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.

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE I: ELECTRONIC CONTRACTING ISSUES

(Consultation Paper)

LRRD No. 1/2004

19 Feb 2004

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE I: ELECTRONIC CONTRACTING ISSUES

The AGC (Law Reform and Revision Division) Team for this project comprises:

Mr Charles Lim Aeng Cheng	-	Principal Senior State Counsel
Mrs Joyce Chao	-	State Counsel

The following persons have rendered invaluable assistance to the team:

Mr Lawrence Tan	-	Senior Consultant, Infocomm Development Authority of Singapore

Legal Editorial and Publication

Ms Yvette Rodrigues	-	Senior Legal Executive, LRRD
Ms Adeline Sim	-	Legal Executive, LRRD
Ms Noraini Bte Jantan	-	Corporate Support Officer, LRRD

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE 1: ELECTRONIC CONTRACTING ISSUES

CONTENTS

EXECUTIVE SUMMARY OF PUBLIC CONSULTATION ON REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE I: ELECTRONIC CONTRACTING ISSUES

1 The Infocomm Development Authority of Singapore and the Attorney-General's Chambers are conducting a review of the Electronic Transactions Act (ETA) and Electronic Transactions (Certification Authority) Regulations (CA Regulations). For this purpose, a public consultation is being carried out in 3 stages dealing with electronic contracting issues, exclusions from the ETA under section 4 and secure electronic signatures and certification authorities.

2 Stage I of the Public Consultation concerns possible amendments to the ETA relating to **electronic contracting**. The consultation seeks guidance and feedback for the Singapore delegation on issues currently under consideration at the international level by UNCITRAL, in relation to on-going work on a draft Convention on Electronic Contracting by the UNCITRAL Working Group on Electronic Commerce. It also seeks public views on the potential impact of the proposed Convention.

3 Work on the UNCITRAL Convention on Electronic Contracting seeks to harmonise national laws as to how international contracts can be entered into electronically. Work on the Convention is in its final stages. If Singapore accedes to such a Convention, it is expected that the ETA will be amended for consistency with the provisions of the Convention.

4 This Consultation Paper on Electronic Contracting Issues highlights the main changes and issues which would arise from adopting the provisions of the draft UNCITRAL Convention on Electronic Contracting as it currently stands. It also discusses some other electronic contracting issues that arise apart from the Convention. Briefly, the Paper focuses on the following issues:

- Party Autonomy: Consent to Accept Electronic Communications and Variation by Agreement
- Recognition of Electronic Signatures
- Formation of Contract: Effectiveness of Electronic Communications and Attribution
- Time and Place of Despatch and Receipt

- Automated Information Systems
- Other Contract Issues e.g. Incorporation by Reference, Provision of Originals, etc.

5 The issues are described in greater detail below:

Party Autonomy: Consent and Variation (Part 2)

Consent to Accept Electronic Communications (para. 2.1)
Whether to adopt a provision (draft UNCITRAL Convention on Electronic Contracting, article 8, paragraph 2) that the electronic transactions legislation should not compel parties to accept contractual offers or acts of acceptance by electronic means in the context of all contractual transactions.

Variation (Section 5 of the ETA) (para. 2.2- 2.5)
Whether to amend or replace section 5 (which provides for variation of Parts II and IV of the ETA by agreement of the parties) in view of overlap with other provisions making specific sections apply subject to agreement otherwise, and the need for mandatory requirements which should not be open to variation by agreement of parties. Also, whether a variation provision would be necessary if there is a consent provision (see para.2.1).

Recognition of Electronic Signatures (Part 3)

Whether provisions on recognition of electronic signatures in the draft UNCITRAL Convention (article 9, paragraph 3) would be consistent with the ETA, especially in relation to function and reliability requirements. (Further issues relating to the definition of electronic signatures and digital signatures will be addressed in Stage III of the consultation on review of the ETA.)

Formation of Contract: Effectiveness of Electronic Communications and Attribution (Part 4)

Formation and Validity of Contracts (para. 4.1)
Whether there should be a provision on when an offer and acceptance in electronic form takes effect.

Invitation to make Offers (para. 4.2)
Whether a proposal to enter a contract made by electronic means to the world at large should be treated as an invitation to make offers, unless the proposal indicates that the person making the proposal intended to be bound in case of acceptance (draft UNCITRAL Convention, article 12).

Effectiveness of Communications between Parties (Section 12 of ETA) (para. 4.3)
Whether references to "declaration, demand, notice or request" should be added to section 12 of the ETA for consistency with the draft UNCITRAL Convention.

Attribution (Section 13 of the ETA) (para. 4.4)
Whether section 13 should be retained or amended in view of complications arising from the advent of the Internet, IT outsourcing and other IT developments. Also whether section 13(2)(b) should apply only if the information system was programmed by a person with authority to program the system on behalf of the originator, and whether "originator" should be defined to exclude an intermediary.

Time and Place of Despatch and Receipt (Section 15 of the ETA) (Part 5)

Whether to replace the rules of despatch and receipt in section 15 by adopting general rules that focus on the control over the electronic message or the capability of retrieving the data message (draft UNCITRAL Convention, article 10). Difficulties in determining whether parties are using the same information system. Whether to define "information system". (Definition of "automated information system" is considered in Part 6.)

Automated Information Systems (Part 6)

Whether to adopt definition of "automated information system" from article 5(f) of the draft UNCITRAL Convention (para.6.1). Whether to clarify that contracts resulting from the interaction of automated information systems shall 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 (draft UNCITRAL Convention, article 14) (para. 6.2). Other issues relating to the use of automated information systems e.g. conflicting terms (para.6.3) and attribution (para. 6.4). Whether to adopt a

provision to deal with the legal effects of errors made by a natural person communicating with an automated information system (para. 6.5).

Other Contract Issues (Part 7)

Incorporation By Reference (para. 7.1)
Whether to adopt a provision to clarify the validity of incorporation by reference in electronic communications. (UNCITRAL Model Law on Electronic Commerce, Article 5 *bis*)

Provision of Originals (para. 7.2)
Whether to provide for the requirement for an original to be met by an electronic functional equivalent and the criteria that must be met. (Draft UNCITRAL Convention, article 8).

Other issues (para 7.3)
Issues relating to the application of the Sale of Goods Act (Cap. 393) to software and digitised products, the validity of shrink-wrap and click-wrap agreements, whether the doctrine of privity of contract poses difficulties in allowing the purchaser to seek remedies from the immediate seller for defective software and consumer protection and other issues.

CONSULTATION PAPER

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE I: ELECTRONIC CONTRACTING ISSUES

PART I INTRODUCTION

1.1 This Joint IDA-AGC[1] Consultation Paper focuses on **Electronic Contracting Issues**. It is intended to solicit the views of industry and business, professionals, the public and Government Ministries and agencies, in order to inform the Government in considering possible amendments to the ETA relating to electronic commerce and to provide guidance and feedback to the Singapore delegation on issues currently under consideration at the international level by UNCITRAL[2].

1.2 This Consultation Paper discusses the following issues:

- Party Autonomy: Consent to Accept Electronic Communications and Variation by Agreement.
- Recognition of Electronic Signatures
- Formation of Contract: Effectiveness of Electronic Communications and Attribution.
- Time and Place of Despatch and Receipt
- Automated Information Systems
- Other Contract Issues e.g. Incorporation by Reference, Provision of Originals, etc.

1.3 With the enactment of the Electronic Transactions Act (Cap.88) in 1998, Singapore became the first country in the world to enact electronic transactions legislation based on the UNCITRAL Model

[1] Infocomm Development Authority of Singapore – Attorney-General's Chambers.

