JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT PROPOSED AMENDMENTS 2009

(Report)

LRRD No.1/2009

30 JUNE 2009

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT PROPOSED AMENDMENTS 2009

CONTENTS

REPORT

PART 1
INTRODUCTION

1.1.1 From 2004 to 2005, the Info-communications Development Authority of Singapore ("**IDA**") and the Attorney-General's Chambers ("**AGC**"), in consultation with the Ministry of Information, Communications and the Arts ("**MICA**") and the Ministry of Law, held a joint public consultation in connection with the review of the Electronic Transactions Act (Cap. 88) ("**ETA**") and Electronic Transactions (Certification Authority) Regulations ("**ETR**").

1.1.2 The public consultation was carried out in three stages[1]. **Stage I** was launched on 18 February 2004 and closed on 15 April 2004. **Stage II** was launched on 25 June 2004 and closed on 25 September 2004. **Stage III** was launched on 22 June 2005 and closed on 17 August 2005. Together, the three stages covered the following issues:

a. electronic contracting issues and the United Nations Convention on the Use of Electronic Communications in International Contracts ("**UN Convention**")[2];
b. the transactions excluded from application of the ETA;
c. the regulation of certification authorities;
d. e-Government issues; and
e. the exemption of liability for network service providers.

1.1.3 IDA and AGC would like to take this opportunity to thank all respondents for their views, which have been most useful. Parts 2 to 5 of this report highlight IDA's and AGC's policy recommendations on the first 4 issues mentioned in paragraph 1.1.2 above, after consideration of the submissions received from the pubic consultation. The Parts are arranged as follows:

Part 2 Electronic Contracting and the UN Convention
Part 3 Transactions Excluded from Application of the ETA
Part 4 Regulation of Certification Authorities
Part 5 E-Government

---

1 Soft copies of the consultation papers for Stage I (LRRD No.1/2004), Stage II (LRRD No.2/2004) and Stage III (LRRD No.1/2005) are available on the AGC website (www.agc.gov.sg, under "Publications\Law Reform Publications") and the IDA website (www.ida.gov.sg, under "Policies and Regulation → IDA Consultation Papers & Decisions").

2 The final text of the UN Convention was adopted by the General Assembly of the United Nations on 23 November 2005. The published text of the UN Convention together with Explanatory Notes (ISBN: 978-92-1-133756-3) is available at: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html

1.1.4 The issue concerning the exemption of liability for network service providers is still under consideration by MICA and AGC. A separate document on this issue will be published in due course.

1.1.5 With the completion of the public consultation, IDA and AGC proceeded to draft the necessary legislative amendments to be made to the ETA and the ETR in respect of the 4 issues mentioned in paragraph 1.1.2 above ("**Proposed Amendments**").

1.1.6 This report invites comments from industry and business professionals, the public, and Government Ministries and agencies on:

a. the Proposed Amendments to the ETA, as set out at **Annex A** ("**Proposed Bill**");
b. the Proposed Amendments to the ETR, as set out at **Annex B**; and
c. the Compliance Audit Checklist, as set out at **Annex C**.

The focus of the current exercise is to seek feedback on the Proposed Amendments and the Compliance Audit Checklist and the precision with which they reflect the proposed policy recommendations. Whilst we do not intend to re-open issues that were discussed in the earlier consultation exercises, we nonetheless welcome suggestions that will aid in refining the legislative regime.

1.1.7 When sending in your feedback, please identify clearly the specific Proposed Amendments you are commenting on and provide your reasons for any proposed changes. We also encourage you to suggest drafting changes to the Proposed Amendments to reflect your proposed changes where appropriate.

❖ Please send your feedback to the Attorney-General's Chambers, marked "**Review of ETA: Proposed Amendments 2009**":
- via e-mail, to **agc_lrrd@agc.gov.sg**;
- by post (a CD-ROM containing a soft copy would be appreciated) to "**Legislation and Law Reform Division, Attorney-General's Chambers, 1 Coleman Street, #05-04 The Adelphi, Singapore 179803**"; and/or
- via fax, to **6332 4700**.

❖ Please include your personal/company particulars as well as your correspondence address, contact number and e-mail address in your submission.

- The closing time and date for responses to this report is **5:00 p.m., Thursday, 30 July 2009**.

- A soft copy of this report can be downloaded from:
  - http://www.ida.gov.sg (under "Policies and Regulation → IDA Consultation Papers & Decisions"); or
  - http://www.agc.gov.sg (under "Publications\Law Reform Publications").

- IDA and AGC reserve the right to make public all or parts of any written submissions made in response to this report and to disclose the identity of the source. The submissions may also be quoted or referred to in subsequent publications or made available to third parties. Any part of the submission considered commercially confidential should be clearly marked and placed as a separate annex. IDA and AGC will take this into consideration when disclosing the information submitted.

PART 2
ELECTRONIC CONTRACTING AND THE UN CONVENTION

2.1 Introduction to Part

2.1.1 In LRRD No.1/2004[3], we sought comments on various changes and issues that would arise from adopting the provisions of the UN Convention (then in draft form), as well as other electronic contracting issues. In Part 5 of LRRD No.1/2005[4], we discussed changes to the draft UN Convention and sought comments on the implications of those changes for electronic contracts.

2.1.2 11 submissions were received in response to LRRD No.1/2004 and eight were received in response to Part 5 of LRRD No.1/2005.

2.1.3 In this Part, we will discuss submissions on the key issues raised in the two consultation papers, and the corresponding Proposed Amendments to the ETA. Some of the issues raised in LRRD No.1/2004 have either already been addressed in LRRD No.1/2005, or superseded by the adoption of the finalised text of the UN Convention on 23 November 2005 by the United Nations General Assembly ("**General Assembly**"). To the extent that any issue is no longer outstanding, it will not be discussed here.

2.1.4 This Part is arranged in the following order:

Part 2.2: Consent and Variation
Part 2.3: Electronic Signatures
Part 2.4: Provision of Originals
Part 2.5: Time and Place of Despatch and Receipt
Part 2.6: Invitation to Make Offers
Part 2.7: Automated Message Systems
Part 2.8: Conflicting Terms
Part 2.9: Error in Electronic Communications
Part 2.10: Applicability of the Convention
Part 2.11: Extension to Non-Contractual Transactions
Part 2.12: Formation and Validity of Contracts
Part 2.13: Effectiveness of Communications between Parties
Part 2.14: Attribution
Part 2.15: Incorporation by Reference
Part 2.16: Other Issues

[3] Consultation paper for Stage I of the *Joint IDA-AGC Public Consultation on Review of the Electronic Transactions Act: Electronic Contracting Issues*.

[4] Consultation paper for Stage III of the *Joint IDA-AGC Public Consultation on Review of the Electronic Transactions Act: Remaining Issues*.

2.2 Consent and Variation

2.2.1 We sought comments in LRRD No.1/2004[5] on whether or not to adopt a consent provision based on Article 8(2) of the draft UN Convention. We also noted that the existing section 5 of the ETA allowed parties to an electronic transaction to vary the provisions of the existing Parts II and IV[6] of the ETA by mutual agreement, and considered:

a. whether to amend or replace the provision in view of overlap with other provisions making specific sections apply subject to agreement otherwise;

b. the need for mandatory requirements which should not be open to variation by agreement of the parties; and

c. whether a variation provision would be necessary if there were a consent provision.

2.2.2 We discussed the comments from respondents to LRRD No.1/2004 in LRRD No.1/2005[7].

2.2.3 Article 8(2) of the UN Convention, as adopted by the General Assembly, remains the same as that reviewed in LRRD No.1/2004 and LRRD No.1/2005. The final adopted text reads as follows:

> "*2. Nothing in this Convention requires a party to use or accept electronic communications, but a party's agreement to do so may be inferred from the party's conduct.*"

2.2.4 Considering the submissions received in response to LRRD No.1/2004 and the views we expressed in LRRD No.1/2005[8], **we propose the following:**

a. **We propose to adopt, in new section 5(1) of the Proposed Bill, a provision reflecting Article 8(2) of the UN Convention in the context of all electronic transactions**, including non-contractual transactions. As stated in the first part of Article 8(2), it is amply clear there is nothing in the UN Convention that creates any

[5] See Part 2 of LRRD No.1/2004.
[6] We have consolidated the existing Parts II and IV of the ETA into a single Part II in the Proposed Bill.
[7] See Part 5.7 of LRRD No.1/2005.
[8] See footnote 7.

substantive requirement for agreement or consent by the parties as to the form of their communications. It is unnecessary to mirror the provision in the Proposed Bill. In the context of Singapore domestic law, however, there may be legal requirements for agreement or consent by the parties before a particular form of communication can be used. These requirements may arise under a specific rule of law[9], or a contract or other legal obligation between the parties. The first part of section 5(1) therefore seeks to clarify that Part II of the Proposed Bill does not affect any such existing requirements. The second part of Article 8(2) has been adopted to clarify that such agreement or consent may be inferred from the conduct of the parties. However, this provision should not override any requirement that the agreement or consent itself must be in a particular form. It is therefore clarified that the consent may be inferred "*unless otherwise agreed or provided by a rule of law*".

b. **We propose to amend the existing section 5 of the ETA to align the wording more closely with Article 3 of the UN Convention** and to clarify the position discussed in paragraph 2.2.5 below.

c. **We propose to remove any wording in the sections in the existing Parts II and IV[10] of the ETA that make those sections apply subject to agreement otherwise of the parties**. This is to avoid overlap with section 5(3) of the Proposed Bill.

[9] Examples:

- A notice of cancellation under the Consumer Protection (Fair Trading) (Cancellation of Contracts) Regulations 2009 (G.N. No. S 65/2009) must be given in a prescribed form and delivered, sent by post or facsimile transmission to the supplier. The notice may be given by other means, including electronic means, if the supplier agrees to accept such notice: regulation 4(9) and (11).
- The existing section 47 of the ETA (and similarly section 37 of the Proposed Bill) allows certain documents to be submitted to public agencies in electronic form if the public agency decides to perform the function electronically and in the form and manner specified by the public agency.

[10] See footnote 6.

2.2.5 The majority of respondents to LRRD No.1/2004 agreed that parties should not, by agreement, be able modify the underlying rules of law as to the minimum standards for electronic functional equivalents. UNCITRAL has confirmed this position with regard to Article 3 of the UN Convention in the following passages[11]:

> "*137. Nevertheless, the Convention recognizes that form requirements exist and that they may limit the ability of the parties to choose their means of communication. The Convention offers criteria under which electronic communications can meet general form requirements. However, nothing in the Convention implies that the parties have an unlimited right to use the technology or medium of their choice in connection with formation or performance of any type of contract, so as not to interfere with the operation of rules of law that may require, for instance, the use of specific authentication methods in connection with particular types of contract (see A/CN.9/571, para. 119).*"
>
> "*85. …it was generally accepted that party autonomy did not extend to setting aside statutory requirements that imposed, for instance, the use of specific methods of authentication in a particular context. This is particularly important in connection with article 9 of the Convention, which provides criteria under which electronic communications and their elements (e.g. signatures) may satisfy form requirements, which are normally of a mandatory nature since they reflect decisions of public policy. Party autonomy does not allow the parties to relax statutory requirements (for example, on signature) in favour of methods of authentication that provide a lesser degree of reliability than electronic signatures, which is the minimum standard recognized by the Convention (see A/CN.9/527, para. 108; see also A/CN.9/571, para. 76).*"
>
> "*86. Nevertheless, as provided in article 8, paragraph 2, the Convention does not require the parties to accept electronic communications if they do not want to. This also means, for instance, that the parties may choose not to accept electronic signatures (see A/CN.9/527, para. 108).*"

[11] Paragraphs 137, 85 and 86 of the Explanatory Notes on the United Nations Convention on the Use of Electronic Communications in International Contracts (ISBN: 978-92-1-133756-3), available at: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html. See also paragraph 14:

> "*14. It should be noted that article 9 establishes minimum standards to meet form requirements that may exist under the applicable law. The principle of party autonomy in article 3, which is also contained in other UNCITRAL instruments, such as in article 6 of the United Nations Sales Convention, should not be understood as allowing the parties to go as far as relaxing statutory requirements on signature in favour of methods of authentication that provide a lesser degree of reliability than electronic signatures. Generally, it was understood that party autonomy did not mean that the Electronic Communications Convention empowered the parties to set aside statutory requirements on form or authentication of contracts and transactions.*"

2.2.6 New section 5(2) aligns the wording of existing section 5 of the ETA more closely with Article 3 of the UN Convention. It does not apply to sections 7 to 10 of the Proposed Bill as it is not intended that parties should be able to relax the minimum standards prescribed by those sections for electronic forms to achieve functional equivalence in respect of requirements under rules of law for writing, signatures, retention and originals respectively. New section 5(3) clarifies that parties to a contract or transaction may nevertheless, by agreement, exclude the use of electronic forms or impose additional requirements in respect of their use in relation to their contracts or transactions.

2.3 Electronic Signatures

2.3.1 In LRRD No.1/2004[12] and LRRD No.1/2005[13], we sought comments on Article 9(3) of the draft UN Convention, the definition of electronic signatures and the reliability requirement it contained, and the comments [14] we submitted to the United Nations Commission on International Trade Law ("**UNCITRAL**") in relation to this issue.

2.3.2 Article 9(3) of the UN Convention, as adopted by the General Assembly, reads as follows:

> "*Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:*
>
> *(a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and*
>
> *(b) The method used is either:*
>
> *(i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or*

[12] See Part 3 of LRRD No.1/2004.
[13] See Part 5.10 of LRRD No.1/2005.
[14] See Annex C of LRRD No.1/2005.

(ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence."

2.3.3 The final adopted text of Article 9(3)(a) of the UN Convention incorporates our comments to UNCITRAL that an electronic signature need not necessarily imply a party's approval of the entire communication to which it is affixed. The more appropriate phrase "*indicate that party's intention in respect of the information contained*" was adopted.[15]

2.3.4 UNCITRAL retained Article 9(3)(b) of the draft UN Convention (now Article 9(3)(b)(i) of the UN Convention), taking the view that the "reliability test" remained relevant to remind courts of the need to take into account factors other than technology (e.g., the relevant agreement of the parties) in ascertaining whether an electronic signature used was sufficient to identify the signatory[16]. However, to address the concerns raised, UNCITRAL introduced a new Article 9(3)(b)(ii) to prevent parties from relying on Article 9(3)(b)(i) to repudiate their signatures where there is no dispute as to the authenticity of the signature. Article 9(3)(b)(ii) validates a signature method - regardless of its reliability in principle - whenever the method used is proven in fact to have identified the signatory and to have indicated the signatory's intention in respect of the information contained in the electronic communication[17].

2.3.5 **For consistency with the UN Convention, we propose to amend the existing section 8 of the ETA to align it with the final adopted text for Article 9(3)(b) of the UN Convention**. (See section 8 of the Proposed Bill.)

2.4 Provision of Originals

2.4.1 In LRRD No.1/2004[18], we discussed the issue of electronic originals and, in LRRD No.1/2005[19], we proposed to include a new provision in the ETA for any document, record or information provided or retained in electronic form to be regarded as the functional equivalent of an original, subject to various conditions relating to integrity and accessibility being

[15] See paragraph 160 of Explanatory Notes on the United Nations Convention on the Use of Electronic Communications in International Contracts (ISBN: 978-92-1-133756-3), available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.
[16] *Ibid*, at paragraph 163.
[17] *Ibid*, at paragraph 164.
[18] See Part 7.2 of LRRD No.1/2004.
[19] See Part 5.11 of LRRD No.1/2005.

met. This was for alignment with Articles 9(4), 9(5) and 9(6) of the draft UN Convention.

2.4.2 In their comments to LRRD No.1/2005, respondents did not raise objections for this general provision to be included in the ETA. However, one respondent re-iterated that the singularity of originals might be an issue.

2.4.3 Articles 9(4) and 9(5) of the UN Convention, as adopted by the General Assembly, remains the same as that reviewed in LRRD No.1/2005, save for some minor editorial changes to Article 9(4)(b). The final adopted text reads as follows:

> *"4. Where the law requires that a communication or a contract should be made available or retained in its original form, or provides consequences for the absence of an original, that requirement is met in relation to an electronic communication if:*
>
> *(a) There exists a reliable assurance as to the integrity of the information it contains from the time when it was first generated in its final form, as an electronic communication or otherwise; and*
>
> *(b) Where it is required that the information it contains be made available, that information is capable of being displayed to the person to whom it is to be made available.*
>
> *5. For the purposes of paragraph 4 (a):*
>
> *(a) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and*
>
> *(b) The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.*"

2.4.4 Draft Article 9(6) [20] was omitted from the UN Convention as UNCITRAL decided that Contracting States that wished to exclude those categories of documents from the UN Convention should do so by way of declarations under the present Article 19 of the UN Convention[21]. In any case, such an exclusion may not be necessary as the documents to be presented for payment under a letter of credit or a bank guarantee are likely to have been agreed on between the parties. (See paragraph 2.4.6 below on exclusion or variation of the relevant ETA provisions by agreement.)

