the certificate is unreliable, regardless of whether the subscriber consents to the suspension; but the accredited certification authority shall complete its investigation into the reliability of the certificate and decide within a reasonable time whether to reinstate the certificate or to revoke the certificate in accordance with paragraph 17 or 18 of the Third Schedule to the Act.

(5) It is the responsibility of any person relying on a certificate to check whether a certificate has been suspended.

(6) An accredited certification authority shall suspend a certificate after receiving a valid request for suspension (in accordance with paragraph 16 of the Third Schedule to the Act); but if the accredited certification authority considers that revocation is justified in the light of all the evidence available to it, the certificate must be revoked in accordance with paragraph 17 or 18 of the Third Schedule to the Act.

(7) An accredited certification authority shall check with the subscriber or his authorised agent whether the certificate should be revoked and whether to reinstate the certificate after suspension.

(8) An accredited certification authority must terminate a suspension initiated by request if the accredited certification authority discovers and confirms that the request for suspension was made without authorisation by the subscriber or his authorised agent.

(9) If the suspension of a certificate leads to a revocation of the certificate, the requirements for revocation shall apply.

(10) The date and time of all transactions in relation to the suspension of certificates

must be logged and kept in a trustworthy manner.

(11) An accredited certification authority must maintain facilities to receive and act upon requests for suspension at all times of the day and on all days of every year.

Revocation of certificates

19.—(1) In order to confirm the identity of the subscriber or authorised agent making a request for revocation under paragraph 17(*a*) of the Third Schedule to the Act, the accredited certification authority must use the subscriber identity verification method specified in the certification practice statement for this purpose.

(2) An accredited certification authority must, after receiving a request for revocation, verify the request, revoke the certificate and publish notification of it under paragraph 20 of the Third Schedule to the Act.

(3) An accredited certification authority must maintain facilities to receive and act upon requests for revocation at all times of the day and on all days of every year.

(4) An accredited certification authority shall give notice to the subscriber immediately upon the revocation of a certificate.

(5) The date and time of all transactions in relation to the revocation of certificates must be logged and kept in a trustworthy manner.

Expiry date of certificates

20. A certificate must state the date on which it expires.

Maintenance of certification practice statement

21.—(1) Every accredited certification authority shall use the Internet draft of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, adopted by the Internet Engineering Task Force and reproduced by the Controller on its Internet website, as a guide for the preparation of its certification practice statement.

(2) Any change to the certification practice statement during the term of the accreditation requires the prior approval of the Controller.

(3) Every accredited certification authority must highlight to its subscribers any limitation of their liabilities and, in particular, it must draw the subscribers' attention to the implication of reliance limits on their certificates.

(4) The subscriber identity verification method for the issuance, renewal, suspension and revocation of a certificate must be specified in the certification practice statement.

(5) A copy of the latest version of the certification practice statement, together with its effective date, must be filed with the Controller and published on the certification authority's Internet website accessible to members of the public.

(6) After the effective date, the latest version filed with the Controller will be the prevailing version for a particular certificate.

(7) Every accredited certification authority must log all changes to the certification practice statement together with the effective date of each change.

(8) An accredited certification authority shall keep in a trustworthy manner a copy of each version of the certification practice statement, together with the date it came into effect and the date it ceased to have effect.

Secure digital signatures

22.—(1) The technical implementation of the requirements in paragraph 3 of the Third Schedule to the Act shall be such as to ensure that it is computationally infeasible for any person, other than the person to whom the signature correlates, to have created a digital signature which is verified by reference to the public key listed in that person's certificate.

(2) The signature on its own should be such as to —

(*a*) ensure that the name or other unique identifiable notation of the person to whom the signature correlates be incorporated as part of the signature and cannot be replaced or forged; and

(*b*) readily present such indicia of identity to a person intending to rely on the signature.