[2] UNCITRAL, or the United Nations Commission on International Trade Law, has a charter to "further the progressive harmonization and unification of the law of international trade". UNCITRAL does its work through six Working Groups. This includes Working Group IV on Electronic Commerce.

Law on Electronic Commerce. Since then, numerous other countries have adopted electronic commerce legislation based on the UNCITRAL model.[3]

1.4 Work is currently being undertaken at the international level by the UNCITRAL Working Group on Electronic Commerce to draft a Convention on Electronic Contracting to harmonise national laws as to how international contracts can be entered electronically.[4] Given the commitment of the Singapore Government to developing e-commerce and the obvious advantages that e-commerce holds for Singapore, Singapore is following closely UNCITRAL's work in this regard with the intention of adopting into our laws the outcomes of this important initiative.

1.5 If Singapore accedes to such a Convention, it is expected that the ETA will be amended for consistency with the provisions of the Convention. Although the Convention concerns international contracts, it is likely that a similar regime will be adopted for domestic contracts since it is generally undesirable to have a duality of regimes for international and domestic contracts. This is particularly so in the context of contracts concluded by electronic means since the actual location of the parties may not be known to or relevant to the parties.

1.6 In view of these developments overseas and internationally, the Ministry of Information, Communications and the Arts (MITA), the Infocomm Development Authority of Singapore (IDA) and the Attorney-General's Chambers (AGC) are undertaking a joint review of the Electronic Transactions Act. Stages II and III, which will follow in the coming months, will deal with other issues arising from the review of the Electronic Transactions Act, namely, **Exclusions from the ETA under section 4** and **Secure Electronic Signatures, Certification Authorities and e-Government**, respectively.

[3] See Annex B for list of recent legislation on electronic transactions and useful websites.

[4] For summary of progress made prior to the 42nd session of UNCITRAL Working Group IV from 11-21 Nov 2003 in A/CN.9/WG.IV/WP.103 at www.uncitral.org. All references in this paper to the draft UNCITRAL Convention are to the version contained therein unless otherwise stated. Report of the 42nd session was not publicly available at the time of completion of this paper.

- Please send your feedback to the Law Reform and Revision Division of the Attorney-General's Chambers, marked **"Re: Electronic Contracting Issues"**
  - via e-mail, at agc_lrrd@agc.gov.sg;
  - by post (a diskette containing a soft copy would be appreciated) to "**Law Reform and Revision Division, Attorney-General's Chambers, 1 Coleman Street, #05-04 The Adelphi, Singapore 179803**"; or
  - via fax, at **6332 4700**

- The closing date for this consultation is **15 March 2004**.

- A soft copy of the consultation paper may be downloaded from http://www.ida.gov.sg/idaweb/pnr/index.jsp or http://www.agc.gov.sg (under Publications).

- If you need any clarifications, please contact:
  - **Mr Lawrence Tan** via e-mail at lawrence_tan@ida.gov.sg; or
  - **Mrs Joyce Chao** via e-mail at agc_lrrd@agc.gov.sg.

- The Consultation will be carried out in 3 stages. This Consultation on Electronic Contracting Issues forms the first stage.

PART 2
PARTY AUTONOMY: CONSENT AND VARIATION

2.1 Consent to Accept Electronic Communications

2.1.1 Article 8, paragraph 2, of the draft UNCITRAL Convention on Electronic Contracting contains a general provision that "Nothing in this Convention requires a person to use or accept information in the form of data messages, but a person's consent to do so may be inferred from the person's conduct".

2.1.2 The consent provision reflects the idea that electronic transactions legislation should not compel parties to accept contractual offers or acts of acceptance by electronic means if they do not want to do so and upholds the principle of party autonomy. It also addresses concerns relating to universal access[5] and other difficulties relating to the receipt[6] and authentication[7] of email.

2.1.3 All recent electronic transactions legislation by developed countries have included consent requirements on the use of electronic communications. Some countries have consent provisions applicable to specific sections of their legislation[8]; others have a general consent

[5] Information may be delivered in a number of ways, including by letter, fax, e-mail or the Web. However, not everyone can send and receive electronic communications, either because they lack access to the necessary facilities or because they do not know how to use or are uncomfortable with the technology. This "digital divide" exists even in technologically advanced countries like the US and Singapore.

[6] It is the practice of many email providers to terminate free email accounts if they have not been accessed regularly. People change their email accounts frequently or may not access their email accounts regularly. Important email may be inadvertently deleted. It is a common practice for people to delete email *en bloc* without bothering to read them if they find their mail box full of junk mail.

[7] The use of electronic communications also gives rise to unique problems of authentication. On the recipient's part, he cannot be sure that an email purporting to be sent by a particular person is indeed so (short of checking by telephone or some other independent means) unless there is an authentication system in place. Authentication systems require proper installation on the recipient's end to work. This is more feasible in the case of a closed system limited to registered users than on the Internet.

[8] The **Australian** Commonwealth Electronic Transactions Act only has consent provisions that apply to specific provisions and consent is only required for persons other than a Commonwealth entity (i.e. an authority of the Commonwealth of Australia) e.g. s.9 (writing), s.10 (signature) etc. In the case of public authorities, their particular requirements have to be met. Consent may be inferred from conduct (s.5).

provision applicable to the whole Act[9]; while still others have both.[10] The US[11] applies a stricter standard in respect of consumer disclosures required to be provided in writing; consent is only effective in that case if there is a clear and conspicuous statement informing the consumer of his options, his right to withdraw consent, etc.

2.1.4 The consent requirement in the UNCITRAL draft Convention is stated in a manner that preserves the status quo. It does not create any new positive requirement for consent, merely that the Convention does not force any person to use or accept electronic communications. It is left to the applicable law to determine whether consent or agreement is required to use electronic communications in a particular case.

2.1.5 **Although the UNCITRAL Convention applies only to international contracts, since it is undesirable to create a different regime just for international contracts, the consent requirement should apply equally to domestic contracts. Therefore, if Singapore accedes to the UNCITRAL Convention, it is likely the ETA will be amended to include a similar consent provision for domestic as well as international contracts.**

[9]The **Canadian** Uniform Electronic Commerce Act employs a general consent provision applicable to the whole Act: "Nothing in this Act requires a person to use or accept information in electronic form, but a person's consent to do so can be inferred from the person's conduct" (s.6(1)). However, the Government's consent cannot be inferred by its conduct but must be expressed by communication (s.6(2)).

The **New Zealand** Electronic Transactions Act has a general provision applicable to the Part of the Act on Application of Legal Requirements to Electronic Transactions i.e. relating to requirements for writing, signatures, retention and originals: "Nothing in [Part 3 of the Act] requires a person to use, provide, or accept information in an electronic form without that person's consent" (s.17(1)). Consent may be inferred from conduct (s.17(2)). The default provisions on time and place of despatch and receipt apply except to the extent that the parties agree otherwise (s.9(a)). However, since the NZ Act only applies to statutory requirements, the requirement for consent applies only to statutory matters. In private dealings, parties may assume that electronic communications will be valid unless another party to the deal specifically says they are not. On its application to Government agencies, the *Electronic Transactions Act 2002: Plain English Section by Section Explanation* published by the Ministry of Economic Development states that "making the electronic means to make the application available on the Internet would constitute implied consent". Further in a case "where there has been an explicit statement [e.g. guidelines in relation to when a Government agency will or will not accept electronic communications], it is most unlikely that consent to use of electronic technology in a manner inconsistent with those guidelines could be inferred from conduct".