2.4.5 Having considered the submissions received, **we propose to adopt the provision as section 10 of the Proposed Bill** [22].

2.4.6 Concerning the singularity issue, we would highlight that under new section 5(2) of the Proposed Bill (see Part 2.2 above), parties would have the flexibility to decide whether or not to use, and the additional safeguards to be adopted in respect of, documents in electronic form if this might pose issues of singularity. Further, negotiable instruments and documents of title, for which singularity would be an important issue, will continue to be excluded from the application of the ETA[23]. As we suggested in LRRD No.1/2005, specific legislation could be made to cater for originals in relation to such matters when appropriate[24].

2.5 Time and Place of Despatch and Receipt

2.5.1 In LRRD No.1/2004[25], we sought comments on the existing section 15 of the ETA (which provides for the time of despatch and receipt of an electronic record) and on our proposal to align section 15 with Article 10 of the draft UN Convention. Various concerns were raised by respondents in response to LRRD No.1/2004.

---

[20] Article 9(6) of the draft UN Convention, which was quoted in LRRD No. 1/2005, read as follows: "*Paragraphs 4 and 5 do not apply where a rule of law or the agreement between the parties requires a party to present certain original documents for the purpose of claiming payment under a letter of credit, a bank guarantee or a similar instrument.*"

[21] *Report of the United Nations Commission on International Trade Law on the work of its thirty-eighth session (4-15 July 2005)* (A/60/17), at paragraphs 74 to 76.

[22] Section 10(1)(*b*) of the Proposed Bill adopts the wording of Article 9(4)(b) of the UN Convention. The additional requirement that the document, record or information must be "*capable of being retained … for subsequent reference*" in the consultation draft of the provision in Annex B of LRRD No.1/2005 (section 9A(1)(b)) has been omitted. As noted in paragraph 5.11.13 of LRRD No.1/2005, such a requirement (found in the electronic transactions legislation of some other jurisdictions) may not be necessary or relevant where the original is required only for the purposes of once-off validation.

[23] See Part 3.3 below.

[24] See paragraph 5.11.9 of LRRD No.1/2005.

[25] See Part 5 of LRRD No.1/2004.

2.5.2 UNCITRAL subsequently made various changes to Article 10 of the draft UN Convention which have addressed these concerns. In LRRD No.1/2005[26], we discussed the changes made to Article 10 of the draft UN Convention.

2.5.3 In their comments to LRRD No.1/2005, respondents were generally supportive of the alignment, stating that this would provide greater clarity on the time and place of despatch of electronic communications.

2.5.4 Article 10 of the UN Convention, as adopted by the General Assembly, remains the same as that reviewed in LRRD No.1/2004 and LRRD No.1/2005, save for some minor editorial changes to Articles 10(1) and 10(2). The final adopted text reads as follows:

> *"1. The time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.*
>
> *2. The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. The time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.*
>
> *3. An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business, as determined in accordance with article 6.*

[26] See Part 5.12 of LRRD No.1/2005.

> *4. Paragraph 2 of this article applies notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under paragraph 3 of this article.*"

2.5.5 After considering the submissions received, **we propose to align the drafting of existing section 15 of the ETA with Article 10 of the UN Convention**. (See section 13 of the Proposed Bill.) **We also propose to delete the existing section 14 of the ETA as it would otherwise conflict with the new section 13 of the Proposed Bill**. Further, the existing section 14 of the ETA may no longer be necessary as parties and courts are now more comfortable with electronic communications and may thus no longer need the assurance provided by the rules in that section.

2.6 Invitation to Make Offers

2.6.1 In LRRD No.1/2004[27], we sought comments on a proposal to adopt, in the ETA, a provision similar to Article 12 of the draft UN Convention, which makes it the default rule that electronic communications proposing to conclude contracts, and addressed to the world at large, are to be treated as invitations to make offers (i.e., invitations to treat), subject to any clear indication that the person making the proposal intended it to be an offer capable of immediate acceptance.

2.6.2 In LRRD No.1/2005[28], we discussed the comments of respondents to LRRD No.1/2004 and reiterated our proposal to adopt a provision similar to Article 12 of the draft UN Convention (by then renumbered as Article 11).

2.6.3 In their comments to LRRD No.1/2005, respondents were generally supportive of our proposal as it would provide certainty in relation to the invitations to make offers.

2.6.4 Article 11 of the UN Convention, as adopted by the General Assembly, remains the same as that reviewed in LRRD No.1/2004 and LRRD No.1/2005, and reads as follows:

> "*A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties*

[27] See Part 4.2 of LRRD No.1/2004.
[28] See Part 5.13 of LRRD No.1/2005.

> *making use of information systems, including proposals that make use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.*"

2.6.5 After considering the submissions received, **we propose to include a new provision, as section 14 of the Proposed Bill, in line with Article 11 of the UN Convention**.

2.7 Automated Message Systems

2.7.1 In LRRD No.1/2004[29] and LRRD No.1/2005[30], we sought comments on a proposal to adopt, in the ETA, a provision similar to Article 12 of the draft UN Convention[31], which provides that contracts formed through the use of automated message systems will not be denied validity or enforceability on the sole ground that no person reviewed each of the individual actions carried out by such systems or the resulting agreement.

2.7.2 Article 12 of the UN Convention, as adopted by the General Assembly, is the same as that set out in LRRD No.1/2005[32], save for the minor addition of the words "*or intervened in*" (in bold below). The final adopted text reads as follows:

> "*A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed* ***or intervened in*** *each of the individual actions carried out by the automated message systems or the resulting contract.*"

2.7.3 Respondents were generally supportive of the proposal. However, one respondent raised the concern of there being fewer opportunities to detect and rectify errors because of the lack of human involvement.

2.7.4 After considering the submissions received, **we propose to include a new provision, as section 15 of the Proposed Bill, in line with Article 12 of the UN Convention**. As for the concern on errors, this concern has been addressed as we have also proposed to include a new provision,

[29] See Part 6.2 of LRRD No.1/2004.
[30] See Part 5.14 of LRRD No. 1/2005.
[31] At the time of issue of LRRD No.1/2004, Article 12 of the draft UN Convention was numbered as Article 14.
[32] See footnote 30.

as section 16 of the Proposed Bill, to deal with input errors (see Part 2.9 below).

2.8 Conflicting Terms

2.8.1 In connection with the subject of automated message systems discussed in Part 2.7 above, we also invited comments in LRRD No.1/2004[33] on how to resolve the issue of conflicting terms in contracts concluded by such systems.

2.8.2 Various methods were suggested by respondents, but the most common solution proposed was to leave the issue to be addressed by normal contract law rules.

2.8.3 After considering the submissions received, **we believe that the best approach to the issue would be to allow normal contract law rules to prevail and therefore propose not to adopt any provision in the ETA concerning this issue**.

2.9 Error in Electronic Communications

2.9.1 In LRRD No.1/2004[34] and LRRD No.1/2005[35], we sought comments on a proposal to adopt, in the ETA, a provision similar to Article 14 of the UN Convention[36], which allows for electronic communications to be withdrawn by the maker if certain conditions are met.

2.9.2 Respondents were generally supportive of our proposal as it would provide clarity on how input errors would affect electronic communications.

2.9.3 Article 14 of the UN Convention, as adopted by the General Assembly, reads as follows:

> *"1. Where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has*

[33] See Part 6.3 of LRRD No.1/2004.
[34] See Part 6.5 of LRRD No.1/2004.
[35] See Part 5.15 of LRRD No.1/2005.
[36] At the time of issue of LRRD No.1/2004, Article 14 of the draft UN Convention was numbered as Article 16.

*the right to withdraw **the portion of** the electronic communication in which the input error was made if:*

(a) The person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and

(b) The person, or the party on whose behalf that person was acting, has not used or received any material benefit or value from the goods or services, if any, received from the other party.

2. Nothing in this article affects the application of any rule of law that may govern the consequences of any error other than as provided for in paragraph 1."

2.9.4 The words "*the portion of*" (in bold above) were added in the chapeau of Article 14(1) of the UN Convention to clarify that only the erroneous portion of the communication could be withdrawn. UNCITRAL decided to delete Article 14(1)(b)[37] since it related to the consequences of the error, which should be left for national law to determine[38]. Article 14(2) was amended to clarify that the specific remedy for input errors in Article 14(1) was not intended to interfere with the general doctrine on error that existed in national laws[39]. Accordingly, whether any withdrawal under Article 14(1) would result in the invalidation of the communication or transaction would depend on the nature of the portion withdrawn. If, for example, the portion withdrawn concerned the quantity of goods ordered, the withdrawal would be likely to result in the invalidation of the transaction as the quantity of goods ordered is an essential term for a contract for the sale of goods. It should also be noted that Article 14 does not provide a right to "correct" the error made.

2.9.5 After considering the submissions received, **we propose to include a new provision, as section 16 of the Proposed Bill, in line with Article 14 of the UN Convention**.

---

[37] Article 14(1)(b) of the draft UN Convention provided for an additional condition to be met before the right of withdrawal would accrue. The condition was that "*the person, or the party on whose behalf that person was acting, takes reasonable steps, including steps that conform to the other party's instructions, to return the goods or services received, if any, as a result of the error or, if instructed to do so, to destroy the goods or services*".

[38] *Report of the United Nations Commission on International Trade Law on the work of its thirty-eighth session (4-15 July 2005)* (A/60/17), at paragraph 101.

[39] *Ibid.*, at paragraph 104.

2.10 Applicability of the Convention

2.10.1 In LRRD No.1/2005[40], we sought comments on whether there should be any additional exclusions [41] from the applicability of the UN Convention[42], and whether to adopt any of the exclusions listed in Article 18(1) of the draft UN Convention (now Article 19(1) of the UN Convention)[43].

2.10.2 Respondents did not propose any further exclusions from the applicability of the UN Convention. They were also of the view that Singapore should not adopt any of the limitations in Article 19(1) of the UN Convention as this might have an adverse effect on Singapore's competitive edge in the emerging e-commerce market.

2.10.3 In view of the submissions received, **we propose not to adopt any further exclusions from the applicability of the UN Convention or any of the limitations in Article 19(1) of the UN Convention**. We will nonetheless be making declarations, in accordance with Article 19(2) of the Convention, to cover those transactions listed in the existing section 4[44] (and hence excluded from application of Parts II and IV[45] the ETA), for which there are no corresponding exclusions within the UN Convention itself[46] (Please also see Part 3 below on the matters which will excluded from application of the ETA.)

2.10.4 Article 19(1) of the UN Convention allows States to declare that the UN Convention will apply only when the parties to the contract concerned

---

40 See Part 5.16 of LRRD No.1/2005.

41 Beyond the exclusions discussed in Part 5.16 of LRRD No.1/2005.

42 These exclusions would need to be declared under the present Article 19(2)of the UN Convention.

43 The UN Convention applies whenever the parties exchanging electronic communications have their places of business in different States, even if those States are not contracting States to the Convention (see Article 1(1) of the UN Convention), as long as the law of a contracting State is the applicable law. Article 19(1) of the UN Convention allows contracting States to declare that they will apply the UN Convention only (a) when both States where the parties have their places of business are contracting States to the Convention; or (b) only when the parties to a contract have agreed that the Convention applies to the electronic communications exchanged by them.

44 The transactions listed under the existing section 4 of the ETA will be moved to the First Schedule of the ETA. See also Part 3 below.

45 See footnote 6.

46 Declarations will be made in respect of:

- the creation or execution of a will;
- the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of implied, constructive and resulting trusts;
- any contract for the sale or other disposition of immovable property, or any interest in such property; and
- the conveyance of immovable property or the transfer of any interest in immovable property.

have their places of business in Contracting States[47] or only when the parties have agreed that the UN Convention applies. **We propose that Singapore should not limit the application of the UN Convention in this manner**.

2.10.5 Article 20 of the UN Convention will apply the UN Convention to the use of electronic communications in connection with the formation or performance of a contract to which any international convention, treaty or agreement, to which Singapore is or may become a Contracting State, applies. Of the international conventions listed in article 20(1), Singapore is currently party to the Convention on the Recognition and Enforcement of Foreign Arbitral Awards and the United Nations Convention on Contracts for the International Sale of Goods. Article 20 allows States various ways to declare that the UN Convention will not apply to the use of electronic communications in connection with the formation or performance of a contract to which such international conventions, treaties and agreements apply.

2.10.6 **We propose that Singapore should not make any declaration to exclude the UN Convention from applying to the use of electronic communications in connection with the formation or performance of a contract to which international conventions, treaties and agreements, of which Singapore is or may become a Contracting State, apply.** There appears to be no reason to exclude the UN Convention from so applying as:

a. the ETA (which will be further aligned with the UN Convention) already applies to such contracts, insofar as they are governed by Singapore law, to provide for the recognition of electronic communications in connection with such contracts;

b. matters in which the use of electronic communications may be a cause for concern are already excluded under section 4 of the ETA and will be declared to be excluded under Article 19(2) of the UN Convention (see paragraph 2.10.3 above); and

c. Article 20 of the UN Convention has a narrow effect – it merely achieves functional equivalence for electronic communications in connection with the formation or performance of a contract to which an international convention, treaty or agreement applies.

[47] i.e., States which are party to the UN Convention.

2.11 Extension to Non-Contractual Transactions

2.11.1 In LRRD No.1/2005[48], we sought comments on:

a. whether the existing sections 13, 14 and 15 of the ETA should be extended to apply to non-contractual transactions[49];

b. whether the existing sections 6, 7 and 8 of the ETA should continue to be of general application (including to non-contractual transactions)[50]; and

c. whether provisions in the UN Convention relating to electronic originals[51] and consent and variation[52] should also apply to non-contractual transactions[53].

2.11.2 Respondents on this issue supported the application of such provisions to non-contractual transactions. In view of this:

a. **we propose not to make any changes to sections 6 and 7 of the ETA** (i.e., they will continue to apply to electronic records generally; see sections 6 and 7 of the Proposed Bill);

b. **we propose that sections 8[54] and 15[55] of the ETA, which we propose to extensively modify for alignment with the UN Convention, will continue to apply to electronic documents or records generally** (see sections 8 and 13, respectively, of the Proposed Bill); and

c. **we propose that new sections 5(1) and 10 of the Proposed Bill (relating to consent and variation, and electronic originals, respectively) will also be of general application**.

2.11.3 In view of the fact that many of the provisions in existing Parts II and IV of the ETA apply generally to both contractual and non-contractual contexts, we have combined them under new Part II of the Proposed Bill which now encompasses provisions on "Electronic Records, Signatures and Contracts".

---

48 See Part 5.17 of LRRD No.1/2005.
49 See paragraphs 5.17.1 to 5.17.3 of LRRD No.1/2005.
50 See paragraph 5.17.4 (and footnote 342) of LRRD No.1/2005.
51 See Part 2.4 above.
52 See Part 2.2 above.
53 See paragraphs 5.17.4 to 5.17.7 of LRRD No.1/2005.
54 See Part 2.3 above.
55 See Part 2.5 above.

2.11.4 Concerning the existing sections 13 and 14 of the ETA, we propose to delete them (see paragraph 2.14.3 below on the deletion of section 13, and paragraph 2.5.5 above on the deletion of section 14).

2.12 Formation and Validity of Contracts

2.12.1 In LRRD No.1/2004[56], we raised the issue of whether there should be a provision on when an offer and acceptance in electronic form takes effect. Specifically, we sought views on whether the general rule (that a contract is concluded only on actual receipt of the offeree's acceptance) or the postal acceptance rule (that the contract is concluded at the point of posting) should apply to contracts concluded electronically.

2.12.2 Responses were divided on the issue. Those who were against the inclusion of such a provision believed it best for this issue to be addressed between the contracting parties themselves, and for disputes to be settled according to prevailing industry practices and normal contractual principles. They also cited the problem of a single rule applying even though some forms of electronic communications were instantaneous and others were not. Respondents who supported the inclusion of such a provision were mixed on which rule should apply, but all believed it best to have an "opt-out" approach where parties could decide to vary or render inapplicable a default rule.