(3) The technical implementation should ensure that —

(*a*) the steps taken towards the creation of the signature must be under the direction of the person to whom the signature correlates; and

(*b*) no other person can reproduce the sequence of steps to create the signature and thereby create a valid signature without the involvement or the knowledge of the person to whom the signature correlates.

(4) The technical implementation should indicate to a relying party of a signature whether the document or record that the signature purports to sign has been modified in any way and this indication should be revealed in the process of verifying the signature.

Compliance Audit Checklist

23.—(1) Every accredited certification authority shall ensure that in the performance of its services it materially satisfies the Compliance Audit Checklist determined by the Controller and published on the Controller's Internet website.

(2) An auditor, when determining whether a departure from the Compliance Audit Checklist is material, shall exercise reasonable professional judgment as to whether a condition that does not strictly comply with the Compliance Audit Checklist is or is not material, taking into consideration the circumstances and the system as a whole.

(3) Without prejudice to the generality of situations which the auditor may consider to be material, the following incidents of non-compliance shall be considered to be material:

(*a*) any non-compliance relating to the validity of a certificate;

(*b*) the performance of the functions of a trusted person by a person who is not suitably qualified; or

(*c*) the use by an accredited certification authority of any system other than a trustworthy system.

(4) The Compliance Audit Checklist shall be interpreted in a manner that is reasonable in relation to the context in which a system is used and is consistent with law.

(5) Notwithstanding an auditor's assessment of whether a departure from the Compliance Audit Checklist is material, the Controller may make his own assessment and reach a conclusion for the purpose of paragraph (1) which is at variance with that of the auditor.

(6) Every accredited certification authority shall provide every subscriber with a trustworthy system to generate his key pair.

(7) Every accredited certification authority shall provide the mechanism to generate and verify digital signatures in a trustworthy manner and the mechanism provided shall also indicate the validity of the signature.

(8) If the digital signature is not valid, the mechanism provided should indicate if the invalidity is due to the integrity of the document or the signature and the mechanism provided shall also indicate the status of the certificate.

(9) For mechanisms provided by third parties other than the accredited certification authority, the resulting signature is considered secure only if the accredited certification authority endorses the implementation of such mechanisms in conjunction with its certificate.

(10) Every accredited certification authority shall be responsible for the storage of keys (including the subscriber's key and the accredited certification authority's own key)

in a trustworthy manner.

(11) The Controller may, from time to time, publish on its Internet website further details of the Compliance Audit Checklist for compliance by every accredited certification authority.

Incident handling

24.—(1) An accredited certification authority shall implement an incident management plan that must provide at the least for management of the following incidents:

(*a*) compromise of key;

(*b*) penetration of certification authority system and network;

(*c*) unavailability of infrastructure; and

(*d*) fraudulent registration and generation of certificates, certificate suspension and revocation information.

(2) If any incident referred to in paragraph (1) occurs, it shall be reported to the Controller within 24 hours.

Confidentiality

25.—(1) Every accredited certification authority and its authorised agent must keep all subscriber-specific information confidential.

(2) Paragraph (1) shall not apply to —

(*a*) any disclosure of subscriber-specific information made —

(i) with the permission of the subscriber;

(ii) for the purposes of the administration or enforcement of section 23 or 24 or Part VI of the Act;

(iii) for any prosecution under any written law; or

(iv) in compliance with an order of court or the requirement of any written law; or

(*b*) any subscriber-specific information which —

(i) is contained in the certificate, or is otherwise provided by the subscriber to the accredited certification authority, for public disclosure; or

(ii) relates to the fact that the certificate has been suspended or revoked.

Change in management

26.—(1) An accredited certification authority shall notify the Controller within 5 days of any changes in —

(*a*) the appointment of any person as a member of its board of directors, its chairman or its chief executive, or their equivalent; or

(*b*) any persons with a controlling interest in the certification authority.