[10] E.g. **Irish** Electronic Transactions Act s.12 (writing requirement), s.13 (signature requirement), etc. General provision in s.24.

[11] The **US E-Sign Act** has a broad consent requirement: sec.101(b)(2). It does not apply to a governmental agency except with respect to contracts to which it is a party.

Q1:	Should the ETA include a consent provision similar to that in the draft UNCITRAL Convention, article 8, paragraph 2 (see para 2.1.1) in the context of all contractual transactions?

2.2 Variation (Section 5 of the ETA)

2.2.1 Although the ETA does not have a general consent requirement as discussed above,[12] it supports the principle of party autonomy through section 5 (which provides for variation of Parts II and IV of the ETA by agreement of the parties) and specific provisions in other sections making those sections subject to agreement otherwise by the parties.

2.2.2 Section 5 of the ETA provides that, as between parties involved in various enumerated electronic transactions, any provision of Part II (which relates to legal recognition of electronic records, requirements for writing, electronic signatures, and retention of electronic records) or Part IV (which relates to formation and validity of contracts, validity of declaration of intent or other statements, attribution, acknowledgement of receipt and time and place of despatch and receipt) of the Act may be varied by agreement.

2.2.3 It is based closely on the wording of article 4 of the UNCITRAL Model Law on Electronic Commerce. An equivalent provision in the draft Convention on Electronic Contracting was considered by the UNCITRAL Working Group at its 41st session.[13] On one view, a party's right to exclude the application of the Convention or derogate or vary any of its provisions should be unrestricted. A contrary view was that the Working Group should consider which provisions of the Convention should be mandatory. It was suggested that a better way to preserve mandatory form requirements might be by including appropriate exclusions in article 2 (relating to exclusions from the Convention). However, finalisation of the provision has been deferred pending full consideration by the Working Group of the other operative provisions of the draft Convention.

[12] Paragraph 2.1.

[13] Article 4 of the draft Convention. Report of Working Group IV (Electronic Commerce) on the work of its 41st session (A/CN.9/528), paragraphs 70-75.

2.2.4 The electronic transactions legislation of many other jurisdictions have adopted similar formulations.[14] In jurisdictions where a general requirement for consent to accept electronic communications has been adopted, they do not have any general variation provision in their legislation. These jurisdictions, however, have provisions for variation in respect of specific provisions and they use the words "except to the extent" or "unless" the parties "otherwise agree".[15]

2.2.5 We will consider in the following paragraphs:

(a) whether to rationalise the provisions on variation by agreement in sections in Part IV of the ETA that overlap with section 5 (paragraph 2.3);
(b) whether the application of section 5 to Part II of the ETA should be amended (paragraph 2.4); and
(c) whether section 5 should be replaced by specific provisions within the relevant sections allowing variation by agreement otherwise by the parties (paragraph 2.5).

2.3 Application of Section 5 to Part IV of ETA

2.3.1 Many of the provisions of Part IV[16] of the ETA expressly provide that they apply "unless otherwise agreed by the parties".[17] In other provisions it is implicit that the agreement of the parties prevails over the default provisions.[18] These repeated references to "unless otherwise agreed by the parties" are redundant in view of section 5. In fact, they may be a source of confusion rather than clarity vis-à-vis the status of provisions that are not similarly prefixed but which fall within Part IV.

2.3.2 **We propose to remove the redundancy between section 5 and the references to the right of parties to vary specific provisions in Part**

[14] Australian Commonwealth Electronic Transactions Act section 105, Illinois Electronic Commerce Security Act.
[15] Canadian Uniform Electronic Commerce Act s.29 (Formation and operation of contracts), s.23 (Time and place of sending and receipt of electronic documents); New Zealand Electronic Transactions Act s.9 (Default rules about Dispatch and Receipt of Electronic Communications).
[16] Part IV relates to formation and validity of contracts, validity of declaration of intent or other statements, attribution, acknowledgement of receipt and time and place of despatch and receipt.
[17] E.g. s.11(1) and 15(1) and (2).
[18] E.g. s.14(1) "where .. the originator has requested or has agreed", s.14(2) "where the originator has not agreed … that acknowledgment be given in a particular form".

IV. Since **all** provisions under Part IV ought to be able to be varied by agreement of the contracting parties, section 5 is adequate for this purpose. Alternatively, section 5 may be replaced by specific provisions within the relevant sections allowing variation by agreement otherwise by the parties. (See further discussion in paragraph 2.5.)

2.4 Application of Section 5 to Part II of ETA

2.4.1 Article 4 of the UNCITRAL Model Law on Electronic Commerce limits its application to chapter III of part one[19]. The Guide to Enactment[20] explains that the provisions contained in chapter II of part one (equivalent to Part II of the ETA) should be regarded as stating the minimum acceptable form requirements and are, for that reason, to be regarded as mandatory, unless expressly stated otherwise.

2.4.2 Unlike the UNCITRAL Model Law, section 5 of the ETA applies to the provisions of Part II[21] of the ETA. This allows parties to agree not to use electronic records to satisfy a rule of law[22] requiring writing,

[19] Equivalent to Part IV of the ETA.

[20] Guide to Enactment of UNCITRAL Model Law on Electronic Commerce (1996), paragraphs 44 and 45 of the Guide to Enactment.

> "44. The Model Law is … intended to support the principle of party autonomy. However, that principle is embodied only with respect to the provisions of the Model Law contained in chapter III of part one. The reason for such a limitation is that the provisions contained in chapter II of part one may, to some extent, be regarded as a collection of exceptions to well-established rules regarding the form of legal transactions. Such well-established rules are normally of a mandatory nature since they generally reflect decisions of public policy. An unqualified statement regarding the freedom of parties to derogate from the Model Law might thus be misinterpreted as allowing parties, through a derogation to the Model Law, to derogate from mandatory rules adopted for reasons of public policy. The provisions contained in chapter II of part one should be regarded as stating the minimum acceptable form requirement and are, for that reason, to be regarded as mandatory, unless expressly stated otherwise.
>
> 45. Article 4 is intended to apply not only in the context of relationships between originators and addressees of data messages but also in the context of relationships involving intermediaries. Thus, the provisions of chapter III of part one could be varied either by bilateral or multilateral agreements between the parties, or by system rules agreed to by the parties. However, the text expressly limits party autonomy to rights and obligations arising as between parties so as not to suggest any implication as to the rights and obligations of third parties."

[21] Part II relates to legal recognition of electronic records, requirement for writing, electronic signatures, and retention of electronic records.

[22] As to the phrase "rule of law" in the ETA, the provision is based on the UNCITRAL Model Law and the meaning intended in the Model Law is instructive. The Guide to Enactment of the UNCITRAL Model Law states that the words "the law" are to be understood as encompassing not

signature or retention of records. It also enables parties to agree to additional requirements for the use of electronic records. For example, section 6 of the Civil Law Act (Cap.43) imposes a requirement that certain contracts must be evidenced in writing. This is a mandatory statutory requirement intended to protect certain parties against fraud. The effect of Part II of the ETA is to allow electronic records, e.g. e-mail, to satisfy such a legal requirement for writing. A party may have legitimate reasons for refusing to accept electronic communications for this purpose or insist on additional safeguards in the use of electronic communications and should be free to agree with the other party accordingly.