2.12.3 Given the lack of consensus on what rules should apply and the difficulty of devising a single rule to apply to all the varied forms of electronic transactions, **we propose not to include any provision stipulating the substantive rules as to formation and validity of contracts**. Earlier drafts of the UN Convention had contained such provisions but they were subsequently deleted by UNCITRAL as they dealt with substantive contractual issues which the UN Convention should not affect[57].

2.12.4 Section 13 of the Proposed Bill will in any case clarify issues regarding the time of despatch and receipt of electronic communications.

---

[56] See Part 4.1 of LRRD No.1/2004.

[57] See also paragraph 4.1.2 of LRRD No.1/2004. The prevailing view of the UNCITRAL Working Group was that the UN Convention "*should not attempt to develop uniform rules for substantive contractual issues that were not specifically related to electronic commerce or to the use of electronic communications in the context of commercial transactions*": *Report of the Working Group IV (Electronic Commerce) on the work of its fortieth session (14-18 October 2002*) (A/CN.9/527), at paragraphs 80 and 81.

2.13 Effectiveness of Communications between Parties

2.13.1 We sought comments in LRRD No.1/2004[58] on whether references to "*declaration, demand, notice or request*" should be added to the existing section 12 of the ETA for consistency with Article 8(1) of the draft UN Convention, which referred to "*a declaration, demand, notice or request that parties are required to make or may wish to make in connection with a contract*".

2.13.2 As the final adopted text for Article 8(1) of the UN Convention omits such references to "*declaration, demand, notice or request*"[59], **we therefore propose not to add such references to the existing section 12 of the ETA** (see section 12 of the Proposed Bill). We nonetheless thank respondents for their comments on this issue.

2.14 Attribution

2.14.1 In LRRD No.1/2004[60], we sought comments on whether to retain the attribution provision in the existing section 13 of the ETA, and discussed whether it should apply to contracts concluded by automated message systems[61].

2.14.2 Respondents generally favoured the retention of section 13 of the ETA and its application to contracts concluded by automated message systems.

2.14.3 Upon consideration, **we nevertheless propose to omit the existing section 13 of the ETA from the Proposed Bill**. This approach is more consonant with the principles of functional equivalence and non-discrimination of electronic communications. There should not be specific rules on attribution of electronic communications as this would result in a duality of regimes compared with non-electronic communications. UNCITRAL had decided not to include any provision on attribution in the UN Convention because there was a lack of consensus internationally on the need for such provisions. Some jurisdictions have taken the position that no specific rules on attribution are necessary because the same legal rules concerning proof that are applicable to paper communications are equally applicable to electronic

[58] See Part 4.3 of LRRD No.1/2004.
[59] The final adopted text of Article 8(1) of the UN Convention reads as follows: "*A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.*"
[60] See Parts 4.4 and 6.4 of LRRD No.1/2004.
[61] See Part 2.7 above for our general discussion on automated message systems.

communications and this is a question of mixed law and fact to be decided by the courts. We also note that some of the rules under the existing section 13 of the ETA, which were devised with EDI [62] technology in mind, may be rather onerous when applied to an Internet context. It will be difficult to adapt the rules to apply to and to keep up with the fast-changing environment of electronic communications.[63]

2.15 Incorporation by Reference

2.15.1 In LRRD No.1/2004[64], we sought comments on whether to include a provision in the ETA stating that "incorporation by reference" applies to electronic transactions, and also whether specific rules should be adopted for incorporation in particular specified circumstances.

2.15.2 The majority of the respondents were of the view that such provision and rules should not be adopted, believing it best to leave common law rules to apply on "incorporation by reference".

2.15.3 In view of the submissions received, **we propose not to adopt any provision or rules on "incorporation by reference" in the Proposed Bill**.

2.16 Other Issues

2.16.1 We sought comments in LRRD No.1/2004[65] on whether any concepts of contract law (including privity of contract and consumer protection for dealing on standard contract terms of suppliers) should be clarified in relation to electronic transactions.

2.16.2 Most respondents offered no comments on this issue. One respondent, however, suggested clarifying that the Unfair Contract Terms Act (Cap. 396) and the Contracts (Rights of Third Parties) Act (Cap. 53B) apply to electronic contracts. Another respondent highlighted the need to strengthen the provisions of those two Acts to protect consumers with regard to electronic transactions and software contracts.

2.16.3 We believe it is sufficiently clear that the two Acts do not exclude electronic transactions or contracts from their application. **We therefore**

---

62 Electronic Data Interchange.

63 For further reading, see *United Nations Convention on the Use of Electronic Communications in International Contracts – A New Global Standard* (2006) 18 SAcLJ 116, paragraphs 59 to 63, available at http://www.sal.org.sg/digitallibrary/Lists/SAL%20Journal/DispForm.aspx?ID=390.

64 See Part 7.1 of LRRD No.1/2004.

65 See Part 7.3 of LRRD No.1/2004.

do not propose to adopt any amendment to the ETA in this respect. The provisions of the ETA would in general apply to the interpretation of the written laws of Singapore, including those two Acts, unless the context indicates otherwise. Concerning the suggestion to strengthen the provisions of the two Acts, this would change the law as it generally applies to all contractual documents, and we believe that this issue would be more appropriately considered if and when those Acts are reviewed.

2.16.4 On a related note, we have not included Articles 7 and 13 of the UN Convention in the Proposed Bill as these saving provisions are intended to clarify that the UN Convention does not affect substantive requirements as to form in domestic regulatory regimes (e.g., consumer protection laws). It is unnecessary to include such provisions since it is clear that the provisions providing for legal recognition of electronic transactions in the Proposed Bill (and the current ETA) do not override any provisions of law that require certain records or communications to be in a specific non-electronic form[66].

[66] See examples in footnote 9. Note discussion in paragraphs 144 to 148 of the Article on *United Nations Convention on the Use of Electronic Communications in International Contracts – A New Global Standard* (2006) 18 SAcLJ 116 by Chong Kah Wei and Joyce Chao Suling.

PART 3
TRANSACTIONS EXCLUDED FROM APPLICATION OF THE ETA

3.1 Introduction to Part

3.1.1 In LRRD No.2/2004[67], we sought comments on the transactions excluded from application of the existing Parts II and IV[68] of the ETA[69] ("**Excluded Transactions List**"), due to their being listed in the existing section 4 of the ETA.

3.1.2 Seven submissions were received in response to LRRD No.2/2004[70]. In this Part, we will discuss the submissions on the key issues raised during the consultation, and the corresponding Proposed Amendments to the ETA, in the following order:

- Part 3.2: Wills
- Part 3.3: Negotiable Instruments and Documents of Title
- Part 3.4: Indentures
- Part 3.5: Trusts
- Part 3.6: Transfers of Immovable Property
- Part 3.7: Powers of Attorney
- Part 3.8: Other Issues

3.1.3 We wish to highlight that the Excluded Transactions List has been moved to the First Schedule of the Proposed Bill. This is an editorial change to streamline the ETA, by placing the key provisions which may be amended by subsidiary legislation in the Schedules.

3.2 Wills

3.2.1 We proposed in LRRD No.2/2004[71] to maintain the creation and execution of wills in the Excluded Transactions List.

3.2.2 With the exception of one respondent, all respondents supported our proposal. Respondents were also generally of the view that there should not be any exceptional cases where the use of electronic wills should be

[67] Consultation paper for Stage II of the *Joint IDA-AGC Public Consultation on Review of the Electronic Transactions Act: Exclusions under Section 4 of the ETA.*

[68] We have consolidated the existing Parts II and IV of the ETA into a single Part II in the Proposed Bill.

[69] Parts II and IV of the ETA contain provisions clarifying that electronic records are the functional equivalent of paper records.

[70] Soft copies of the submissions are available on the IDA website (www.ida.gov.sg, under "Policies and Regulation → IDA Consultation Papers & Decisions").

[71] See Part 3 of LRRD No.2/2004.

allowed. The main reason cited for their views was that this would erode the safeguards provided by the strict formalities required for the creation and execution of wills. One respondent added that the power of the courts to dispense with compliance with the formalities for creating wills should be considered in the context of an amendment to the Wills Act (Cap. 352) rather than as an exclusion to the ETA. Concerns were also raised on the reliability and authenticity of electronic wills, and the lack of international recognition for electronic wills. The dissenting respondent advocated that all transactions in the Excluded Transactions List be removed in view of advances in technology.

3.2.3 After considering the submissions received, **we maintain our proposal to retain the creation and execution of wills in the Excluded Transactions List**. (See item 1 of the First Schedule of the Proposed Bill.) We reiterate our views in LRRD No.2/2004[72] concerning the significant disadvantages to the use of electronic wills. We also maintain that the formalities required for the creation and execution of wills to the electronic medium are not easily translated into the electronic medium, notwithstanding advances in technology.

3.3 Negotiable Instruments and Documents of Title

3.3.1 We proposed in LRRD No.2/2004[73] to maintain negotiable instruments and documents of title in the Excluded Transactions List.

3.3.2 The submissions received, and our views on the matter, were discussed in Part 5 of LRRD No.1/2005[74] in the context of electronic originals[75]. To avoid doubt, we maintain our position that **negotiable instruments and documents of title should continue to remain in the Excluded Transactions List**. Specific legislation may be made to allow for the recognition of electronic versions of such instruments when appropriate.

3.3.3 **We propose, however, to align the provisions on negotiable instruments and documents of title in the Excluded Transactions List with the corresponding Article 2(2) of the UN Convention**. To that end, **we propose to include *"bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of***

[72] See Part 3 of LRRD No.2/2004.
[73] See Parts 4 and 9 of LRRD No.2/2004.
[74] Consultation paper for Stage III of the *Joint IDA-AGC Public Consultation on Review of the Electronic Transactions Act: Remaining Issues*.
[75] See Part 5.11 of LRRD No.1/2005.

***money*" in the Excluded Transactions List**. (See item 2 of the First Schedule of the Proposed Bill.)

3.4 Indentures

3.4.1 In LRRD No.2/2004[76], we explored whether to maintain indentures[77] in the Excluded Transactions List, and whether provisions should be included to provide for electronic equivalents for sealing and attestation of documents.

3.4.2 One respondent supported the continued exclusion of indentures. The same respondent also believed that there was little merit in providing for electronic equivalents for sealing and attestation if indentures were to continue to be excluded. Four other respondents suggested that indentures could be removed from the Excluded Transactions List but emphasised that indentures relating to land should remain within the list. As to requirements for sealing and attestation, these four respondents were divided on whether and how to provide for electronic equivalents, and the safeguards that would be required.

3.4.3 After considering the submissions received, **we propose to retain the creation, performance and enforcement of indentures in the Excluded Transactions List**. (See item 3 of the First Schedule of the Proposed Bill.) We propose that indentures should remain on the Excluded Transactions List since most indentures relate to the transfer or conveyance of immovable property and the proposal currently is to retain such transactions on the Excluded Transactions List[78]. Further, as there is no consensus on whether and how to allow for electronic sealing, we propose not to make any amendments to the ETA to provide for electronic sealing at present. These proposals may be reviewed if proposals to abolish the requirement for deeds to be made on parchment and to be sealed are enacted[79]. For attestations, we also propose not to make any specific amendment to the ETA to cater for electronic equivalents. We would nonetheless highlight that if attestation is required for documents which are not on the Excluded Transactions List, section 8 of the Proposed Bill[80] would allow for the affixation of the witness's signature by electronic means.

---

[76] See Part 5 of LRRD No.2/2004.

[77] An indenture is a deed entered into between 2 or more persons.

[78] See Part 3.6 below.

[79] Proposed Instruments (Formalities) Bill (LRRD No.1/2001).

[80] Section 8 of the Proposed Bill provides that "*[w]here a rule of law requires a signature, or provides for certain consequences if a document or record is not signed, that requirement is met in relation to an electronic record if – (a) a method is used to identify the person and to indicate that*

3.5 Trusts

3.5.1 In LRRD No.2/2004[81], we suggested that the exclusion relating to trusts could be narrowed to only testamentary trusts and trusts relating to land.

3.5.2 Of the five respondents to this issue, one objected to narrowing the exclusion because of the inability to verify the electronic declaration of trusts. Another respondent suggested that express private trusts should also be excluded, and yet another opined that digital signatures should be used to safeguard the identity of the creator. On the question of whether the ETA should apply to implied trusts (in addition to constructive and resulting trusts), four respondents responded in the affirmative.

3.5.3 After considering the submissions received, **we propose to amend the Excluded Transactions List to carve out implied trusts**. **Other than this amendment, we propose to retain the present language in the Excluded Transactions List relating to the exclusion of trusts**. (See item 3 of the First Schedule of the Proposed Bill.)

3.6 Transfers of Immovable Property

3.6.1 We sought comments in LRRD No.2/2004[82] on whether the exclusions in the existing sections 4(1)(*d*) and (*e*) of the ETA pertaining to transfers of immovable property could be narrowed by excluding classes of persons and/or land transactions from their operation.

3.6.2 With the exception of the respondent advocating the removal of all transactions from the Excluded Transactions List, all respondents did not support narrowing the exclusions as transfers of immovable property are typically high value transactions, and the physical execution of land transfer/lease documents would provide the safeguards necessary for "unsophisticated" homeowners or tenants.

3.6.3 After considering the submissions, **we propose to retain, in the Excluded Transactions List, the existing exclusions relating to the conveyance or transfer of immovable property which are currently in sections 4(1)(*d*) and (*e*) of the ETA**. (See items 4 and 5 of the First Schedule of the Proposed Bill.)

---

person's intention in respect of the information contained in the electronic record…" (emphasis added). See also paragraph 2.3 of Part 2 above.

[81] See Part 6 of LRRD No.2/2004.

[82] See Part 8 of LRRD No.2/2004.

3.6.4 We are aware that, notwithstanding the exclusion of transfers of immovable property under the ETA, the use of electronic communications has been recognised to satisfy requirements for writing and signature in relation to agreements for the transfer of immovable property in various local cases[83]. It remains to be seen whether any additional safeguards will need to be put in place to protect "unsophisticated" homeowners or tenants.

3.7 Powers of Attorney

3.7.1 We also sought comments in LRRD No.2/2004[84] on whether powers of attorney should be removed from the Excluded Transaction List.

3.7.2 Again, with the exception of the respondent advocating the removal of all transactions from the Excluded Transactions List, all respondents were of the view that powers of attorney should remain in the list. This was in line with their comments on transfers of immovable property and in view of the fact that powers of attorney are typically associated with such transfers.

3.7.3 After considering the submissions received, **we propose to retain the creation, performance and enforcement of powers of attorney in the Excluded Transactions List**. (See item 3 of the First Schedule of the Proposed Bill.)

3.8 Other Issues

3.8.1 In LRRD No.2/2004[85], we sought comments on whether there should be any further additions to the current Excluded Transactions List and whether any specific class of parties or transactions should be excluded from the operation of section 4 of the ETA (and the Excluded Transactions List).

3.8.2 Almost all respondents were of the view that there should not be further additions to the current Excluded Transactions List. Nonetheless, **for alignment with Article 2(1)(b) of the UN Convention, we propose to add the following matters to the Excluded Transactions List:**

- **"*transactions on a regulated exchange*";**
- **"*foreign exchange transactions*";**

[83] *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd* [2005] 2 SLR 651, followed in Singh Chiranjeev and Another v Joseph Mathew and Others [2009] 2 SLR 73.
[84] See Part 7 of LRRD No.2/2004.
[85] See Part 10 of LRRD No.2/2004

- ***"inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments"*; and**
- ***"the transfer of security rights in sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments held with an intermediary"***.

(See items 6, 7, 8 and 9 of the First Schedule of the Proposed Bill.)

3.8.3 UNCITRAL excluded these transactions because "*the financial service sector is already subject to well-defined regulatory controls and industry standards that address issues relating to electronic commerce in an effective way for worldwide functioning of that sector*" [86]. Domestically, it is expected that the use of electronic communications in such highly specialised and complicated transactions will be governed by specific legislation, where appropriate, or by agreement between the parties.

3.8.4 **We propose, however, that the exclusion in Article 2(1)(a) of the UN Convention relating to "*[c]ontracts concluded for personal, family or household purposes*" should not be adopted.** Such contracts were excluded from the UN Convention due to the nature of the Convention as an instrument for the harmonisation of international trade law, and due to the Working Group's recognition that consumer protection rules were domestic in nature and varied greatly from jurisdiction to jurisdiction. It is expected that specific legislation will provide the necessary safeguards in these areas where necessary[87].

3.8.5 Almost all respondents believed that no specific class of parties or transactions should be excluded from the operation of section 4 of the ETA (and the Excluded Transactions List).