(2) For the purposes of paragraph (1)(*b*), a person has a controlling interest in a certification authority if —

(*a*) that person has an interest in the voting shares of the certification authority and exercises control over the certification authority; or

(*b*) that person has an interest in the voting shares of the certification authority of an aggregate of not less than 30% of the total votes attached to all voting shares in the certification authority, unless he does not exercise control over the certification authority.

(3) The notification required in relation to paragraph (1)(*b*) shall be in such form as the Controller may require and shall include the following information:

(*a*) the name of the person with a controlling interest; and

(*b*) the percentage of the voting shares in the certification authority acquired by that person.

PART VI

REQUIREMENTS FOR REPOSITORY

Availability of general purpose repository

27.—(1) A general purpose repository shall be available at all times of the day and on all days of every year.

(2) A general purpose repository must ensure that the total aggregate period of any down time in any period of one month shall not exceed 0.3% of the period.

(3) Any down time, whether scheduled or unscheduled, shall not exceed 30 minutes

duration at any one time.

Specific purpose repository

28. Subject to the approval of the Controller, a repository may be dedicated for a specific purpose for which specific hours of operation may be acceptable.

PART VII

ACCREDITATION MARK

Use of accreditation mark

29. Any person who, not being an accredited certification authority, uses an accreditation mark or a colourable imitation thereof shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 12 months or to both.

PART VIII

APPLICATION TO PUBLIC AGENCIES

Application to public agencies

30.—(1) For the purposes of regulation 3(*b*)(iii) of the Third Schedule to the Act, a public agency that is approved by the Minister under that paragraph to act as a certification authority shall comply with the provisions of Parts III (with the exception of regulations 5, 6, 8 and 9), IV (with the exception of regulation 10), V (with the exception of regulation 26), VI, VII (with the exception of regulation 29), VIII and IX (with the exception of regulations 35 and 36) as if it were an accredited certification authority.

(2) The provisions referred to in paragraph (1) shall apply, with the necessary modifications and such other modifications as the Controller may determine, to a public agency referred to in that paragraph.

PART IX

ADMINISTRATION

Waiver

31.—(1) Any accredited certification authority that wishes to apply for a waiver of any of the requirements specified in these Regulations may apply in writing to the

Controller at the time when it submits an application for accreditation.

(2) The application must be supported by reasons for the application and include such supporting documents as the Controller may require.

Disclosure

32.—(1) The accredited certification authority must submit half-yearly progress and financial reports to the Controller.

(2) The half-yearly progress reports must include information on —

(*a*) the number of subscribers;

(*b*) the number of certificates issued, suspended, revoked, expired and renewed;

(*c*) system performance including system up and down time and any extraordinary incidents;

(*d*) changes in the organisational structure of the certification authority;

(*e*) changes since the preceding progress report was submitted or since the application for the accreditation; and

(*f*) changes in the particulars of any trusted person since the last submission to the Controller, including the name, identification number, residential address, designation, function and date of employment of the trusted person.

(3) The accredited certification authority has a continuing obligation to disclose to the Controller any changes in the information submitted.

(4) All current versions of the accredited certification authority's applicable certification practice statements together with their effective dates must be published in the accredited certification authority's Internet website.

Discontinuation of operations of accredited certification authority

33.—(1) If an accredited certification authority intends to discontinue its operations, the accredited certification authority may arrange for its subscribers to re-subscribe to another accredited certification authority.

(2) The accredited certification authority shall make arrangements for its records and certificates to be archived in a trustworthy manner.

(3) If the records are transferred to another accredited certification authority, the transfer must be done in a trustworthy manner.

(4) An accredited certification authority shall —

(*a*) give to the Controller written notice of its intention to discontinue its operations not later than 3 months before the discontinuation;

(*b*) give to its subscribers written notice of its intention to discontinue its operations not later than 2 months before the discontinuation; and

(*c*) advertise, in such daily newspapers and in such manner as the Controller may determine, its intention to discontinue its operations not later than 2 months before the discontinuation.

Audit

34.—(1) The Controller may, by notice in writing, require an accredited certification authority to undergo and pass an audit.