2.4.3 **There appears to be no objection in allowing parties to agree not to use electronic records or to use electronic records subject to certain additional requirements.** Such "variation" of the provisions of Part II (which are intended to facilitate the use of electronic communications) does not derogate from the underlying rules of law (e.g. the requirement for writing, signature, etc) that are considered to be mandatory (under the principle expressed in relation to the UNCITRAL Model Law[23]). Similarly, agreeing to additional requirements in relation to the use of electronic communications does not derogate from the underlying rules of law.[24] The provision requiring consent to use electronic communications found in the draft Convention shows that it is not intended to force any person to accept electronic communications in contractual transactions.[25]

---

only statutory or regulatory law but also judicially-created law and other procedural law, including common law. However, "the law", as used in the Model Law, is not meant to include areas of law that have not become part of the law of a State and are sometimes, somewhat imprecisely, referred to by expressions such as "lex mercatoria" or "law merchant". The definition of "rule of law" in the ETA merely states that it includes written law, which in turn is defined in the Interpretation Act (Cap.1) to mean "the Constitution and all previous Constitutions having application to Singapore and all Acts, Ordinances and enactments by whatever name called and subsidiary legislation made thereunder for the time being in force in Singapore". In its ordinary meaning, the term would also include common law. (By contrast, the New Zealand and Australian electronic transactions legislation apply only to statutory enactments.)

[23] See footnote 20.

[24] The legal consequences would however differ. In the case of a rule of law, illegality may arise from failure to satisfy the rule of law and often the law will render a transaction void on account of such failure. Failure to comply with an agreement, depending on the context may prevent the formation of a binding contract (thus in effect rendering the transaction void) or result in a breach of contract (which may or may not be grounds for termination of the contract and may result in liability for damages). It would therefore be prudent for parties to agree also on the consequences of failure to comply with the additional requirements they seek to impose.

[25] Consent requirement is discussed in paragraph 2.1.

2.4.4 As it stands, however, section 5 appears even to allow parties to agree to less stringent or different requirements from those in Part II. For example, parties could agree to use an electronic record that is not "accessible so as to be usable for subsequent reference" in satisfaction of a requirement for writing. In effect, this would significantly undermine the safeguards that the rules of law requiring writing are intended to provide, whenever parties chose to use electronic records. **Parties should not be allowed to opt for requirements that fall below the standards set out in the provisions of Part II.** These should be regarded as mandatory minimum standards imposed on electronic records to make them functional equivalents of the forms required by the rules of law which they seek to satisfy.

2.4.5 **Similarly, it should also be made clear that section 5 does not allow parties to agree to derogate from express requirements relating to the use of electronic records provided under other laws.** Section 9(4) specifically provides that section 9 (which allows retention in the form of electronic records to satisfy legal requirements for retention of a document, etc) does not apply to any rule of law which expressly provides for the retention of documents in the form of electronic records or preclude the Government from specifying additional requirements for such retention. In such a case, it is envisaged that the requirements for retention of electronic records would have been exhaustively provided by that rule of law and any additional specifications by relevant public bodies. Thus, parties are not allowed to vary the requirements by agreement.

2.4.6 Some jurisdictions expressly exclude the possibility of contracting out of certain fundamental requirements in respect of criminal provisions, consumer transactions, obligations of good faith, reasonableness, diligence and care and the allocation of loss where less than commercially reasonable security procedures are used.

2.4.7 **We are of the view that variation of Part II of the ETA by agreement of the parties should continue to be possible, subject to the limitation that parties should not be permitted to agree to standards that are lower than the mandatory requirements for electronic communications provided in the ETA or in other rules of law.**

2.5 Replacement or Variation of Section 5

2.5.1 There has been feedback to IDA that the words "may be varied by agreement" in section 5 of the ETA may result in some ambiguity as to the applicability of the ETA provisions. It was suggested that section 5 should be reworded to the effect that the provisions of the ETA shall apply to the extent that they are not inconsistent with any relevant agreement. An alternative way of expressing the same concept is to say that the Act (or a section or other provision) applies subject to the agreement otherwise by the parties.

2.5.2 Although we do not think the suggested amendment to section 5 would not make any significant difference to the operation of the provision as the existing wording of section 5 already allows parties to agree to arrangements that differ from certain provisions of the ETA, **adopting the language of inconsistency[26] may have a conceptual advantage in that it avoids any suggestion that legislation may be varied by agreement of the parties or that the explicit agreement of the parties is required to vary the application of the provisions in Part IV.[27]**

2.5.3 In jurisdictions where a general requirement for consent to accept electronic communications has been adopted, the words "except to the extent" or "unless" the parties "otherwise agree" have been used in specific provisions.[28]

2.5.4 It may be preferable to replace section 5 by specific provisions within the relevant sections making the sections apply subject to the agreement otherwise of the parties. Such specific provisions would allow a more nuanced approach to the right of parties to agree to arrangements different from the default position provided by the ETA.

[26] i.e. that the provisions of the ETA shall apply to the extent that they are not inconsistent with any relevant agreement.
[27] The alternative formulation (i.e. that a provision applies subject to the agreement otherwise by the parties) may still imply a need for express agreement.
[28] See footnote 15.

Q2. Do you agree that parties should be able to agree:
(a) not to use electronic records to satisfy rules of law requiring writing, signature and retention of records;
(b) to requirements that are more stringent than those in Part II of the ETA? (See paragraph 2.4.3.)

Q3. Do you agree that parties should not be able to agree to standards that are lower than the mandatory requirements for electronic communications provided in the ETA or in other rules of law? (See paragraph 2.4.7.)

Q4. Should section 5 be replaced with specific provisions within the relevant sections making the provisions apply subject to agreement otherwise by the parties. (See paragraph 2.3.2 and 2.5.4.)?

Q5. If section 5 is retained, should it be amended to adopt the language of inconsistency[29] rather than making reference to a right to vary provisions of the ETA? (See paragraph 2.5.2)

2.5.5 It may be questioned whether, there is a need for both a general consent requirement and provisions for variation of the provisions of the ETA. The current draft of the UNCITRAL Convention on Electronic Contracting, as well as the legislation of many jurisdictions, contain both. This may be explained on the grounds that the consent provision relates to consent to the use of electronic communications. Without such consent, the provisions on variation do not come into play at all. Only if the party has consented to use or receive electronic communications will the issue of variation of the rules applicable to those communications become relevant.[30]

Q6. Should there be both a general consent provision and provision for variation ETA provisions by agreement of the parties (whether in section 5 or in specific provisions)?

[29] See footnote 26.

[30] The Report of Working Group IV on the work of its 41st session (paragraph 138) (A/CN. 9/528) notes that draft article 4 (on Party Autonomy) allowed parties to exclude the application of the convention as a whole or only to derogate from or vary the effect of any of its provisions. While an exclusion of the convention as a whole would normally require a specific reference to that effect, variations from its individual provisions could be effected without specific reference to the provisions being derogated from.

PART 3
RECOGNITION OF ELECTRONIC SIGNATURES

3 Recognition of Electronic Signatures

3.1 Section 8 of the ETA provides for electronic signatures to satisfy any rule of law that requires a signature, or provides for certain consequences if a document is not signed.

3.2 The UNCITRAL Model Law on Electronic Signatures and the draft Convention on Electronic Contracting provide similarly, but impose an additional reliability requirement. Article 9, paragraph 3, of the draft Convention provides as follows:

> "3. Where the law requires that a contract or other communications, declaration, demand, notice or request that the parties are required to make or choose to make in connection with a contract should be signed, or provides consequences for the absence of a signature, that requirement is met in relation to a data message if:
>
> Variant A
>
> (a) A method is used to identify that person and to indicate that person's approval of the information contained in the data message,[31] and
> (b) That method is as reliable as appropriate to the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
>
> Variant B[32]
>
> … an electronic signature is used which is as reliable as appropriate to the purpose for which the data message was generated or communicated in the light of all the circumstances, including any relevant agreement.