3.8.6 In conclusion, as discussed above in this Part, **we propose to adopt only the exclusions set out in the Excluded Transactions List in the First Schedule to the Proposed Bill**.

---

[86] See paragraph 7 of Explanatory Notes on the United Nations Convention on the Use of Electronic Communications in International Contracts (ISBN: 978-92-1-133756-3), available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.

[87] Paragraph 29 of *Report of the United Nations Commission on International Trade Law on the work of its thirty-eighth session (4-15 July 2005)*(A/60/17), suggested that exclusion extended to contracts governed by family law and the law of succession, such as matrimonial property contracts, though the correctness of this view has been questioned. In any case, the interests of parties to such agreements would be protected as the application of such agreements would come under the purview of courts.

PART 4
REGULATION OF CERTIFICATION AUTHORITIES

4.1 Introduction to Part

4.1.1 In Part 2 of LRRD No.1/2005[88], we sought comments on amendments to the ETA and the ETR to facilitate further development of the certification authority ("**CA**"), authentication and security solutions market.

4.1.2 Six submissions were received in response to Part 2 of LRRD No.1/2005[89]. All the respondents generally agreed with the proposed changes to the CA regulatory framework, although some suggested some further modifications for our consideration.

4.1.3 In this Part, we will discuss the submissions on the key issues raised during the consultation, and the corresponding Proposed Amendments to the ETA, in the following order:

Part 4.2: Technology Neutral Approach
Part 4.3: Voluntary Licensing / Accreditation
Part 4.4: Financial Criteria and Fees
Part 4.5: Term of Accreditation
Part 4.6: Operational Criteria & Auditing Requirements

4.2 Technology Neutral Approach

4.2.1 In LRRD No.1/2005[90], we proposed to remove technology specific details from the ETA and to leave such details to regulations to be made under the ETA. This was to ensure that the same benefits as those currently accorded to public key infrastructure technology ("**PKI**") could be quickly and conveniently accorded to new authentication technologies (such as biometrics) through the enactment of new regulations under the ETA.

4.2.2 All respondents agreed with our proposal. **We therefore propose to remove the PKI-specific provisions from the ETA (i.e., Parts VI, VII, VIII and IX of the ETA)**. However, instead of enacting separate regulations, we propose that these provisions be placed in a Schedule of the ETA for greater ease of reference. The provisions in the Schedules

[88] Consultation paper for Stage III of the *Joint IDA-AGC Public Consultation on Review of the Electronic Transactions Act: Remaining Issues*.

[89] Soft copies of the submissions are available on the IDA website (www.ida.gov.sg, under "Policies and Regulation → IDA Consultation Papers & Decisions").

[90] See Part 2.6 of LRRD No.1/2005.

can be amended by subsidiary legislation[91] to specify new authentication technologies as specified security procedures. (See sections 21 to 23 and the Second Schedule of the Proposed Bill.)

4.3 Voluntary Licensing / Accreditation

4.3.1 We also proposed, in LRRD No.1/2005[92], to replace the current "licensing" regime of CAs with an "accreditation" framework to better represent the voluntary nature of the CA framework.

4.3.2 All respondents agreed with our proposal. One respondent commented that high standards needed to be maintained for accreditation. Another suggested that clarification should be provided on whether an organisation that issues certificates to its own customers for the purpose of identification and performance of electronic transactions without involving any third party would come under the purview of the ETA and whether the organisation would have to apply for accreditation.

4.3.3 In view of the submissions received, **we maintain our proposal to replace the current "licensing" regime with an "accreditation" framework**. The same benefits currently enjoyed by licensed CAs will nonetheless continue to be afforded to accredited CAs.

4.3.4 Concerning the standards for accreditation, the provisions in the existing Part VIII of ETA outline the duties of all CAs, whether or not they are licensed or accredited. In other words, any organisation that issues certificates in Singapore must comply with these provisions. **We propose to retain these provisions in the ETA as they constitute "hygiene" requirements for all CAs to observe**. (See the Third Schedule of the Proposed Bill). There is, however, no need for all organisations that issue certificates to apply for accreditation as it is a voluntary scheme.

4.4 Financial Criteria and Fees

4.4.1 We proposed in LRRD No.1/2005[93] to:

a. remove the $1 million banker's guarantee, insurance and paid-up capital requirements for CAs ("**Financial Criteria**"); and

[91] i.e., by publishing an order made by the Minister in the *Gazette*.
[92] See Part 2.7 of LRRD No.1/2005.
[93] See Part 2.8 of LRRD No.1/2005.

b. reduce the total fees payable by a CA to $2,000 for the first application and initial two-year period of accreditation; and to $1,000 for every subsequent two years of renewal of accreditation.

4.4.2 Four respondents welcomed and agreed with our proposed reduction of CA fees, but only three of those respondents commented on the removal of the Financial Criteria. One respondent suggested that the requirement for the banker's guarantee should not be totally removed but should instead be reduced (e.g., from $1 million to $500,000) as it would provide some form of security/guarantee to users of CAs. The respondent also suggested that the minimum requirement for paid-up capital should not be totally removed but should instead be reduced to help ensure that CAs have sufficient funds to continue their operations. The same respondent added that it had no issues with the removal of the insurance requirements. However, another respondent suggested that some baseline financial (e.g., indemnity insurance) and operational requirements should be imposed for the initial accreditation of the CA. The third respondent opined that any reduction of Financial Criteria and fees should be assessed against the CA's financial health and status.

4.4.3 The rest of the respondents did not express any views on the matter.

4.4.4 After considering the comments received**, we maintain our proposal to remove the Financial Criteria and reduce the fees payable by CAs in respect of accreditation**. Concerning the removal of the Financial Criteria, we reiterate our views in LRRD No.1/2005[94]. We believe that consumer liability in any business decision between a private company and the public would be best dealt with commercially and not through regulation.

4.5 Term of Accreditation

4.5.1 We proposed in LRRD No.1/2005[95] to increase the term of accreditation of CAs (and renewal thereof) from one year to two years. The key reason for this was to lower the cost of the security audit for the CAs, which has to be conducted prior to each renewal.

4.5.2 There were three respondents on this issue. While all three respondents agreed that a longer accreditation period was good, two of them suggested that the accreditation period could be even longer (e.g., three

[94] See Part 2.8 of LRRD No.1/2005.
[95] See Part 2.9 of LRRD No.1/2005.

years). The third respondent suggested that the Controller should have the discretion to accredit for shorter periods on a case-by-case basis.

4.5.3 After considering the submissions received, **we maintain our proposal to increase the term of accreditation (and renewal thereof) to two years**. We believe that a one-year accreditation period may be onerous for CAs in view of the security audit requirements, and that a two-year accreditation period would be optimal.

4.6 Operational Criteria & Auditing Requirements

4.6.1 In LRRD No.1/2005[96], we proposed to remove the requirement for a comprehensive audit on the CA's compliance with the ETA and ETR and licence conditions, and to limit the audit requirements to only the relevant security guidelines.

4.6.2 There were five respondents on this issue. Two respondents agreed with our proposal, and three expressed reservations. The three were of the view that the audit served to attest to the integrity of a CA, and should therefore cover more areas than just the security guidelines. One of the three suggested that the audit should cover all processes and requirements in the ETA and ETR, otherwise customers would have to conduct their own investigations on whether the CA truly met those requirements.

4.6.3 After considering the submissions received, **we propose to retain the present scope of the audit but to streamline and merge the audit requirements, currently found in the existing regulation 10(1)(*a*) to (*d*) of the ETR, into a single Compliance Audit Checklist, as set out at Annex C**. This checklist would provide a single reference document for CAs and their auditors to carry out the audit but would still adequately cover the checks required for consumer protection and confidence in the integrity of the CAs.

[96] See Part 2.10 of LRRD No.1/2005.

PART 5
E-GOVERNMENT

5.1 Introduction to Part

5.1.1 In Part 4 of LRRD No.1/2005[97], we sought comments on amendments to the ETA to facilitate further developments in e-Government. Specifically, we proposed to amend the existing sections 9 and 47 of the ETA to provide, in the context of electronic transactions with Government agencies, for:

a. deviations from statutorily prescribed forms;
b. non-documentary information to be submitted to Government agencies through electronic means;
c. flexibility in using electronic systems administered by intermediaries;
d. default acceptance by Government agencies of electronic retention of documents; and
e. the acceptance by Government agencies of electronic originals.

5.1.2 Six submissions were received in response to Part 4 of LRRD No.1/2005[98]. All the respondents generally agreed with the proposed amendments, with some making further suggestions for incorporation into the ETA.

5.1.3 In this Part, we will discuss the submissions on the key issues raised during the consultation, and our decisions on the amendments to be adopted, in the following order:

Part 5.2: Amendments to Section 47 of the ETA
Part 5.3: Amendments to Section 9 of the ETA

5.2 Amendments to Section 47 of the ETA

5.2.1 We proposed in Part 4 (and Annex B) of LRRD No.1/2005 that the existing section 47 of the ETA be amended to provide that a legal requirement for any document, record or information to be provided or submitted to, or created or retained for, any Government agency, would be satisfied by providing, submitting, creating or retaining (as the case may be) such electronic record, and in such manner, as may be specified by the relevant Government agency[99]. This would be notwithstanding

[97] Consultation paper for Stage III of the *Joint IDA-AGC Public Consultation on Review of the Electronic Transactions Act: Remaining Issues*.

[98] Soft copies of the submissions are available on the IDA website (www.ida.gov.sg, under "Policies and Regulation → IDA Consultation Papers & Decisions").

[99] See Parts 4.7 and 4.10, and Annex B, of LRRD No.1/2005.

that the electronic system specified by the Government agency for such purposes might be administered by a third-party intermediary[100], or that the electronic record might not resemble the actual form prescribed by legislation[101].

5.2.2 We also proposed to amend the existing section 47 of the ETA to clarify that non-documentary information submitted to a Government agency would satisfy any legal requirement for such information to be submitted to that agency[102], and also to allow for Government agencies to accept electronic originals[103]. (In connection with the latter, please also refer to Part 2.4 above where we discussed the inclusion of a new provision governing the reliability and accessibility conditions to be met for submission of electronic originals.)

5.2.3 Respondents generally agreed with our proposed amendments to the existing section 47 of the ETA. Some concerns were raised, such as the need for adequate administrative and workflow procedures for dealing with electronic forms, and to ensure that the use of intermediaries did not absolve the Government of its legal obligations towards citizens (e.g., for breach of security leading to disclosure of sensitive information).

5.2.4 We would highlight that our proposed provision operates only to clarify that the requirement for a person to file, create, retain, use, provide or hold information or certain documents in a particular form is satisfied by doing so in an electronic form specified by the public agency concerned. It does not affect any obligations of secrecy or confidentiality of the Government to the public. With respect to the administrative and workflow procedures for dealing with electronic forms, we are of the view that it would be desirable to maintain flexibility on this and allow Government agencies to decide on the procedures most appropriate and relevant to them.

5.2.5 Having considered the submissions received, **we maintain our proposed amendments and propose to amend section 47 of the ETA accordingly**. (See section 37 of the Proposed Bill.)

[100] See Part 4.9 and Annex B of LRRD No.1/2005.
[101] See Part 4.7 and Annex B of LRRD No.1/2005.
[102] See Part 4.8 and Annex B of LRRD No.1/2005.
[103] See Part 4.11 and Annex B of LRRD No.1/2005.

5.3 Amendments to Section 9 of the ETA

5.3.1 The existing Section 9 of the ETA currently provides that where there are legal requirements for retention of certain documents, those requirements can be met by retaining the documents in electronic form subject to, among other conditions, consent from the relevant Government agency being obtained.

5.3.2 In Part 4 of LRRD No.1/2005, we proposed to amend the existing section 9 of the ETA to remove this consent requirement[104]. The intention behind this was to provide for the default acceptance by Government agencies of electronic retention of documents. Government agencies would nonetheless be allowed to "opt-out" of the default position[105]. We also proposed to retain the current provision in the existing section 9 of the ETA allowing for additional requirements relating to the retention of electronic records to be specified by the relevant Government agencies.

5.3.3 Respondents again generally agreed with our proposed amendments to the existing section 9 of the ETA. However, they also asked for proper publicity of "opt-out" decisions and any additional requirements specified by Government agencies. There was a suggestion that these decisions and requirements could be published on the respective Government agencies' websites.

5.3.4 The proposed provision already requires the opt-out to be made by subsidiary legislation, namely, as an order by the Minister, published in the Government *Gazette*. As stated in LRRD No.1/2005[106], we agree that Government agencies should give adequate publicity of their "opt-out" decisions and additional specified requirements. Nonetheless, it would be preferable to retain administrative flexibility on how they may go about doing so. For example, they could choose to publicise such decisions on their website or through even more proactive communication efforts. **We therefore propose not to adopt any provision requiring website publication of "opt-out" decisions or additional specified requirements**.

5.3.5 Hence, after considering the comments received, **we maintain our proposed amendments and propose to amend the existing section 9 of the ETA accordingly**. (See section 9 of the Proposed Bill.)

[104] See Part 4.10 and Annex B of LRRD No.1/2005.
[105] By publication of an order by the Minister in the Government *Gazette* specifying the documents, records and/or information to which the revised section 9 will not apply.
[106] See paragraph 4.10.8 of LRRD No.1/2005.

ANNEX A

PROPOSED ELECTRONIC TRANSACTIONS BILL 2009

The proposed Electronic Transactions Bill 2009 seeks to repeal and re-enact the existing Electronic Transactions Act (Cap.88) as substantial portions of the existing Act have been re-arranged and re-numbered. Changes to the existing text of the Electronic Transactions Act are indicated in italics and the source references are indicated in square brackets after the relevant provisions of the Bill.

Key to abbreviation of source references:

ETA	Electronic Transactions Act (Cap.88)
UN	United Nations Convention on the Use of Electronic Communications in International Contracts
UNCITRAL	UNCITRAL Model Law on Electronic Commerce
US	US Electronic Signatures in Global and National Commerce Act

Electronic Transactions Bill

Bill No. /2009.

Read the first time on 2009.

ELECTRONIC TRANSACTIONS ACT 2009

(No. of 2009)

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

PART II

ELECTRONIC RECORDS, SIGNATURES *AND CONTRACTS*

PART III

SECURE ELECTRONIC RECORDS AND SIGNATURES

PART IV

REGULATION OF *SPECIFIED SECURITY PROCEDURES AND* CERTIFICATION AUTHORITIES

PART V

ENFORCEMENT OF PART IV

PART VI

USE OF ELECTRONIC RECORDS AND SIGNATURES *BY PUBLIC AGENCY*

PART VII

GENERAL

A BILL

i n t i t u l e d

An Act to make provisions for the security and use of electronic transactions and for matters connected therewith.

Be it enacted by the President with the advice and consent of the Parliament of Singapore, as follows:

PART I

PRELIMINARY

Short title and commencement

1. This Act may be cited as the Electronic Transactions Act 2009 and shall come into operation on such date as the Minister may, by notification in the *Gazette*, appoint.

Interpretation

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

"*addressee*", *in relation to an electronic communication, means a party who is intended by the originator to receive the electronic communication, but does not include a party acting as an intermediary with respect to that electronic communication;*

[UN Art 4(e)]

"*automated message system*" *means a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person each time an action is initiated or a response is generated by the system;*

[UN Art 4(g)]

"*communication*" *includes any statement, declaration, demand, notice, request, offer or the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract;*

[UN Art 4(a)]

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

[US sec. 106(2)]

"*electronic communication*" *means any communication that the parties make by means of electronic records;*

[UN Art 4(b)]

"electronic record" means a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another[1];

[ETA s.2]

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

[ETA s.2]

"information system" means a system for generating, sending, receiving, storing or otherwise processing electronic records;

[UN Art 4(f)]

"originator", in relation to an electronic communication, means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but it does not include a party acting as an intermediary with respect to that electronic communication;

[UN Art 4(d)]

"public agency" means a department or ministry of the Government, an organ of state or a statutory body;

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

[ETA s.2]

"rule of law" includes written law;

[ETA s.2]

"secure electronic record" means an electronic record *that is* treated, *by virtue of section 17(1) or any other provision of this Act,* as a secure electronic record *for the purposes of section 19;*

[ETA s.18(4)]

"secure electronic signature" means an electronic signature *that is* treated, *by virtue of section 18 or any other provision of this Act,* as a secure electronic signature *for the purposes of section 19;*

[ETA s.18(4)]

---

[1] The existing definition of "electronic record" reads as follows and the underlined words will be deleted in the proposed new definition:

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

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

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

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

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

[ETA s.2]

"signed" or "signature" and its grammatical variations *means a method used to identify a person and to indicate the intention of that person in respect of the information contained in a record and includes an electronic method;*

[ETA definition modified by UN Art 9(3)(a)]

"specified security procedure" means a security procedure which is specified in the Second Schedule.