(2) The audit referred to in paragraph (1) must be —

(*a*) conducted in accordance with the auditing requirements specified in this regulation; and

(*b*) completed within such time as the Controller may, by notice in writing, specify.

(3) The audit must be conducted by a qualified independent audit team approved by the Controller for this purpose comprising of a person who is a Certified Public Accountant and a person who is a Certified Information Systems Auditor and either of whom must possess sufficient knowledge of digital signature and certificates.

(4) The firm or company to which the audit team belongs must be independent of the certification authority being audited and must not be a software or hardware vendor that is or has provided services or supplied equipment to the certification authority.

(5) Auditing fees shall be borne by the certification authority.

(6) A copy of the audit report shall be submitted to the Controller within 4 weeks of the completion of an audit.

Penalties

35. Any person who fails, without any reasonable excuse, to comply with regulation 13(2), 14, 16(2) or (11), 17(3), 18(10), 19(5), 21(7) or (8) or 25(1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000.

Composition of offences

36. Any offence under section 23(2) of the Act or under these Regulations may be compounded by the Controller under section 36 of the Act.

Revocation

37. The Electronic Transactions (Certification Authority) Regulations (Cap. 88, Rg 1) (referred to in these Regulations as the previous Regulations) are revoked.

Transitional provision

38.—(1) A certification authority which, immediately before 1st November 2010, was a licensed certification authority under the previous Regulations shall with effect from that date be deemed to be an accredited certification authority under these Regulations.

(2) The deemed accreditation under paragraph (1) shall, unless it is suspended or cancelled, and insofar as it is not inconsistent with these Regulations —

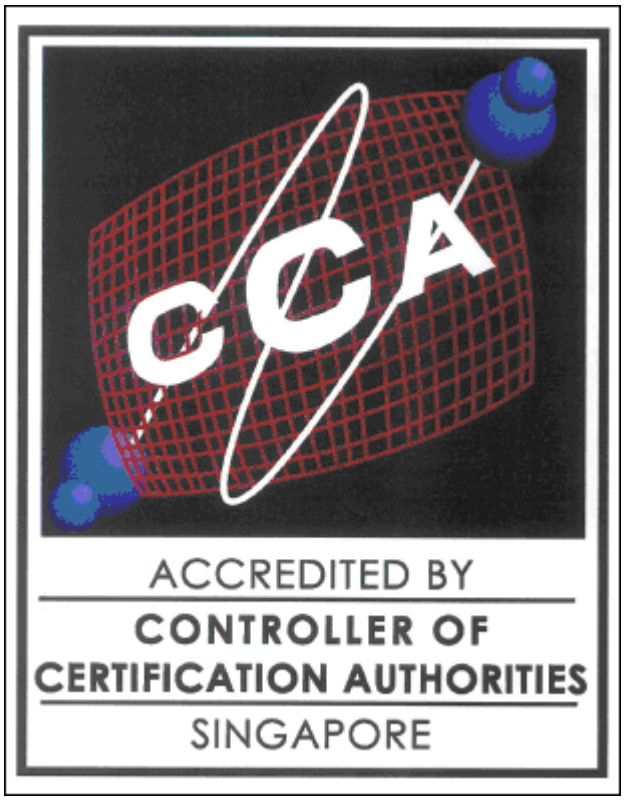
(*a*) be subject to the conditions and restrictions imposed on the licence granted under the previous Regulations; and

(*b*) expire on, and be renewable before, the date when the licence granted under the previous Regulations would have expired if these Regulations had not been enacted.

THE SCHEDULE

Regulation 2

ACCREDITATION MARK FOR ACCREDITED CERTIFICATION AUTHORITIES



Made this 28th day of October 2010.

CHAN YENG KIT
Permanent Secretary,
Ministry of Information,
Communications and the Arts,
Singapore.

[MICA ICT.271.022.017V12; AG/LLRD/SL/88/2010/1 Vol. 1]