[31] The draft UNCITRAL Convention also defines "Electronic signature" in article 5 with reference to the same functions.
[32] Based on article 6, paragraph 3, of the UNCITRAL Model Law on Electronic Signatures.

4. An electronic signature is considered to be reliable for the purposes of satisfying the requirements referred to in paragraph 3 of this article if:

(a) The signature creation data are, within the context in which they are used, linked to the signatory and no other person;
(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
(d) Where the purpose of the legal requirement for a signature is to provide assurances as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

5. Paragraph 4 of this article does not limit the ability of any person:

(a) To establish in any other way, for the purposes of satisfying the requirement referred to in paragraph 3 of this article, the reliability of an electronic signature;
(b) To adduce evidence of the non-reliability of an electronic signature.".

3.3 **Function of electronic signature.** The requirement in paragraph 3(a) of Variant A is reflected in the definition of "electronic signature" in the ETA [33] which requires an electronic signature to be "executed or adopted with the intention of authenticating or approving the electronic record". Although there is no express reference to the identification function in the ETA definition, that function must be implicit in the use of an electronic signature.

3.4 In contrast, the Commonwealth Model Law on Electronic Transactions[34] merely states that the signature is "created or adopted

[33] "electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record (s.2 of the ETA).
[34] At the Commonwealth Law Minister's Meeting 2002, the Model Law was presented for consideration by Ministers as a basis for the passage of laws by member countries that seek to adopt

in order to sign a document".[35] The word "sign" was used to show that the legal effect of an electronic signature is the same as a handwritten signature.

3.5 Since a signature can perform a variety of functions depending on the nature of the document that was signed (as recognised in the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce[36]) it may be questioned whether the definition of "electronic signature" is too restrictive in its reference to the listed functions.[37] For example, sometimes a person may sign a document without any intention of approving the information contained therein, but merely to indicate that he has seen the document.

3.6 **Reliability requirement.** Both Variants of article 9 of the UNCITRAL Convention impose a requirement that the electronic signature used must be "as reliable as appropriate to the purpose for which the data message [being signed] was generated or communicated, in the light of the circumstances, including any relevant agreement". It establishes a flexible approach to the level of security required of the method of identification used. Variant B, in addition, goes on to list a set of criteria which will render an electronic signature sufficiently reliable i.e. if an electronic signature satisfies all those criteria, it will be considered to be reliable. Paragraph 5 of

---

legislation on the major issues covered by the UNCITRAL Model Law and adapted for the specific use of common law jurisdiction LMM 102/89. See http://www.thecommonwealth.org.

[35] The Canadian Uniform Electronic Commerce Act, which forms the basis of electronic transactions legislation recently enacted by various provinces in Canada, also adopts this wording.

[36] Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce, para.53.

[37] The Report of the Electronic Commerce Expert Group to the Attorney General, Australia (31 March 1998) on "Electronic Commerce: Building the Legal Framework" summarises 5 main functions of signature requirements as:

(a) evidentiary – to ensure the availability of admissible and reliable evidence e.g. Statute of Frauds.
(b) cautionary – to encourage deliberation and reflection before action, serving to draw attention that the transaction has significant legal consequences.
(c) reliance – to warrant veracity of contents of record or adoption by signer for purpose of protecting the recipient relying on those contents.
(d) channelling – to mark intent to act in a legally significant way.
(e) record-keeping – for execution of government regulations.

Apart from being used to identify a person and to provide certainty as to the personal involvement of that person in the act of signing or to associate that person with the content of a document, a signature might additionally or alternatively attest to the intent of a person to be bound by the content of a signed contract, to endorse authorship of a text, to associate himself with the content of a document written by someone else, or the fact that (and the time when) a person had been at a given place.

article 9 makes it clear that reliability may be established in any other way.

3.7 Section 8(2) of the ETA reflects the flexible approach in Variant A (as well as Variant B) and paragraph 5 of article 9 as it provides that an electronic signature may be proved in any manner. In addition, it provides that such proof includes showing a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the party.

3.8 The reliability criteria in Variant B resembles more closely the criteria for a secure electronic signature in section 17 of the ETA. Section 16 of the ETA provides criteria[38] for considering whether a security procedure is commercially reasonable. There is a rebuttable presumption in the case of a secure electronic signature that the signature is that of the person to whom it correlates and that it was affixed by that person with the intention of signing or approving the electronic record.

3.9 Despite the differences in formulation, the ETA seems largely consistent with the proposed draft UNCITRAL Convention as far as the provisions on recognition of electronic signatures are concerned.

Q7: Should the ETA be amended to adopt the provisions of article 9 of the draft UNCITRAL Convention on the recognition of electronic signatures?

Q8: Should section 8 of the ETA or the definition of "electronic signature" be amended in any way? If yes, please explain the problem addressed by the suggested amendments.

3.10 Further issues relating to the definition of electronic signatures and to digital signatures will be addressed in Stage III of the public consultation on Review of the ETA which will follow shortly.

[38] The criteria are non-exhaustive as s.16(2) uses the term "including".

PART 4

FORMATION OF CONTRACT: EFFECTIVENESS OF ELECTRONIC COMMUNICATIONS AND ATTRIBUTION

4.1 Formation and Validity of Contracts

4.1.1 Currently, it is unclear 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)[39] applies with regard to transactions concluded via electronic means. On one view, electronic communications (by analogy with telexes and telefaxes) should be considered as forms of instant communications and therefore actual receipt should be required. On the other hand, not all electronic transactions are instantaneous. Electronic records may be collated and transmitted in batches, saved in computer systems for retransmission or forwarded from computer system to computer system only when the recipient requests his electronic messages. In this case, the postal acceptance rule should arguably apply.[40]

4.1.2 It has therefore been suggested that the ETA should clarify which rule should prevail, with the possibility of statutory exceptions to achieve balance between the parties concerned.[41] For example, it may be statutorily provided that an offer and acceptance in the form of a data message become effective when they are received by the addressee. Earlier versions of the draft UNCITRAL Convention[42] contained such a provision, reflecting the essence of the rules of contract formation

---

[39] On the postal acceptance rule, see *Cheshire, Fifoot and Furmston's Law of Contract*, Second Singapore and Malaysian Edition, edited by Andrew Phang Boon Leong, p.117-120. The principle was stated in *Adams v Lindsell* (1818) 1 B & Ald 681, and confirmed in *Byrne v Van Tienhoven* (1880) 5 CPD 334 at 348. It was applied in Singapore as early as 1932: *Lee Seng Heng v Guardian Assurance Co. Ltd [*1932] SLR 110.

[40] *Reed, Computer Law* (3rd ed, 1996) pp 304-305.

[41] Andrew Phang & Yeo Tiong Min in *The Impact of Cyberspace on Contract Law*, The Impact of the Regulatory Framework on E-commerce in Singapore (Technology Law Development Group Symposium, Singapore Academy of Law, 5 Apr 2002) at p.43-45.

[42] A/CN.9/WG.IV/WP.103. article 13, paragraph 2. Variant A provided "When conveyed in the form of a data message, an offer and the acceptance of an offer become effective when they are received by the addressee". Variant B provided "Where the law of a Contracting State attaches consequences to the moment in which an offer or an acceptance of an offer reaches the offeror or the offeree, and a data message is used to convey such an offer or acceptance, the data message is deemed to reach the offeror or the offeree when it is received by the offeror or the offeree."

contained in the United Nations Sales Convention[43]. The provision was however deleted at the 42nd session of the UNCITRAL Working Group IV as it dealt with matters of substantive contract law which the draft Convention should not affect. [44] Such a provision would provide certainty on substantive contractual issues such as withdrawal, revocation or modification of an offer or acceptance.