(2) In this Act, "place of business", in relation to a party, means —

(a) any place where the party maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location; or

(b) if the party is a natural person and he does not have a place of business, the person's habitual residence.

[UN Art 4(h) and 6(3)]

(3) For the purposes of subsection (2) —

(a) if a party has indicated his place of business, the location indicated by him is presumed to be his place of business unless another party proves that the party making the indication does not have a place of business at that location;

[UN Art 6(1)]

(b) if a party has not indicated a place of business and has more than one place of business, then the place of business is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by

the parties at any time before or at the conclusion of the contract;

[UN Art 6(2)]

(c) a location is not a place of business merely because that location is —

(i) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or

(ii) where the information system may be accessed by other parties;

[UN Art 6(4)]

(d) the sole fact that a party makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

[UN Art 6(5)]

(4) Where an electronic communication does not relate to any contract, references to a contract in subsection (3) shall refer to the relevant transaction.

Purposes and construction

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

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

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

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

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

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

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

[ETA s.3]

(g) to implement the United Nations Convention on the Use of Electronic Communications in International Contracts adopted by the General Assembly of the United Nations on 23 November 2005 and to make the law of Singapore on electronic transactions, whether or not involving parties whose places of business are in different states, consistent with the provisions of that Convention.

Excluded matters

4.—(1) *The provisions of this Act specified in the first column of the First Schedule shall not apply to any rule of law requiring writing or signatures in any of the matters specified in the second column of that Schedule.*

[ETA s.4]

(2) The Minister may, by order in the Gazette, amend the First Schedule.

Party autonomy

5.—(1) Nothing in Part II affects any rule of law or obligation requiring the agreement or consent of the parties as to the form of a communication or record, and (unless otherwise agreed or provided by a rule of law) such agreement or consent may be inferred from the conduct of the parties.

[UN Art 8(2)]

(2) Nothing in Part II shall prevent the parties to a contract or transaction from —

(a) excluding the use of electronic records, communications or signatures in the contract or transaction by agreement; or

(b) imposing additional requirements as to the form or authentication of the contract or transaction by agreement.

(3) Subject to any other rights or obligations of the parties to a contract or transaction, the parties may, by agreement –

(a) exclude section 6, 11, 12, 13, 14, 15 or 16 from applying to the contract or transaction; or

(b) derogate from or vary the effect of all or any of those provisions in respect of the contract or transaction.

[ETA s.5; UN Art 3]

PART II

ELECTRONIC RECORDS, SIGNATURES *AND CONTRACTS*

Legal recognition of electronic records

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

[ETA s.6; UNCITRAL Art 5; UN Art 8]

Requirement for writing

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

[ETA s.7; UNCITRAL Art 6; UN Art 9(2)]

Requirement for signature

8. *Where a rule of law requires a signature, or provides for certain consequences if a document or record is not signed, that requirement is met in relation to an electronic record if —*

(a) a method is used to identify the person and to indicate that person's intention in respect of the information contained in the electronic record; and

(b) the method used is either —

(i) as reliable as appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

(ii) proven in fact to have fulfilled the functions described in paragraph (a), by itself or together with further evidence.

[ETA s.8; UNCITRAL Art 7; Replaced by UN Art 9(3)]

Retention of electronic records

9.—(1) Where a rule of law requires that certain documents, records or information be retained, *or provides for certain consequences if they are not,* that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied:

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

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

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

(d) any additional requirements relating to the retention of such electronic records specified by the public agency which has supervision over the requirement for retention of such records are complied with.

[Provides for ETA s.9(4)(b)]

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

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

(4) Nothing in this section shall *apply to* —

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

(b) any rule of law requiring that any documents, records or information be retained if the Minister has, by order in the Gazette, specified that this section shall not apply to that requirement in respect of those documents, records or information.

[ETA s.9; UNCITRAL Art 10]

Provision of originals

10.—*(1) Where a rule of law requires any document, record or information to be provided or retained in its original form, or provides for certain consequences if it is not, that requirement is satisfied by providing or retaining the document, record or information in the form of an electronic record if the following conditions are satisfied:*

(a) there exists a reliable assurance as to the integrity of the information contained in the electronic record from the time the document, record or information was first made in its final form, whether as a document in writing or as an electronic record;

(b) where the document, record or information is to be provided to a person in its original form, the electronic record that is provided to the person is capable of being displayed to the person; and

(c) any additional requirements relating to the provision or retention of such electronic records specified by the public agency which has supervision over the requirement for the provision or retention of such records are complied with.

(2) For the purposes of subsection (1)(a) —

(a) the criterion for assessing integrity shall be whether the information has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the circumstances.

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

(4) Nothing in this section shall apply to any rule of law requiring that any document, record or information be provided or retained in its original form if the Minister has, by order in the Gazette, specified that this section shall not apply to that requirement in respect of such document, record or information.

[UN Art 9(4) and (5); UNCITRAL Art 8]

Formation and validity of contracts

11.—(1) For the avoidance of doubt, it is declared that in the context of the formation of contracts,[2] an offer and the acceptance of an offer may be expressed by means of electronic *communications*.

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

[ETA s. 11; UNCITRAL Art 11(1); UN Art 8(1)]

Effectiveness between parties

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

[ETA s. 12; UNCITRAL Art 12(1)]

Time and place of despatch and receipt

13.—*(1) The time of despatch of an electronic communication is the time when it leaves an information system under the control of the*

---

[2] The existing section 11(1) reads as follows and the underlined words will be deleted in the proposed new section 11(1):

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

originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.

[UN Art 10(1)]

(2) The time of receipt of an electronic communication is the time when the electronic communication becomes capable of being retrieved by the addressee at an electronic address designated by the addressee.

[UN Art 10(2)]

(3) The time of receipt of an electronic communication at an electronic address that has not been designated by the addressee is the time when the electronic communication becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address.

[UN Art 10(2)]

(4) For the purposes of subsection (3), an electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the electronic address of the addressee.

[UN Art 10(2)]

(5) An electronic communication is deemed to be despatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business.

[UN Art 10(3)]

(6) Subsections (2) to (4) shall apply notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under subsection (5).

[ETA s.15 replaced by UN Art 10(4)]

Invitation to make offer

***14**. A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including proposals that make use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.*

[UN Art 11]

Use of automated message systems for contract formation

15. *A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.*

[UN Art 12]

Error in electronic communications

16.*—(1) Where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made.*

[UN Art 14(1)]

(2) Subsection (1) shall not apply unless the person, or the party on whose behalf that person was acting —

(a) notifies the other party of the error as soon as possible after having learned of the error and indicates that he made an error in the electronic communication; and

(b) has not used or received any material benefit or value from the goods or services, if any, received from the other party.

[UN Art 14(1)]

(3) Nothing in this section affects the application of any rule of law that may govern the consequences of any error other than as provided for in subsections (1) and (2).

[UN Art 14(2)]

PART III

SECURE ELECTRONIC RECORDS AND SIGNATURES

Secure electronic record

17.—(1) If a *specified* security procedure or a commercially reasonable security procedure agreed to by the parties involved has been properly applied to an electronic record to verify that the electronic record has not

been altered since a specific point in time, such record shall be treated as a secure electronic record *for the purposes of section 19* from such specific point in time to the time of verification.

(2) For the purposes of this section and *section 18*, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including —

(*a*) the nature of the transaction;

(*b*) the sophistication of the parties;

(*c*) the volume of similar transactions engaged in by either or all parties;

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

(*e*) the cost of alternative procedures; and

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

[ETA s. 16]

Secure electronic signature

18. If, through the application of a *specified* security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made —

(*a*) unique to the person using it;

(*b*) capable of identifying such person;

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

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

such signature shall be treated as a secure electronic signature *for the purposes of section 19.*

[ETA s. 17]

Presumptions relating to secure electronic records and signatures

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

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

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

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

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

[ETA s. 18; Definition in s.18(4) moved to s.2]

PART IV

REGULATION OF *SPECIFIED SECURITY PROCEDURES AND* CERTIFICATION AUTHORITIES

Interpretation of this Part and Part V

20.*—(1) In this Part and Part V, unless the context otherwise requires —*

"accredited person" means a person involved in the provision of a specified security procedure who is accredited under the provisions made under section 23;

"authorised officer", *in relation to the exercise of any power under the relevant Parts*, means a person authorised by the Controller *to exercise of that power* under *section 27*;

[ETA s.2]

"certificate" *has the same meaning as in the Third Schedule;*

[ETA s.2]

"certification authority" *has the same meaning as in the Third Schedule;*

[ETA s.2]

"Controller" means the Controller of Certification Authorities appointed under *section 22(1)* and includes a Deputy or an Assistant Controller of Certification Authorities appointed under section *22(2);*

[ETA s.2]

"digital signature" has the same meaning as in the Third Schedule;

[ETA s.2]

"recognised certificate" means a recognised certificate within the meaning of section 24;

"recognised certification authority" means a recognised certification authority within the meaning of section 24;

"relevant Parts" means the provisions of this Part, Part V and any regulations made thereunder.

(2) For the avoidance of doubt, a reference to this Part shall include a reference to the Second and Third Schedules.

Specified security procedures

21.*—(1) The Minister may, by order in the Gazette, amend the Second Schedule to add, delete or modify any specified security procedure for the purposes of this Act.*

(2) The provisions set out in the Third Schedule shall apply to the corresponding specified security procedures.

(3) The Minister may, by order published in the Gazette, amend the Third Schedule to make provisions relating to any of the specified security procedures, including —

(a) specifying the conditions under which any security procedure may be treated as a secure electronic signature for the purposes of section 19;

(b) specifying the conditions under which any electronic record may be treated as a secure electronic record for the purposes of section 19;

(c) prescribing the effect of and duties relating to the use of specified security procedures, including the rights and duties of

any persons relating to the use of such procedures and specifying the rules relating to presumptions, the assumption of risk, the foreseeability of reliance and liability limits applicable to the use of specified security procedures; and

(d) providing that a contravention of any provision in that Schedule shall be an offence and providing a penalty not exceeding a fine of $20,000 or imprisonment for a term not exceeding 2 years or both.

Appointment of Controller and other officers

22.—(1) The Minister shall appoint a Controller of Certification Authorities for the purposes of *the relevant Parts* and, in particular, for the purposes of *accrediting*, certifying, monitoring and overseeing the activities of certification authorities.

(2) The Controller may, after consultation with the Minister, appoint such number of Deputy and Assistant Controllers of Certification Authorities and officers as the Controller considers necessary to exercise and perform all or any of the powers and duties of the Controller under this Act.[3]

(3) The Controller, the Deputy and Assistant Controllers and officers appointed by the Controller under subsection (2) shall exercise, discharge and perform the powers, duties and functions conferred on the Controller under this Act[4] subject to such directions as may be issued by the Minister.[5]

[ETA s. 41]

---

[3] The reference to "any regulations made thereunder" are omitted from the new section as, by virtue of section 26A of the Interpretation Act (Cap. 1), the reference to the Act includes a reference to any subsidiary legislation made under the Act.

[4] See footnote 3.

[5] Section 41(4) has been omitted as provision has been made in section 23(2)(*f*) for regulations to be made in respect of the maintenance of the publicly accessible database of accredited certification authorities. Section 41(5) has been moved to paragraph 1(2) of the Third Schedule.

Regulation of *specified security procedures* and certification authorities

23.—(1) The Minister may make regulations for the *carrying out of the relevant Parts and, without prejudice to such general power, may make regulations for all or any of the following purposes —*

(a) for the regulation, licensing or accreditation of any persons involved in the provision of any specified security procedure, including the conduct of any inquiry into the conduct of such persons and the recovery of the costs and expenses involved in such an inquiry;

(b) to safeguard or maintain the effectiveness and efficiency of the common security infrastructure relating to the use of secure electronic signatures and the authentication of electronic records, including the imposition of requirements to ensure interoperability between certification authorities or in relation to any security procedure;

(c) to ensure that the common security infrastructure relating to the use of secure electronic signatures and the authentication of electronic records complies with Singapore's international obligations;

(d) prescribing the forms and fees applicable for the purposes of the relevant Parts.

(2) Without prejudice to the generality of subsection (1), the Minister may make regulations for *the regulation and accreditation of certification authorities or their authorised representatives, including —*

(a) prescribing the accounts *to be* kept by certification authorities;

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

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

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

(e) providing for the use of any accreditation mark in relation to the activities of accredited certification authorities and controlling the use thereof;

(f) the maintenance of a publicly accessible database by the Controller containing a certification authority disclosure record for each accredited certification authority; and

(g) the duties and liabilities of an accredited certification authority in respect of its customers.

(3) Regulations made under this section may provide that a contravention of a specified provision shall be an offence and may provide penalties not exceeding a fine of $50,000 or imprisonment for a term not exceeding 12 months or both.

[ETA s. 42 and 46]

Cross-border recognition of certification authorities _and certificates_

24.—(1) *A certification authority or a certificate shall be a recognised certification authority or a recognised certificate, as the case may be, for the purposes of this Act if it satisfies the requirements prescribed under subsection (2).*

(2) The Minister may make regulations prescribing any requirements for the purposes of subsection (1), including any requirements —

(a) relating to interoperability arrangements with the certification authority;

(b) that the certification authority satisfies certain requirements relating to accredited certification authorities;

(c) that the certificate has been guaranteed by an accredited certification authority;

(d) that the certification authority or certificate has been registered, accredited or licensed under any specified registration, accreditation or licensing scheme established outside Singapore; or

(e) that the certification authority or certificate has been recognised under a specified bilateral or multilateral agreement with Singapore.

[ETA s. 43]

PART V

ENFORCEMENT OF PART IV

Obligation of confidentiality

25.—(1) Except for the purposes of *the relevant Parts* or for any prosecution for an offence under any written law or pursuant to an order of court, no person who has, pursuant to any powers conferred under *the relevant Parts*, obtained access to any electronic record, book, register, correspondence, information, document or other material shall disclose such electronic record, book, register, correspondence, information, document or other material to any other person.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both.

[ETA s. 48]

Offence by body corporate

26. Where an offence under *the relevant Parts* is committed by a body corporate, and it is proved to have been committed with the consent or connivance of, or to be attributable to any act or default on the part of, any director, manager, secretary or other similar officer of the body corporate, or any person who was purporting to act in any such capacity, he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

[ETA s. 49]

Authorised officer

27.—(1) The Controller may in writing authorise any officer or employee to exercise any of the powers of the Controller under this *Act*, *except the power of authorisation under this section.*[6]

---

[6] Section 50(2) which is omitted from the proposed bill reads as follows:

"(2) The Controller and any such officer shall be deemed to be a public servant for the purposes of the Penal Code (Cap. 224)."

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

[ETA s. 50]

Controller may give directions for compliance

28.—(1) The Controller may, by notice in writing, direct *any accredited person,* or any officer or employee *of an accredited person* —

(a) to take such measures or stop carrying on such activities as are specified in the notice if they are necessary to ensure compliance with *the relevant Parts;*[7] *or*

(b) to co-operate with any other certification authorities or public agencies as the Controller thinks necessary in the case of a public emergency.

(2) Any person who fails to comply with any direction specified in a notice issued under subsection (1) shall be guilty of an offence and 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.

(3) If any doubt arises as to the existence of a public emergency for the purposes of subsection (1)(b), a certificate signed by the Minister delivered to the certification authority shall be conclusive proof on the point.

[ETA s. 51]

Power to investigate

29.—(1) The Controller or an authorised officer may investigate the activities of *any accredited person* in relation to its compliance with *the relevant Parts.*[8]

(2) For the purposes of subsection (1), the Controller may in writing issue an order to *an accredited person* to further its investigation or to secure compliance with *the relevant Parts*.[9]

[ETA s. 52]

---

[7] See footnote 3.

[8] See footnote 3.

[9] See footnote 3.

Access to computers and data

30.—(1) The Controller or an authorised officer shall be entitled at any time to —

(*a*) have access to and inspect and check the operation of any computer system and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under this Act; and

(*b*) use or caused to be used any such computer system to search any data contained in or available to such computer system.

(2) The Controller or an authorised officer shall be entitled to require —

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

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

to provide him with such reasonable technical and other assistance as he may require for the purposes of subsection (1).

(3) Any person who —

(*a*) obstructs the lawful exercise of the powers under subsection (1); or

(*b*) fails to comply with a request under subsection (2),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 12 months or to both.