4.1.3 The contrary view is that such a provision should not be adopted as it will create a duality of regimes for electronic and paper-based transactions. Furthermore, since some forms of electronic communications are instantaneous and some are not, it is doubtful whether a single rule should apply to all these differing situations.[45] There may also be complications in applying such a provision to transactions that involve both paper-based and electronic communications. No single rule of offer and acceptance is likely to provide a complete solution for electronic transactions as the circumstances of communication vary widely. Technology and practice in this area are still developing and convergence of technologies is likely to have a significant impact on the way electronic transactions are carried out.

4.1.4 **If there is to be a provision providing a default rule for the formation of electronic contracts,** parties should be allowed to opt-out of the default rule by agreement otherwise. **Alternatively, parties may be required to opt-in to such a regime if they decide to adopt it, instead of making it the default rule.** That way, parties will have a ready-made set of rules they may adopt if they wish to. A drawback of the latter approach is that those who are unaware of the provision are the least likely to have considered the need to provide for the situation and will be deprived of benefiting from the provision when they most need it.

[43] Article 15, paragraph 1 of the UN Sales Convention reads: "An offer becomes effective when it reaches the offeree." Article 18, paragraph 2 reads: "An acceptance of an offer becomes effective at the moment the indication of assent reaches the offeror…"

[44] Further article 13 may have created a duality of regimes. It was pointed out that article 13 was not required to facilitate a determination of the time of contract formation because article 8 already expressly recognized the possibility of offer and acceptance being communicated by means of data messages. A/CN.9/WG.IV/XLII/CRP.1/Add.7.

[45]See also Phang Khang Chau & Phua Wee Chuan, *Response To: "The Impact of Cyberspace on Contract Law"*, The Impact of the Regulatory Framework on E-commerce in Singapore (Technology Law Development Group Symposium, Singapore Academy of Law, 5 Apr 2002) at p.61.

Q9: Should the ETA provide when an offer and acceptance in electronic form takes effect? If yes, please suggest the terms of the necessary legislative provision to effect the change and comment whether the provision should apply only if the parties opt-in.

4.2 Invitation to make Offers

4.2.1 Article 12 of the draft UNCITRAL Convention on Electronic Contracting contains a provision to treat a proposal for concluding a contract making use of information systems that is not addressed to one or more specific persons to be treated as an invitation to make offers[46], unless it indicates the intention of the person making the proposal to be bound in case of acceptance. The Working Group noted that the provision, which was inspired by the United Nations Sales Convention, was intended to clarify an issue that had raised a considerable amount of discussion since the advent of the Internet. The proposed rule results from an analogy with offers made through more traditional means to the world at large.[47]

4.2.2 The underlying concern which the provision addresses is that a presumption of binding intention would be detrimental for sellers holding limited stocks of certain goods, if the seller were to be liable to fulfil all purchase orders received from a potentially unlimited number of buyers. The provisions would also be relevant in cases of on-line pricing errors.[48]

4.2.3 There is however a question whether the "invitation to treat" model is appropriate for transposition into the Internet environment and whether distinctions should be drawn between websites offering goods

[46] i.e. invitation to treat.

[47] See Report of Working Group on the work of its 41st session (A/CV.9/528) paragraphs 109-120, especially paragraph 110. At the 42nd session of Working Group IV, it was agreed to retain variant B as a basis for future discussion (A/CN.9/WG.IV/XLII/CRP.1/Add.6).

[48] Numerous cases of pricing errors by on-line suppliers have occurred. Few cases have been decided by courts since most such disputes are settled privately. The outcome of cases would presumably turn upon whether there was a binding contract at the time the supplier sought to withdraw from the transaction. This would often be determined by the actual terms of the communications involved in the specific transaction, the terms of any pricing policy and how effectively they are brought to the attention of the buyer (possibly raising the issues of incorporation discussed in paragraph 7.1) and whether it would be obvious to the buyer that the pricing error was a mistake. See article entitled *Are Sellers Bound by Mistakes in Online Advertisements?* (30 Jun 2003) by Henno Groell, Lyn Penfold and Jorge L. Contreras on www.haledorr.com which surveys the German and UK approach to on-line pricing errors.

or services using interactive applications[49] and those which do not. For example, some case law supports the view that "click-wrap" agreements and Internet auctions might be interpreted as immediately binding.

4.2.4 A question also arises whether there might be any difficulty, in the context of an electronic proposal, in indicating the intention to create a binding contract immediately upon receiving a response. Presumably an express statement to the effect should suffice. But would the use of the term "offer" to describe the proposal be sufficient indication of the intention to be bound? Indeed, it is already common practice to include a statement to the contrary (i.e. that the proposal is not intended to be binding) in electronic advertisements.[50]

4.2.5 A further objection to such a provision is that it sets out a separate regime for electronic contracts.

Q10: Should the ETA provide that proposals to enter a contract made by electronic means to the world at large are to be treated as an invitation to make offers, unless the proposal indicates that the person making the proposal intended to be bound in case of acceptance?

4.3 Effectiveness of Communications between Parties (Section 12 of ETA)

4.3.1 **Section 12 of the ETA** provides that a declaration of intent or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is an electronic record. It reflects article 8, paragraph 1, of the draft UNCITRAL Convention.[51] The draft Convention however refers to "a declaration, demand, notice or request that parties are required to make or may wish to make in

[49] The term "interactive applications" is intended to be an objective term describing a situation apparent to any person accessing the system i.e. that the exchange of information was prompted through a system by means of immediate actions and responses having an appearance of automaticity.

[50] Amazon.com, for example, provides a direct link to its pricing policy from the terms of use on its website. The policy explicitly states that the price of any item is not confirmed until the customer completes the order. In addition, Amazon indicates that items in the catalog may be mispriced and the price will be verified prior to shipment. If the correct price is higher, Amazon will, at its discretion, either contract the customer prior to shipment or cancel the order and notify the customer accordingly. See footnote 48.

[51] On electronic contracting. A/CN.9/WG.IV/XLII/CRP.1/Add.1.

connection with a contract". These provisions provide for the validity of both pre- and post-contractual communication made in electronic form.[52]

Q11: Should references to "declaration, demand, notice or request" be added to section 12 of the ETA for consistency with the UNCITRAL draft Convention?

4.4 Attribution (Section 13 of the ETA)

4.4.1 Section 13 of the ETA, in summary, deems an electronic record to be that of the originator even if it was not created personally by the originator if it was sent by (a) a person authorised to do so by the originator or (b) an information system programmed by or on behalf of the originator to send that electronic record. Further, section 13(3) enables an addressee to regard an electronic record received by him as coming from the originator if it was received according to a procedure agreed with the originator, even if the electronic record was sent by someone else. If the electronic record was sent by an unauthorised person, the addressee can still regard it as coming from the originator if that person was allowed by the originator to send the electronic record as if it was the originator who sent it.[53]

4.4.2 But the addressee is not entitled to presume that the message came from the originator from the point in time when the originator informed the addressee that the message is not his, and gives the addressee reasonable time to act, or when the addressee knows or ought to know that the message was not the originator's or if, in all the circumstances of the case, it is unconscionable for the addressee to regard the electronic record as that of the originator or to act on that assumption.[54]

[52] Section 11 of the ETA (and article 13 of the draft UNCITRAL Convention) make parallel provisions in the context of electronic records used in contract formation.

[53] Jeffrey Chan Wah Teck "Legal Issues in E-Commerce and Electronic Contracting: The Singapore Position", a workshop paper presented at the 8th ASEAN Law Association General Assembly 2003, available at www.sal.org.sg. See also article by Andrew Phang and Daniel Seng "*The Singapore Electronic Transactions Act 1998 and the Proposed Article 2B of the Uniform Commercial Code"* [1999] 7 International Journal of Law and Information Technology 103, at p.110.

[54] Section 13(4)

4.4.3 The rules are specifically designed to provide certainty to enable e-commerce to be relied upon as a tool for business. It attempts to balance issues of certainty and the allocation of risk. The position, simply stated, is that the party using a human agent or pre-programmed computer system assumes responsibility for their actions unless the other party knew or ought to know that the message is not the originator's (i.e. did not reflect the originator's intentions). The provision has been in the ETA since the enactment of the ETA and we are not aware that it has caused any practical difficulties.

4.4.4 Nevertheless, the provisions of the UNCITRAL Model Law[55], on which section 13 of the ETA is based, has from time to time been criticised either on the ground that they are redundant (i.e. they so obvious as to be tautological) or, worse still, contradictory to the existing domestic law rules in some jurisdictions.

4.4.5 Further, the provision was enacted before the advent of the Internet. In view of the wide range of business models now available for electronic commerce, e.g. IT outsourcing, where the contracting party may be different from the party that provides the information technology platform and "fronts" the transaction, it may be counterproductive to attempt to settle general rules of attribution. Indeed, in recognition of the complexity of attribution issues in the context of automated information systems, the draft UNCITRAL Convention on Electronic Contracting does not address the issue of attribution at all. The issue of attribution in relation to automated information systems is further discussed in **Part 6**.[56]

Q12: Should the attribution provision in section 13 be retained? If section 13 is retained, should it be amended in any way?
(See also amendments to section 13 discussed in paragraphs 4.4.6 to 4.4.9. below)

4.4.6 **Authority to program information system.** It is also noted that section 13(2)(a) refers to "a person who had authority to act on behalf of the originator", whereas section 13(2)(b) refers to an information system programmed "on behalf of the originator" without addressing the issue of authority. Arguably the requirement for authority is

[55] Article 13.
[56] Para. 6.4.

implicit in the reference to "on behalf". Nevertheless, consistent wording could be adopted in section 13(2)(b) to make it clear that the provision applies only if the information system was programmed by a person with authority to program the system on behalf of the originator.

4.4.7 On the other hand, it could be difficult for an addressee to determine whether an information system was programmed with the authority of the purported originator and it would not conduce to certainty if the addressee is required to determine this fact. It would be counterproductive and a hindrance to electronic commerce if the addressee had to check with the originator on the authority of the programmer for each transaction. Possibly the addressee should be able to rely upon the electronic communication as coming from the originator if it appeared to be the originator's and the addressee is not put on notice of any irregularity. Furthermore, such a provision requiring proof of authority of the programmer may create different regime for electronic contracts.

4.4.8 The lack of a definition of the term "information system" in the ETA is discussed in paragraph 5.13.

4.4.9 **Definition of originator.** The ETA does not contain any definition of "originator". The UNCITRAL draft Convention defines the term "originator" as "a person by whom, or on whose behalf, the data message purports to have been sent or generated … but does not include a person acting as an intermediary with respect to that data message". "Intermediary" has not however been defined by the draft UNCITRAL Convention. Adopting this definition of "originator" could help to avoid a circuitous reading of section 13.[57]

[57] Section 13(1) arguably begs the question as to who may be considered the originator of a particular electronic record.

PART 5
TIME AND PLACE OF DESPATCH AND RECEIPT (SECTION 15 OF THE ETA)

5.1 **Section 15** of the ETA provides for the **time** of despatch and receipt of an electronic record unless otherwise provided. An electronic record is ***despatched*** when it enters an information system outside the control of the originator or his agent.[58] As regards ***receipt*** of an electronic record, a number of separate rules apply. If an information system has been designated for receipt of the record, the electronic record is received when it enters the designated information system. If the electronic record was sent to another information system that was not designated by the addressee, receipt occurs when it is retrieved by the addressee.[59] If no information system was designated by the addressee, receipt occurs when the electronic record enters the information system of the addressee.[60]

5.2 The record is deemed to be despatched at the **place** of business of the originator and received at the addressee's place of business.[61] This recognises the unique environment of cyberspace where the information system is often located at a place different from the location of the parties. The place of receipt or despatch of an electronic record may be relevant in determining where a contract is deemed to have been concluded, and this in turn may be critical in deciding the applicable law. A number of rules are therefore provided to determine the place of business of the originator and the addressee.[62]

5.3 It has been noted at UNCITRAL that the different criteria for determining receipt of data messages[63] may lead to conflicting results.[64] For example, if "information system" covers systems that carry data messages to their addressees, e.g. an external server, a data message may be deemed to be received by an addressee even though it

[58] Section 15(1)
[59] Section 15(2)(a)
[60] Section 15(2)(b).
[61] Section 15(4).
[62] Section 15(5).
[63] Namely, entry into *a designated information system* as opposed to entry into *an information system of the addressee*.
[64] A/CN.9/WG.IV/XLII/CRP.1/Add.3, para.9.

is lost prior to retrieval, as long as the loss occurred after it had entered the server's system in the case of *entry into a designated information system*. If the addressee did not designate an information system, entry into the server's system may not be *entry into an information system of the addressee*.

5.4 Section 15 of the ETA is based on article 15 of the UNCITRAL Model Law on Electronic Commerce. The UNCITRAL Working Group on Electronic Commerce is currently considering modifications to a similar provision in **article 10 of the draft Convention** on Electronic Contracting in the following terms:[65]

"Article 10

1. The time of dispatch of a data message is deemed to be the time when the data message [enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator] [leaves an information system under the control of the originator], or, if the message had not [entered an information system outside the control of the originator or of the person who sent the data message on behalf of the originator] [left an information system under the control of the originator of the person who sent the data message on behalf of the originator], at the time when the message is received.

2. The time of receipt of a data message shall be deemed to be the time when it becomes capable of being retrieved by the addressee or by any other person named by the addressee. A data message is presumed to be capable of being retrieved by an addressee when it enters an information system of the addressee, unless it was unreasonable for the originator to have chosen that particular information system for sending the data message, having regard to the circumstances of the case and the content of the data message.".

5.5 These modifications replace the objective factual situations in the existing provision with general rules that focus on the control over the electronic message or the capability of retrieving the data message.

[65] See Report of Working Group IV paragraphs 132-151. A/CN/9/WG/IV/XLII/CRP.1/Add.3.

5.6 The two alternative formulations under consideration by the UNCITRAL Working Group in the case of **despatch**[66], namely when the message *left an information system under the originator's control* or when it *entered an information system* outside *the originator's control*, are actually different sides of the same coin. The former has the advantage of being more in line with the notion of despatch than the latter formulation. However, the latter formulation may be preferable because it focuses on an element that the parties would have more easily accessible evidence, since transmission protocols of data messages typically indicate the time of delivery of messages but do not state the time they leave their own systems.