[ETA s. 53]

Obstruction of Controller or authorised officer

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

[ETA s. 54]

Production of documents, data, etc.

32. The Controller or an authorised officer shall, for the purposes of the execution of *the relevant Parts*, have power to do all or any of the following:

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

(*b*) require the production of any identification document from any person in relation to any offence under this Act[10];

(*c*) make such inquiry as may be necessary to ascertain whether *the relevant Parts* have been complied with.

[ETA s. 55]

General penalties

33. Any person guilty of an offence under this Act[11] for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 6 months or to both.

[ETA s. 56]

Sanction of Public Prosecutor

34. No prosecution in respect of any offence under this Act[12] shall be instituted except by or with the sanction of the Public Prosecutor.

[ETA s. 57]

Jurisdiction of Courts

35. A District Court shall have jurisdiction to hear and determine all offences under this Act[13] and, notwithstanding anything to the contrary in the Criminal Procedure Code (Cap. 68), shall have power to impose the full penalty or punishment in respect of any offence under this Act[14].

[ETA s. 58]

---

[10] See footnote 3.

[11] See footnote 3.

[12] See footnote 3.

[13] See footnote 3.

[14] See footnote 3.

Composition of offences

36.—(1) The Controller may, in his discretion, compound any offence under this Act[15] which is prescribed as being an offence which may be compounded by collecting from the person reasonably suspected of having committed the offence a sum not exceeding —

(a) one half of the amount of the maximum fine that is prescribed for the offence; or

(b) $5,000,

whichever is the lower.

(2) The Minister may make regulations prescribing the offences which may be compounded.

[ETA s. 59]

PART VI

USE OF ELECTRONIC RECORDS
AND SIGNATURES *BY PUBLIC AGENCY*

Acceptance of electronic filing and issue of documents

37.—(1) Any *public agency* that, pursuant to any written law —

(*a*) accepts the filing of documents, or *obtains information in any form*;

(b) requires that documents be created or retained;

(*c*) *requires documents, records or information to be provided or retained in their original form;*

(*d*) issues any permit, licence or approval; or

(*e*) provides for the method and manner of payment,

may, notwithstanding anything to the contrary in such written law, *carry out that function by means of electronic records or in electronic form*.

[ETA s. 47(1)]

---

[15] See footnote 3.

(2) In any case where a *public agency* decides to perform any of the functions in subsection (1) *by means of electronic records or in electronic form, the public agency* may specify —

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

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

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

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

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

[ETA s. 47(2)]

(3) For the avoidance of doubt, notwithstanding anything to the contrary in any written law but subject to any specification made under subsection (2), where any person is required by any written law to —

(a) file any document with or provide information in any form to a public agency;

(b) create or retain any document for a public agency;

(c) use a prescribed form for an application or notification to, or other transaction with, a public agency;

(d) provide to or retain for a public agency any document, record or information in its original form; or

(e) hold a licence, permit or other approval from a public agency,

such a requirement is satisfied by an electronic record specified by the public agency for that purpose and —

(i) in the case of a requirement referred to in paragraph (a), (c) or (d), transmitted or retained (as the case may be) in the manner specified by the public agency;

(ii) in the case of a requirement referred to in paragraph (b), respectively created or retained in the manner specified by the public agency; or

(iii) in the case of a requirement referred to in paragraph (e), issued by the public agency.

(4) Subject to sections 9 and 10, nothing in this Act shall by itself compel any public agency to accept or issue any document or information in the form of electronic records or to accept any payment in electronic form.

PART VII

GENERAL

Liability of network service providers

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

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

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

(2) Nothing in this section shall affect —

(*a*) any obligation founded on contract;

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

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

(*d*) any liability of a network service provider under the Copyright Act (Cap. 63) in respect of —

(i) the infringement of copyright in any work or other subject-matter in which copyright subsists; or

(ii) the unauthorised use of any performance, the protection period of which has not expired.

(3) For the purposes of this section —

"performance" and "protection period" have the same meanings as in Part XII of the Copyright Act;

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

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

[ETA s. 10]

Power to exempt

39. The Minister may exempt, subject to such terms and conditions as he thinks fit, any person or class of persons from all or any of the provisions of this Act or any regulations made thereunder.

[ETA s. 60]

Regulations

40. The Minister may make regulations to prescribe anything which is required to be prescribed under this Act and generally for the carrying out of the provisions of this Act.

[ETA s. 61]

Repeal and transitional provisions

41.*—(1) The Electronic Transactions Act (Cap. 88) (referred to in this section as the repealed Act) is repealed.*

(2) Subject to subsection (3), this Act shall apply to all acts or transactions done in relation to an electronic record, including the generation, signing or communication of an electronic record, made on or after the date of commencement of this Act.

(3) If, immediately before the date of commencement of this Act —

(a) by virtue of section 8 of the repealed Act, an electronic signature was treated as having satisfied any rule of law requiring a signature, or providing certain consequences if a document is not signed;

(b) by virtue of section 9 of the repealed Act, an electronic record was treated as having satisfied a rule of law requiring certain documents, records or information to be retained; or

(c) by virtue of section 15 of the repealed Act, an electronic record was treated as having been despatched or received,

the provisions of this Act shall not affect that treatment of the electronic signature or electronic record, as the case may be.

FIRST SCHEDULE

Section 4

MATTERS EXCLUDED BY SECTION 4

Provision	*Matter*
1. Part II	The creation or execution of a will
2. Part II	Negotiable instruments, documents of title, *bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money* [UN Art 2(2)]
3. Part II	The creation, performance or enforcement of an indenture, declaration of trust or power of attorney, with the exception of *implied*, constructive and resulting trusts

Provision	*Matter*
4. Part II	Any contract for the sale or other disposition of immovable property, or any interest in such property
5. Part II	The conveyance of immovable property or the transfer of any interest in immovable property
6. Part II	*Transactions on a regulated exchange* [UN Art 2(1)(b)(i)]
7. Part II	*Foreign exchange transactions* [UN Art 2(1)(b)(ii)]
8. Part II	*Inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments* [UN Art 2(1)(b)(iii)]
9. Part II	*The transfer of security rights in sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments held with an intermediary* [UN Art 2(1)(b)(iv)]

SECOND SCHEDULE

Sections 2 and 21

SPECIFIED SECURITY PROCEDURES

1. *Digital signatures, as defined in the Third Schedule.*

THIRD SCHEDULE

Sections 20 and 21

DIGITAL SIGNATURES

GENERAL

Interpretation

1.—(1) *In this Schedule,* unless the context otherwise requires —

"accredited certification authority" means a certification authority accredited by the Controller pursuant to any regulations made under section 24;

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

"certificate" means a record issued for the purpose of supporting digital signatures which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;

"certification authority" means a person who or an organisation that issues a certificate;

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

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

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

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

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

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

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

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

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

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

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

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

"public key" means the key of a key pair used to verify a digital signature;

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

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

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

"suspend", *in relation a certificate*, means to temporarily suspend the operational period of the certificate from a specified time;

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

(*a*) are reasonably secure from intrusion and misuse;

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

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

(*d*) adhere to generally accepted security procedures;

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

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

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

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

[ETA s. 2]

(2) In the application of *the relevant Parts* to certificates issued by the Controller and digital signatures verified by reference to those certificates, the Controller shall be deemed to be *an accredited* certification authority.

[ETA s. 41(5)]

Secure electronic record with digital signature

2. The portion of an electronic record that is signed with a digital signature shall be treated as a secure electronic record *for the purposes of section 19* if the digital signature is a secure electronic signature by virtue of *paragraph 3*.

[ETA s. 19]

Secure digital signature

3. When any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature *for the purposes of section 19* with respect to such portion of the record, if —

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

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

(i) the certificate was issued by *an accredited* certification authority operating in compliance with the regulations made under *section 23*;

(ii) the certificate was issued by a *recognised* certification authority;

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

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

[ETA s. 20]

Presumptions regarding certificates

4. It shall be presumed, unless evidence to the contrary is adduced, that the information (except for information identified as subscriber information which has not been verified) listed in a certificate issued by *an accredited* certification authority *or a recognised certification authority, or in a recognised certificate*, is correct if the certificate was accepted by the subscriber.

[ETA s. 21]

Unreliable digital signatures

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

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

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

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

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

[ETA s. 22]

Reliance on certificates foreseeable

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

[ETA s. 23]

Prerequisites to publication of certificate

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

(*a*) the certification authority listed in the certificate has not issued it;

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

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

[ETA s. 24]

Publication for fraudulent or unlawful purpose

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

[ETA s. 25]

False or unauthorised request

9. Any person who knowingly misrepresents to a certification authority his identity or authorisation for the purpose of requesting for a certificate or for suspension or revocation of a certificate shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 6 months or to both.

[ETA s. 26]

Recommended reliance limit

10.—(1) *An accredited* certification authority *or a recognised certification authority* shall, in issuing a certificate to a subscriber, specify a recommended reliance limit in the certificate.

(2) The *accredited* certification authority *or recognised certification authority* may specify different reliance limits in different certificates as it considers fit.

[ETA s. 44]

Liability limits for *accredited* certification authorities

11. Unless *an accredited* certification authority *or a recognised certification authority* waives the application of this *paragraph*, *an accredited* certification authority *or a recognised certification authority* shall not be liable —

(*a*) for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the *accredited* certification authority *or recognised certification authority* complied with the requirements of this Act; or

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

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

(ii) failure to comply with *paragraphs 14 and 15* in issuing the certificate.

[ETA s. 45]

DUTIES OF CERTIFICATION AUTHORITY

Trustworthy system

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

[ETA s. 27]

Disclosure

13.—(1) A certification authority shall disclose —

(*a*) its certificate that contains the public key corresponding to the private key used by that certification authority to digitally sign another certificate (referred to in this *paragraph* as a certification authority certificate);

(*b*) any relevant certification practice statement;

(*c*) notice of the revocation or suspension of its certification authority certificate; and

(*d*) any other fact that materially and adversely affects either the reliability of a certificate that the authority has issued or the authority's ability to perform its services.

(2) In the event of an occurrence that materially and adversely affects a certification authority's trustworthy system or its certification authority certificate, the certification authority shall —

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

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

[ETA s. 28]

Issue of certificate

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

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

(*b*) has —

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

(ii) in the absence of a certification practice statement, complied with the conditions in *sub-paragraph* (2).

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

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

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

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

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

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

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

[ETA s. 29]

Representations upon issuance of certificate

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

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

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

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

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

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

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

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

[ETA s. 30]

Suspension of certificate

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

(*a*) the subscriber listed in the certificate;

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

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

[ETA s. 31]

Revocation of certificate

17. A certification authority shall revoke a certificate that it issued —

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

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

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

[ETA s. 32]

Revocation without subscriber's consent

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

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

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

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

(*d*) an individual subscriber is dead; or

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

(2) Upon effecting such a revocation, other than under *sub-paragraph* (1)(*d*) or (*e*), the certification authority shall immediately notify the subscriber listed in the revoked certificate.

[ETA s. 33]

Notice of suspension

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

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

[ETA s. 34]

Notice of revocation

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

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

[ETA s. 35]

DUTIES OF SUBSCRIBERS

Generating key pair

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

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

[ETA s. 36]

Obtaining certificate

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

[ETA s. 37]

Acceptance of certificate

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

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

(i) to one or more persons; or

(ii) in a repository; or

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

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

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

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

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

[ETA s. 38]

Control of private key

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

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

[ETA s. 39]

Initiating suspension or revocation of certificate

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

[ETA s. 40]

ANNEX B

PROPOSED ELECTRONIC TRANSACTIONS (CERTIFICATION AUTHORITY) REGULATIONS 2009

No. S 000 -

ELECTRONIC TRANSACTIONS ACT 2009
(ACT NO. 2009)

ELECTRONIC TRANSACTIONS (CERTIFICATION AUTHORITY) REGULATIONS 2009

ARRANGEMENT OF REGULATIONS

In exercise of the powers conferred by sections 23 and 40 of the Electronic Transactions Act 2009, the Minister for Information and the Arts hereby makes the following Regulations:

PART I

PRELIMINARY

Citation

1. These Regulations may be cited as the Electronic Transactions (Certification Authority) Regulations *2009 and shall come into operation on 2009.*

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;[1]

"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.

[regulation 2]

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.

---

[1] The definition of "licence" which reads as follows will be deleted:

""licence" means a licence granted under these Regulations."

(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. [2]

[regulation 3]

[3]**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.*

---

[2] The existing regulation 3 reads as follows:

"**Application to be licensed certification authority**
3. —(1) Every application to be a licensed certification authority shall be made in such form and manner as the Controller may, from time to time, determine and shall be supported by such information as the Controller may require.
(2) The Controller may require the applicant to furnish such additional information as are necessary in support of the application.
(3) The Controller may allow applications for renewal of licences to be submitted in the form of electronic records subject to such requirements as the Controller may impose.
(4) A licence shall be subject to such conditions, restrictions and limitations as the Controller may, from time to time, determine."

[3] Regulation 4 of the existing Regulations will be deleted.

(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 newspaper*s* and in such manner as the Controller may determine, *not* later than 2 months before the expiry of the *accreditation*.[4]

[regulation 5]

[5]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

---

[4] The existing regulation 5 reads as follows:

"**Renewal of licence**
5. —(1) Regulation 3 shall apply to an application for renewal of a licence as it applies to a fresh application for a licence.
(2) A certification authority shall submit an application for the renewal of its licence no later than 3 months before the expiry of its licence.
(3) If the certification authority has no intention to renew its licence, the certification authority shall —
(a) inform the Controller in writing no later than 3 months before the expiry of the licence;
(b) inform all its subscribers in writing no later than 2 months before the expiry of the licence; and
(c) advertise such intention in such daily newspaper and in such manner as the Controller may determine, no later than 2 months before the expiry of the licence."

[5] Regulation 6 of the existing Regulations will be deleted.

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

[regulation 11]

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 28* 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 contravenes or 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.

[regulation 12]

***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 28* 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 its certification practice statement; and

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

[regulation 13]

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) *Subject to paragraph (1), 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.

[regulation 14]

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.[6]

(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.[7]

(3) In considering whether to defer the execution of the decision, the Controller shall have regard to whether the deferment is

---

[6] The existing regulation 15(1) which reads as follows will be modified and renumbered as regulation 9(1) and the underlined words will be deleted:

"**15.** —(1) Where —
(a) the Controller refuses to grant or renew a licence under regulation 11;
(b) the Controller revokes a licence under regulation 12;
(c) the licence is revoked or suspended, or a certification authority is reprimanded, under regulation 13; or
(d) a performance bond or banker's guarantee is invoked under regulation 7(2),
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 whose decision shall be final."

[7] The existing regulation 15(2) which reads as follows will be modified and renumbered as regulation 9(2) and the underlined words will be deleted:

"**15**(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, as the case may be, until a decision is made by the Minister or when the appeal is withdrawn."

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.

[regulation 15]

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*.[8]

[regulation 7(1)(a)]

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 —

---

[8] Regulation 7 of the existing Regulations will be deleted.

(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.

[regulation 8]

Certification practice statement

12. *An accredited certification authority* must have *and comply with* a certification practice statement approved by the Controller.[9]

[regulation 9(1)(a)]

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.

[regulation 16]

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);

---

[9] Regulation 9 of the existing Regulations will be deleted.

(*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.

[regulation 17]

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 *paragraph 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 *paragraph 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 *paragraph 3(b)(i) of the Third Schedule to* the Act.

[regulation 18]

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 *paragraph 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.

[regulation 19]

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.

[regulation 20]

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.

[regulation 21]

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.

[regulation 22]

Expiry date of certificates

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

[regulation 23]

***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.

[regulation 24]

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 anyway and this indication should be revealed in the process of verifying the signature.

[regulation 25]

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 other laws.

(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.

[regulation 26]

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.

[regulation 27]

Confidentiality

25.—(1) Except for the purposes of *Part V* of the Act or for any prosecution under any written law or pursuant to an order of court, every *accredited* certification authority and its authorised agent must keep all subscriber-specific information confidential.

(2) Any disclosure of subscriber-specific information by the *accredited* certification authority or its agent must be authorised by the subscriber.

(3) This regulation shall not apply to subscriber-specific information which —

(*a*) is contained in the certificate for public disclosure;

(*b*) is otherwise provided by the subscriber to the *accredited* certification authority for this purpose; or

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

[regulation 28]

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;

(b) the percentage of the voting shares in the certification authority acquired by that person.[10]

[regulation 29]

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.

[regulation 30]

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.

[regulation 31]

PART VII

ACCREDITATION MARK

Use of accreditation mark

***29.**—(1) Subject to any conditions imposed by the Controller, an accredited certification authority may use an accreditation mark.*

---

[10] The existing regulation 29 reads as follows:

"**29.** A licensed certification authority shall inform the Controller of any changes in the appointment of any person as its director or chief executive, or of any person to perform functions equivalent to that of a chief executive, within 3 working days from the date of appointment of that person."

(2) Except in accordance with paragraph (1), no person shall use an accreditation mark or a colourable imitation thereof.

(3) Any person who contravenes paragraph (2) 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 *paragraph 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(3))*, 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 the *public agency* that is approved by the Minister under *paragraph 3(b)(iii) of the Third Schedule to* the Act.

[regulation 32]

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*.

[regulation 33]

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.

[regulation 34]

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*.[11]

[regulation 35]

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.

---

[11] The existing regulation 35(4) which reads as follows will be modified with the underlined words deleted and renumbered as regulation 33(4):

"**35**(4) A licensed certification authority shall —
(a) give the Controller a minimum of 3 months' written notice of its intention to discontinue its operations;
(b) give its subscribers a minimum of 2 months' written notice of its intention to discontinue its operations; and
(c) advertise, in such daily newspaper and in such manner as the Controller may determine, at least 2 months' notice of its intention to discontinue its operations."

(6) A copy of *the* audit report shall be submitted to the Controller within 4 weeks of the completion of an audit.[12]

[regulation 10]

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* 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.

[regulation 36]

Composition of offences

36. Any offence under *section 28(2) of the Act or* under these Regulations may be compounded by the Controller under *section 36* of the Act.

[regulation 37]

Revocation

37. *The Electronic Transactions (Certification Authority) Regulations (Cap. 88, 2001 Ed., Rg 1) (referred to in these Regulations as the previous Regulations) are revoked.*

Transitional

38.*—(1) A certification authority which, immediately before the date of operation of these Regulations, 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

---

[12] Regulation 10(6) of the existing Regulations which reads as follows will be deleted:

"**10**(6) Failure to pass the audit may be a ground for revocation of a licence."

(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

[To be confirmed]

Made this day of 2009.

[……..]
Permanent Secretary,
Ministry of Information,
Communications and the Arts,
Singapore.

ANNEX C

COMPLIANCE AUDIT CHECKLIST

COMPLIANCE AUDIT CHECKLIST

1. Certificate Authority Overall Governance

S/No	Control Steps	Checks
Obligations to Subscribers, Relying Party and User Community		
1	**User Community Obligation** The Auditor shall review that the Certification Authority (CA) has informed the User Community of: 1. The CA's procedures for certificate registration, issuance, suspension and revocation; 2. Any *force majeure* that relieves the CA of its duties; 3. The time-intervals between each update and publication of the certificate suspension, revocation and Certification Revocation List (CRL) information; 4. The scope and limitations of the CA's liabilities with respect to the expected reliance to be placed in the information contained in the certificates; 5. The CA's Certificate Practice Statement (CPS) and Certificate Policies (CP). In addition, the Auditor shall review that: 1. The mode of communication should be reasonable to reach a majority of the User Community; 2. All updates are within the established time-intervals defined by the CA.	1. Sight evidence that the CA has performed its obligation to the User Community as defined in the Control Step.
2	**Subscribers Obligation** The Auditor shall review that the CA has informed the Subscribers of their responsibility to validate the accuracy of the information contained in their certificates upon issuance. In addition, the Auditor shall review that: 1. Subscribers' explicit consent has been obtained before publication of their certificates on the repository; 2. The CA has informed the Subscribers on how the private keys have been protected.	1. Sight evidence that the CA has performed its obligation to the Subscribers as defined in the Control Step; 2. Sampled observations of Subscribers' acknowledgements on their responsibility; 3. Inquire the CA if any Subscribers' certificates are published and sight obtained consent.
3	**Relying Party Obligation** The Auditor shall review that the CA has informed the Relying Party on steps to be taken to verify the authenticity and validity of a certificate. The steps shall include but are not limited to the verification of: 1. Issuer's signature; 2. Policy parameters; 3. Usage parameters; 4. Validity period; 5. Revocation or suspension information; and 6. Reliance limit.	1. Sight evidence that the CA has performed its obligation to the Relying Party as defined in the Control Step.
Certificate Practice Statement (CPS) and Certificate Policies (CP)		
4	The Auditor shall review that the CA has prepared its CP and CPS using guidelines stated in IETF's *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* (RFC 3647).	1. Inquire the CA on how they prepared the CP and CPS using RFC3647 as guidelines.

S/No	Control Steps	Checks
5	The Auditor shall review that the CP and CPS include the following: 1. Effective date; 2. Version number; 3. Change history; 4. Publication & Repository responsibilities; 5. CA's identification and authentication processes; 6. CA's Certificate Life-Cycle Operations; 7. Physical controls; 8. Procedural controls; 9. Personnel controls; 10. Technical security controls; 11. Audit trails; 12. Certificate and CRL profiles; 13. CA's self-assessment and external audit requirements; 14. Business and Legal matters; 15. Limited liability clauses. In addition, the Auditor shall review that each CP has been defined for each class of certificates. It is possible that all classes of certificates use the same CP.	1. Sight that the CP and CPS minimally contain the information as defined in the Control Step; 2. Sight that each CP has been defined for each class of certificate.
Security Management		
6	The Auditor shall review that an IT Security Policy exists and: • Is approved by the CA's management; • Is reviewed regularly; • Is communicated to, understood and acknowledged by personnel directly involved in the CA operations.	1. Sight the existence of an IT Security Policy; 2. Sight evidence that the IT Security Policy is approved and reviewed yearly; 3. Sampled observations of personnel acknowledgement forms which indicate they have read and understood the IT Security Policy.
7	The Auditor shall review that regular updates on security risks and exposures are communicated to personnel directly involved in the CA operations. The regular updates can be in the form of email, circulars, website updates or training.	1. Sampled observations of security risks and exposure updates communiqué.
8	The Auditor shall review that personnel responsible for security management have been trained by: 1. Inspecting qualifications/certifications such as CISSP or equivalent; OR 2. Inspecting if the personnel have attended training and the content of the training.	1. Observation of training records or certifications.
9	The Auditor shall review the access control matrixes and its follow-up actions on a regular basis.	1. Observation of monthly access control matrix review reports; 2. Sampled observations which indicate follow-up actions are implemented within 24 hours.

S/No	Control Steps	Checks
10	The Auditor shall review the existence and implementation of: 1. Vulnerability management procedures covering, but not limited to: a. sources of information; b. planning and execution of counter measures. 2. Incident management procedures covering, but not limited to: a. compromise of key; b. penetration of systems or network; c. unavailability of network; d. security incidents; e. fraudulent activities surrounding the registration, generation, suspension and revocation of certificates; f. informing the Controller within 24 hours of any incidents. In addition, the Auditor shall review that the CA has documented and acted on identified incidents.	1. Sight the existence of vulnerability management procedures and that they minimally contain the information as defined in the Control Step. 2. Sampled observations that the vulnerability management procedures are tested and reviewed at least once every 6 months. 3. Sight the existence of incident management procedures and that they minimally contain the information as defined in the Control Step. 4. Sampled observations that the incident management procedures are tested and reviewed at least once every 6 months. 5. Sampled observations of incident records and observations that follow-up actions have been performed.
Risk Management		
11	The Auditor shall review that the CA performs a regular risk assessment of its CA infrastructure, which includes: 1. Cryptographic algorithm and key parameters; 2. Physical security; 3. Operating system security; 4. Network security; 5. Application security; 6. PKI software.	1. Observation of risk assessment reports and that the assessment minimally covers the areas as defined in the Control Step; 2. Sampled observations that follow-up actions are implemented within 1 month; 3. Sight evidence that assessment is performed at least yearly or after major changes to CA infrastructure (involving more than 50% of core infrastructure).
12	The Auditor shall review that the CA has the following: 1. Risk Management Policy; 2. Risk Management Procedures. In addition, the Auditor shall review that the CA management review, update and approve the policy and procedures regularly.	1. Sight the existence of Risk Management Policy and Procedures; 2. Sight evidence that the IT Risk Management Policy is reviewed, updated and approved yearly; 3. Sight evidence that the IT Risk Management Procedures are reviewed, updated and approved half-yearly.
Personnel Controls		
13	The Auditor shall review that the CA has taken steps to verify that personnel to be employed for direct CA operations are subject to security screening. The security screening should cover: 1. Criminal history; 2. Bankruptcy status; AND 3. Personnel self-declaration on criminal and bankruptcy history. In addition, the Auditor shall review that the CA performs regular reviews of the security screening of personnel.	1. Sight security screening process documentation that the security screening minimally covers the areas as defined in the Control Step; 2. Sampled observations of security screening documents; 3. Sampled observations of personnel self declaration forms.

S/No	Control Steps	Checks
14	The Auditor shall review that: 1. All personnel involved in CA operations have signed a confidentiality agreement; 2. These confidentiality agreements are reviewed when the terms of their employment contracts change.	1. Sampled observations of confidentiality agreements; 2. Sampled observations that confidentiality agreements are reviewed during employment contract changes (hires and terminations).
15	The Auditor shall review that the CA has documented and implemented segregation of duties for key CA operational roles, including but not limited to: 1. Requestor – Approval; 2. Maker – Checker; 3. Administration – Security; 4. Operations – Security.	1. Sight access control matrixes that conflicting roles are not present; 2. Observation that system access controls are according to segregation of duties.
16	The Auditor shall review that the CA implements dual control to: 1. Root equivalent accounts to systems; 2. Administrative accounts to key applications.	1. Sight access matrix that personnel assigned to root accounts and administrative accounts have dual controls.
17	The Auditor shall review that the CA designs and implements job responsibilities and the corresponding access matrix (logical and physical). The job responsibilities and access matrix should be documented and contain: 1. Effective date and validity; 2. Role description and assignees; 3. Access control assigned (including physical security); 4. Training requirements. The job responsibilities and access matrix should include names of backups. In addition, the Auditor shall review that the CA reviews the job responsibilities and access matrix regularly.	1. Sight access control matrix that it minimally covers the areas as defined in the Control Step; 2. Sample observations that job responsibilities and access matrix are reviewed at least once every 3 months; 3. Observation that system access controls are according to assigned responsibilities.
Subscriber's data		
18	The Auditor shall review that the CA has designed and implemented steps to protect the confidentiality and privacy of the Subscribers' data, including transactional and historical data about the Subscribers' usage.	1. Sight the existence of procedures surrounding protection of Subscribers' data; 2. Sampled observations of protection mechanism.
19	The Auditor shall review that explicit permissions have been obtained from the Subscribers by the CA for third party disclosure.	1. Sampled observations of permissions obtained from Subscribers for third party disclosure.
Incident Management		
20	The Auditor shall review that the CA has an approved Incident Management Plan. The Plan should include, but is not limited to the following: 1. Key compromise (RA Key, CA certification Key); 2. Intrusion to systems and network; 3. Breach of physical security; 4. Infrastructure downtime; 5. Fraudulent activities surrounding certificate management. The Auditor shall also review that the CA has informed the Controller promptly for **confirmed** incidents.	1. Sight existence of an Incident Management Plan that minimally covers the areas as defined in the Control Step; 2. Sampled observations that the CA has informed the Controller within 24 hours for confirmed incidents.

S/No	Control Steps	Checks
21	The Auditor shall review that the CA has an approved Incident Response Action Plan. The Plan should include, but is not limited to the following: 1. Compromise control; 2. Revocation conditions and procedures(e.g. revocation of CA certificate in the event that the CA certification key is lost or compromised); 3. Notification Parties and procedures; 4. Service disruption procedures; 5. Audit trail protection and analysis; 6. Media and public relations. The Auditor shall also review that the CA has tested and trained personnel on usage of the Incident Response Action Plan.	1. Sight existence of an Incident Response Action Plan that minimally covers the areas as defined in the Control Step; 2. Sight evidence that the key personnel were trained on the Plan; 3. Sight evidence that the Plan is tested at least annually; 4. Sampled observations that the Plan is used for actual incidents.
Business Continuity Planning		
22	The Auditor shall review that the CA has the following plans available: 1. Business Continuity Plans; 2. Disaster Recovery (DR) Plans. The Plans should include 1. Continuity plans in the event of CA certification key loss or compromise; 2. Named personnel in the recovery team; 3. The availability of cold backups (redundant systems); 4. Location of the DR site; 5. Backup procedures for use in the event of *force majeure* not being excluded from their obligations. In addition, the Auditor shall review that the Plans have been tested and inadequacies were rectified.	1. Sight existence of a Business Continuity Plan that minimally covers the areas as defined in the Control Step; 2. Sight existence of a Disaster Recovery Plan that minimally covers the areas as defined in the Control Step; 3. Sampled observations that Plans are tested and reviewed at least once every 6 months; 4. Sample observations that inadequacies in the Plans are rectified.
23	The Auditor shall review that the named personnel in the recovery team have been trained in the execution of the Plans.	1. Sampled observations of Plan training records of recovery team.
24	The Auditor shall review that the cold backups of the hardware used in the Plans are available and accessible.	1. Sight sampled cold backups can be started.
25	The Auditor shall review that the DR site has basic security (physical and environmental) in place.	1. Inquire the CA on security controls in place at DR site; 2. Sampled observations of security controls in DR site.

2. Certificate Management Controls

S/No	Control Steps	Checks
26	The Auditor shall review that the following exists as certificate attributes: 1. Certificate policy; 2. Usage parameters; 3. Expiration parameters; 4. Distinction between CA certificate and user certificate. In addition, the Auditor shall review that the following information do not exist: 1. Distinguished name fields; 2. Other information of users that may be used in social engineering.	1. Observation of sampled certificates that have certificate attributes as defined in the Control Step.
Registration Process		
27	The Auditor shall review that the CA has defined and implemented authentication methods to verify the certificate applicant. The Auditor shall also review that the authentication documents used are retained.	1. Sight authentication procedures; 2. Sample certificates issued by the CA and sight corresponding authentication documents.
Generation Process		
28	The Auditor shall review that the procedures adhered to in the generation process are in accordance to the CP.	1. Sampled observations of evidence that the generation process is carried out in accordance to the CP.
29	The Auditor shall review that the: 1. Information in the certificate is the same as in the request; 2. The correct key pair is associated with the certificate information.	1. Sampled comparisons that request information is the same as in the generated certificates; 2. Sight evidence that the correct key pair is associated with the certificate information.
Issuance Process		
30	The Auditor shall review that the issuance channel used for the transmission of certificate, passwords and private keys between the CA and Subscribers is secure. In addition, the Auditor shall review that receipt of certificates is acknowledged and accepted by the Subscribers.	1. Inquire the CA on protection mechanisms used for the transmission of certificates; 2. Sampled observations of the implemented protection mechanisms; 3. Sampled observations of acknowledgements of receipt and acceptance by Subscribers.
Publication Process		
31	The Auditor shall review that the CA has published its certificate, CP, CPS and repository in a secure channel. In addition, the Auditor shall review that the following information is available for the User Community to verify: 1. Company Name; 2. Registration number; 3. X500 name; 4. Internet address; 5. Telephone number; 6. CA certificate; 7. Location of repository.	1. Inquire the CA on protection mechanisms used for publication; 2. Sampled observations of the implemented protection mechanisms; 3. Sight that the information is available for the User Community and minimally contains the information defined in the Control Step.
32	The Auditor shall review that the CA obtained explicit consent for publication of Subscriber's certificate information.	1. Sampled observations of consent given for certificate information that was published.

S/No	Control Steps	Checks
33	The Auditor shall review that access to the repository: 1. Is read-only to the public, Subscribers and User Community; 2. Has restricted access to the CA's assigned personnel for updating the repository. In addition, the Auditor shall review that the modifications to the CPS are subject to a change management procedure of request and approval.	1. Inquire the CA on access controls to the repository; 2. Sampled observations of the implemented access controls; 3. Sampled observations of change management request and approval forms.
Renewal Process		
34	The Auditor shall review that the renewal requests are submitted using a secure channel OR using the same authentication method in the registration process.	1. Observation of security mechanism of renewal channel; 2. Inspection of sampled renewal requests for evidence that the secure renewal channel is used.
Certificate Suspension Process		
35	The Auditor shall review that suspended certificates are re-activated by the CA after investigations have completed and no compromise has been confirmed.	1. Sampled observations of re-activated certificates have supporting documents that indicate no compromise has taken place.
36	The Auditor shall review that the CA has taken steps to verify the identity of the requestor of certificate suspension.	1. Sampled observations of identity verification documents.
37	The Auditor shall review that information of suspended certificates are updated in the CRL and are digitally signed by the CA.	1. Sight evidence that the CRL is updated within 1 hour upon verification that suspension request is valid; 2. Sight updates include reason and date/time of suspension; 3. Sight all updates are digitally signed by the CA.
38	The Auditor shall review that the CA has taken steps to ensure that the suspension information in the CRL is protected from unauthorized modifications.	1. Inquire the CA on protection mechanisms used to prevent unauthorized modifications of suspension information; 2. Sampled observations of the protection mechanisms.
39	The Auditor shall review that the CA has informed the Subscriber of suspension.	1. Sampled observations of communication to Subscribers.
Revocation Process		
40	The Auditor shall review that the CA revokes the certificate when: 1. Information marked with extension "critical" is inaccurate; 2. Private key or media holding the private key is suspected or actually compromised; 3. Subscriber is no longer a member of the community subject to CP; 4. The Subscriber requests it; 5. Suspected or actual violations of the generation or issuance process; 6. CA certificate is compromised.	1. Sight revocation procedures cover the conditions described in the Control Step; 2. Sampled observations of incidents which meet revocation conditions are revoked.
41	The Auditor shall review that the CA has taken steps to verify the identity of the requestor of certificate revocation.	1. Sight the CA verification procedures; 2. Sampled observations of verification documents.

S/No	Control Steps	Checks
42	The Auditor shall review the certificate revocation information contain, but is not limited to the following: 1. Reason for revocation; 2. Revocation date/time. In addition, the Auditor shall review that the certificate revocation information is digitally signed and published by the CA.	1. Sampled observations of certification revocation information as described in the Control Step; 2. Sampled observations that the revocation information is digitally signed by the CA; 3. Sampled observations that the revocation information is published.
43	The Auditor shall review that the CA has informed the Subscriber of revoked certificates.	1. Sampled observations of communication that the CA has informed the Subscriber of revoked certificates within 1 hour.
44	The Auditor shall review that the CA has taken steps to ensure that the certificate revocation information is protected from unauthorized modifications.	1. Inquire the CA on protection mechanisms used to prevent unauthorized modifications of revocation information; 2. Sampled observations of the protection mechanisms.
45	The Auditor shall review that the CA do not re-activate revoked certificates.	1. Inquire the CA on measures taken to prevent the re-activation of revoked certificates; 2. Sampled observations of the measures.
Archival Process		
46	The Auditor shall review that all certificate suspension and revocation information, certificates, registration documents are archived for 7 years.	1. Sampled observations of archived information (one for each year).
47	The Auditor shall review that the CA tests the archival process for accuracy, security and accessibility for digital archives.	1. Sight test results; 2. Sight evidence that testing is performed at least yearly; 3. Sampled observations that negative testing has been rectified.
Audit Trails		
48	The Auditor shall review that the CA keeps audit trails of certificate registration, generation, issuance, renewal, suspension and revocation.	1. Inquire the CA on the audit trails kept; 2. Sampled observations of the audit trails.
49	The Auditor shall review the security mechanism the CA implements for the protection of audit trails.	1. Inquire the security mechanisms used to protect the audit trails; 2. Sampled observations of the security mechanisms.
50	The Auditor shall review that the CA conducts periodic reviews of the audit trails.	1. Sight audit review documents; 2. Sight evidence that audit trails are reviewed at least once every 2 days.
51	The Auditor shall review that the CA keeps audit trails for 12 months.	1. Sampled observations of audit trails (sampled for each month).

3. Key Management Controls

S/No	Control Steps	Checks
Generation		
52	The Auditor shall review that segregation of duties exists between personnel involved in system setup and maintenance and personnel involved in the key generation process. In addition, the Auditor shall also review that keys are stored under dual control.	1. Sight access control matrixes that conflicting roles are not present and dual control exists for key assignment; 2. Observation that system access controls are according to segregation of duties.
53	The Auditor shall review that separate key pairs exists for digital signature and encryption.	1. Observation of separate key pairs.
54	The Auditor shall review that the CA uses random key values in the generation of keys. The Auditor shall also review that the seed (input) used in the random generator is not static and not predictable.	1. Inquire the CA on how seeds are produced; 2. Sampled observations of seed generation.
55	The Auditor shall review that the CA provides reviews and approves the key generation system used by the Subscribers.	1. Sampled observations of approval of key generation system used by the Subscribers.
Distribution		
56	The Auditor shall review that the CA has prescribed procedures for transferring the keys from the key generation system to the storage device in a secure manner.	1. Inquire the CA on protection mechanism of transferring keys; 2. Sampled observations of the protection mechanism.
Storage		
57	The Auditor shall review the CA has provided Subscribers the necessary instructions and programs to safeguard and encrypt the Subscribers' private keys.	1. Sight instructions and programs to Subscribers.
58	The Auditor shall review that the CA stores its keys in tamper proof devices. In addition, the Auditor shall review that: 1. Access to the tamper proof devices is dual controlled by personnel not involved in the setup, maintenance and operations of the CA systems; 2. The CA documents and approves the change of key custodians; 3. Backup custodians to reduce key-man risks exist.	1. Observation of tamper proof devices; 2. Sampled observations of key custodian change documentation; 3. Sight access control matrixes for key custodians, backups and segregation of duties of custodians.
Usage		
59	The Auditor shall review that the CA implements dual control loading of the certificates. In addition, the Auditor shall review that the CA performs integrity checks prior to loading of the certificates.	1. Inquire the CA on procedures of dual control on loading of certificates; 2. Inquire the CA on integrity checks; 3. Sampled observations that integrity checks and dual control are implemented.
Backups		
60	The Auditor shall review that the CA private keys are backed up.	1. Observation of the backup private keys; 2. Sight evidence that the backup keys are subject to the same controls as the original keys.

S/No	Control Steps	Checks
61	The Auditor shall review that the CA stores its backup keys in a separate physical location as the original key.	1. Observation of separate physical location for backup keys.
Key Change		
62	The Auditor shall review that the CA change the CA and Subscriber keys periodically. In addition, the Auditor shall review that the CA has provided notice to: 1. The Subscribers' relying parties of new key pairs used to sign certificates; 2. The Subscriber or owner of changed key in a secured manner.	1. Sampled observations of key change documentation; 2. Sampled observations that the CA has provided notice to the Subscriber as defined in the Control Step.
63	The Auditor shall review that the CA has a key interlock procedure and implements the procedure during key change.	1. Sight the key interlock procedures; 2. Sampled observations that procedures were followed.
Destruction		
64	The Auditor shall review that the CA archives and securely stores the backup copies upon the termination of a CA signature private key.	1. Sampled observations of archives and backups.
Key Compromise		
65	The Auditor shall review that the CA has an escalation process in the event of suspected or actual key compromise. In addition, the Auditor should review that the Controller is informed within 24 hours of suspected or actual key compromise.	1. Inquire the CA of historical compromise; 2. Sample compromise events and sight for evidence that the CA has informed the Controller within 24 hours.
66	The Auditor shall review that the CA has revoked all affected Subscriber certificates in the event of CA certification private key compromise.	1. Inquire the CA of historical compromise; 2. Observation that affected certificates have been revoked.
67	The Auditor shall review that the CA has revoked all affected keys and certificates in the case of subscriber private key compromise.	1. Inquire the CA of historical compromise; 2. Observation that affected keys and certificates have been revoked.
Key Archival		
68	The Auditor shall review that the CA has archived: 1. All CA Public keys (permanently) 2. All Subscriber encryption keys.	1. Sampled observations of archives.
69	The Auditor shall review that the archives are protected from unauthorized modification.	1. Inquire the CA of the protection mechanisms; 2. Sampled observations of the protection mechanism having been implemented.

S/No	Control Steps	Checks
Cryptographic Engineering		
70	The Auditor shall review that the CA performs its cryptographic processes in a hardware cryptographic module that minimally conforms to: 1. FIPS 140-1 Security Level 3; 2. FIPS 140-2 Security Level 3. For Registration Authority (RA) operations away from the CA, the cryptographic module should minimally conform to: 1. FIPS 140-1 Security Level 2; 2. FIPS 140-2 Security Level 2.	1. Sight evidence that the cryptographic hardware used has the appropriate FIPS certification.
71	The Auditor shall review that the CA has communicated to its Subscribers that their cryptographic operation should conform minimally to: 1. FIPS 140-1 Security Level 1; 2. FIPS 140-2 Security Level 1.	1. Sampled observations of communication to Subscribers and that it contains the minimum requirement of FIPS compliance.
72	The Auditor shall review that the CA ensures: 1. Cryptographic keys and algorithms are sufficient to protect the cryptographic results; 2. Asymmetric cryptographic algorithms conform to the IEEE standard specifications.	1. Inquire the CA on the sufficiency testing of the cryptographic keys and algorithms; 2. Sight evidence that the asymmetric cryptographic algorithms used are IEEE compliant.

4. System and Operational Controls

S/No	Control Steps	Checks
73	The Auditor shall review that access control matrixes (physical and logical) are defined for all operating systems, network devices, applications and databases used in the CA operations exist. The access control matrixes should include, but are not limited to: 1. Personnel names; 2. Access granted; 3. Validity of access rights; 4. The next access control matrix review date. In addition, the Auditor shall review the application and currency of the access controls defined in the access control matrixes.	1. Sight access control matrix minimally covers the areas as defined in the Control Step; 2. Observation of system, network, application and database access controls are implemented in accordance to the access control matrix.
74	The Auditor shall review that the CA performs an assessment of the CA infrastructure components, which includes: 1. Operating system; 2. Network devices; 3. Security software (e.g. Intrusion Detection System and Anti-virus Software). A full assessment is required for new components and an incremental assessment is required for updates or modifications to the infrastructure.	1. Sight assessment report and follow-up actions. 2. Sampled observations that follow-up actions are implemented.
75	The Auditor shall review that the CA performs regular scans using tools of its systems and network devices to identify security vulnerabilities. The tools must be able to scan system and network vulnerabilities. In addition, the Auditor shall review that follow-up actions have been performed.	1. Sampled observations of scan results; 2. Sight evidence that scanning is performed at least once a week; 3. Sampled observations that follow-up actions are implemented.
76	The Auditor shall review that the CA has deployed Intrusion Detection System (IDS). In addition, the Auditor shall review that follow-up actions have been performed for potential intrusions.	1. Sampled observations of follow-up actions of detected intrusions; 2. Sight evidence that the IDS covers 100% of components of the CA infrastructure.
77	The Auditor shall review that the CA performs regular log review of the following (using the access control matrixes): 1. Unauthorized access and modifications to key system files and utilities; 2. Unauthorized access and modifications of Subscribers' data. The Auditor shall also review that follow-up actions has been performed for identified unauthorized access.	1. Observation of log review reports 2. Sampled observations that follow-up actions have been implemented.

S/No	Control Steps	Checks
Physical Security		
78	The Auditor shall review that: 1. The location of the CA system is not publicly identified; 2. Physical security systems are installed; 3. Inventory of access control cards are dual-controlled; 4. Loss of access control cards are reported and follow-up actions are performed; 5. Systems performing certification should be partitioned under lock and key; 6. Entry to the partition must be logged with timestamps; 7. Entry logs are reviewed: 8. Access to infrastructure components (power control, communication riders and cabling) is restricted to authorized personnel; 9. An approval process for temporal or bypass access exists; 10. An IDS exists.	1. Sampled observations that the CA carries out the items described in the Control Step; 2. Sight evidence that entry logs are reviewed daily.
General Security Controls		
79	The Auditor shall review that: 1. Systems performing certification functions are not used for general purposes (e.g. word processing, emailing, web surfing); 2. Strong password policies are implemented; 3. System administrators are trained; 4. CA application operators are trained; 5. Inactive lockouts are implemented (no longer than 10 minutes of inactivity before lockout); 6. Updated security patches are reviewed, tested, applied and implemented.	1. Sampled observations that the CA carries out the items described in the Control Step.
General Operational Controls		
80	The Auditor shall review that: 1. System administrators are trained; 2. CA application operators are trained.	1. Sampled observations of training records.
Change and Configuration Management		
81	The Auditor shall review that: 1. All changes are supported by change requests; 2. All change requests are approved before construction; 3. All source codes should be version-controlled; 4. There is an approved process of moving from development to production; 5. Segregation of duties exists for source code migration.	1. Sampled observations that the CA carries out the items described in the Control Step.
Network Security		
82	The Auditor shall review that: 1. Network access control exists to separate and isolate CA systems from the other systems; 2. Communications between CA systems should be secure and data should not be transmitted in the clear; 3. IDS is present and that the IDS monitors the CA systems.	1. Sampled observations that the CA carries out the items described in the Control Step.

S/No	Control Steps	Checks
Monitoring and Audit Trails		
83	The Auditor shall review that the CA has the following audit trails: 1. Application transactions: a. Registration; b. Certification; c. Publication; d. Suspension; and e. Revocation. 2. System log files: a. Security violations; b. Errors; c. Execution of privilege functions; d. Changes in access control and system configurations. In addition, the Auditor shall review that the: 1. audit trails are protected from unauthorized access; 2. and retained for a minimum period of 12 months.	1. Sampled observations of audit trails and that they cover the items described in the Control Step; 2. Inquire the CA on the protection mechanism of audit trails; 3. Sampled observations of the protection mechanism; 4. Sampled observations of audit trail retention (sample from each month).
84	The Auditor shall review that the CA performs regular reviews of the audit trails and follow-up actions are performed.	1. Observation of audit trail review reports; 2. Sampled observations that follow-up actions have been implemented.

5. Application Integration Controls

S/No	Control Steps	Checks
85	The Auditor shall review that the application toolkits provided by the CA to the user and developer community comply with the following: 1. The user shall be informed when a private key is being accessed; 2. The user shall be alerted if its private key is being used for a purpose that is not consistent with that defined as acceptable use by the issuer; 3. Mechanisms shall be available to check the integrity of the applications for unauthorised modifications, especially the integrity of signing and verification functions; 4. Application security risk assessment on the CA's software infrastructure should be conducted yearly to ensure that the CA's software that manages, issues and revokes certificates is developed to manage the risk identified; 5. The application should securely purge the private key temporarily stored for processing to minimise private key exposure; 6. The application shall verify the validity and authenticity of the certificate; 7. The verification process shall trace and verify all the components in the certification path; 8. For validity and authenticity verification, it shall be necessary to verify that: a. The certificate issuer's signature is valid; b. The certificate is valid (i.e. has not expired, been suspended or revoked); and c. The certificate extensions flagged as "critical" are being complied with.	1. Sight that each application toolkit provided by the CA minimally complied with the requirements as defined in the Control Step.

6. Compliance with ETA and ETR

S/No	Control Steps	Checks
Compliance with ETA		
86	The Auditor shall review that the CA has complied with the following paragraphs of the Third Schedule of the Electronic Transactions Act (ETA): • Sub-paragraph 10(1); • All of paragraph 12; • All of paragraph 13; • All of paragraph 14; • All of paragraph 16; • All of paragraph 17; • All of paragraph 18; • All of paragraph 19; • All of paragraph 20.	1. Inquire the CA on its compliance with the relevant provisions of the ETA as defined in the Control Step; 2. Sight evidence that the CA has complied with the relevant provisions of the ETA as defined in the Control Step.
Compliance with ETR		
87	The Auditor shall review that the CA has complied with the following regulations of the Electronic Transactions (Certification Authority) Regulations (ETR): • Sub-regulations 11(1) and 11(3); • All of regulation 12; • All of regulation 13; • All of regulation 14; • All of regulation 15; • Sub-regulations 16(2), 16(3), 16(4), 16(5), 16(6), 16(7), 16(9), 16(10) and 16(11); • Sub-regulations 17(2) and 17(3); • Sub-regulations 18(2), 18(3), 18(4), 18(6), 18(7), 18(8), 18(10) and 18(11); • All of regulation 19; • All of regulation 20 • Sub-regulations 21(1), 21(2), 21(3), 21(4), 21(5), 21(7), and 21(8); • All of regulation 22; • Sub-regulations 23(6), 23(7), 23(8), 23(9), and 23(10); • All of regulation 24; • All of regulation 25; • Sub-regulations 26(1) and 26(3); • All of regulation 27; • All of regulation 28; • Sub-regulation 29(1); • Sub-regulations 32(3) and 32(4).	1. Inquire the CA on its compliance with the relevant provisions of the ETR as defined in the Control Step; 2. Sight evidence that the CA has complied with the relevant provisions of the ETR as defined in the Control Step.