5.7 In the case of **receipt**,[67] they focus on the moment when the message became capable of being retrieved.[68] This modification may however be criticised on the ground that they may lack the high level of predictability and certainty with respect to contract formation required by practical business concerns. The originator of a message would have no means of determining when a message that had entered an information system outside his own control was capable of being retrieved from that system. Parties would be unable to determine beforehand when their messages become effective. The existing provisions on receipt will safeguard the interests of the originator, whereas the modifications would leave the originator at the mercy of

[66] Article 10, paragraph 1 of the UNCITRAL Convention (See para.5.5.).
[67] Article 10, paragraph 2 of the UNCITRAL Convention (See para.5.5.).
[68] This is similar to the rule adopted in some jurisdictions in the absence of a designated information system. The message is deemed to be received when the addressee *became aware* of the data message and the message was *capable of being retrieved*. The Canadian Uniform Electronic Commerce Act provides a presumption that an electronic record is received only when the addressee becomes aware of the record *and* it is accessible by the recipient: UECA section 23(2)(b). The Australian Commonwealth Electronic Transactions Act and New Zealand Electronic Transactions Act provide that the time of receipt is the time when the electronic communication comes to the attention of the addressee. The Report of the Australian Electronic Commerce Expert Group to the Attorney-General on Electronic Commerce: Building the Legal Framework, paras 2.15.15 and 2.15.17, noted the need to address the issue of whether an electronic record is communicated only if it is actually read by the recipient.
Such a rule is more equitable than holding an addressee bound by a message sent to an information system that the addressee could not reasonably expect would be used in the context of its dealings with the originator or for the purpose for which the message was sent. On the other hand, it may be potentially unfair for the addressee unilaterally to have power to determine whether and when receipt would occur. The test is also inherently more uncertain since it will often depend on factors within the knowledge of the recipient or the ISP alone. It may also be difficult to obtain evidence from an ISP based outside the jurisdiction of the court. The test of entry into a particular information system is, on the other hand, technically easier to prove.

an addressee's willingness to become aware of a data message or the possible malfunctioning of the addressee's system.

5.8 The modifications also seem to abandon the notion of "designated information system". The possibility of designating a specific information system to receive certain information is of great practical importance, in particular for large corporations that may have multiple communication systems. It would be unreasonable to bind a large corporation just because a message was sent to one of its many electronic mailboxes and it had become *capable of being retrieved* by the corporation. Although the distinction between designated and non-designated systems may seem complicated, it serves a useful practical purpose since an addressee should not be bound by messages that were sent to an information system where the addressee did not expect to receive them.

5.9 The UNCITRAL Working Group however noted that the new proposal in fact reaches the same result as the existing provision, albeit through a different formulation. Linking the time of receipt to the capability of retrieving an electronic message is consistent with the normal principle that non-electronic contractual communications have to reach the addressee's sphere of control.[69] Further, the test of reasonableness[70] implicitly contemplates the possibility of designating a particular means of electronic communication. An addressee would be able to challenge the originator's choice to send a message to a particular address as unreasonable because it disregarded the addressee's designation of another system.

5.10 This proposal does not however state what criteria will be applicable in place of the "entry" criteria in case the message is unreasonably addressed. Would awareness of the message and the ability to retrieve suffice? Or is actual retrieval required? Presumably much would depend on the surrounding facts.

5.11 The UNCITRAL Working Group agreed to retain paragraph 3 (equivalent to section 15(3) of the ETA) which clarifies that receipt may occur even if the place of receipt did not coincide with the party's

[69] i.e. the actual receipt rule. See article 24 of the UN Convention on Contracts for the International Sale of Goods.
[70] See article 10, paragraph 2 in paragraph 5.4 above.

place of business and paragraph 5 (equivalent to section 15(5) of the ETA) which deems the originator's place of business to be the place of despatch and the addressee's place of business to be the place of receipt. This is important because, unlike postal communications, data messages are often deemed to be received when delivered to information systems outside the party's place of business.

5.12 **Parties using the same information system.** The UNCITRAL Working Group deleted paragraph 4 of the draft UNCITRAL Convention dealing with despatch and receipt where the originator and the addressee use the same information system on the basis that the issue would be considered in conjunction with paragraph 1. There is much academic debate on whether it can ever be said that two parties use the same information system. For example, even if two users are logged on to the same network (e.g. UNO wireless LAN), each party's information system is arguably designated by his unique IP address and is therefore arguably different from the other party's information system. Paragraph 4 provided that where the originator and the addressee use the same information system, both the despatch and the receipt occur when the data message becomes capable of being retrieved and processed by the addressee. The subjective criterion for despatch based on when the message becomes capable of being retrieved was proposed because the objective criteria based on the moment when the message "enters an information system" could not be used.

Q13: Would there be any other implications in adopting the provisions on time and place of despatch or receipt in article 10 of the draft UNCITRAL Convention? (See paragraphs 5.5 and 5.11)

5.13 Definition of Information System

5.13.1 The term "information system", used extensively in sections 13 (Attribution)[71] and 15 (Time and place of despatch and receipt) of the ETA, is not defined in the ETA. This was possibly because the drafters anticipated that this could be developed on the basis of future experience in a changing environment in line with the prescriptions as to the interpretation and application of the ETA in section 3 i.e. to

[71] Issues relating to Attribution are discussed in paragraph 4.4.

facilitate electronic commerce, eliminate barriers to electronic commerce, etc.[72]

5.13.2 Before the advent of the Internet, most information systems were owned and controlled by the user. Today, in the context of Internet and Internet Service Providers (ISP), an electronic record may have entered a person's mailbox held with the ISP, but the person may not be aware of it and may not be able to access it. For example, hotmail.com is hosted on a Microsoft server in the US. If the ISP server or the Internet is down, the user would be unable to access his email. Further it is usual for persons to have multiple email accounts which they may only check infrequently. A similar problem arises where data management has been outsourced.

5.13.3 Discussions at UNCITRAL highlight the point that the notion of "information system" is ambiguous in view of the range of information technology options now available and in use.[73] "Information system" is defined in the draft Convention to mean a system for generating, sending, receiving, storing or otherwise processing data messages. The term is intended to cover the entire range of technical means for generating, sending, receiving, storing or otherwise processing data messages and, depending on context, could include a communications network, an electronic mailbox or even a telecopier. However, it was pointed out that care should be taken to avoid confusion between information systems and information service providers or telecommunications carriers that might offer intermediary services or technical support infrastructure for the exchange of data messages. The UNCITRAL Working Group noted that the notion of "entry" into an information system referred to the moment when a data message became available for procession[sic] within an information system.

5.13.4 **Adopting the current definition of "information system" from the draft UNCITRAL Convention[74] would probably not serve any purpose for the ETA.** The existing flexible approach is probably

[72] Jeffrey Chan Wah Teck "Legal Issues in E-Commerce and Electronic Contracting: The Singapore Position" p.246, a workshop paper presented at the 8th ASEAN Law Association General Assembly 2003, available at www.sal.org.sg.
[73] Discussions of UNCITRAL Working Group at its 42nd Session on articles 10 and 12 of the draft Convention on Electronic Contracting in A/CN.9/wg.IV/XLII/CRP.1/Add.3 and Add.6.
[74] See para 5.13.3.

advisable in view of the unpredictability of future developments in technology. Specific provisions such as sections 13 and 15 that make reference to the term may however need to be clarified as appropriate. (Section 13 (Attribution) is discussed in paragraph 4.4 and section 15 (Time and Place of Despatch and Receipt) is considered in this Part).

Q14: Should the ETA adopt a definition of "information system" based on the draft UNCITRAL Convention whether generally, or in relation to any specific provisions?

5.13.5 The adoption of a definition of the term "automated information system" is considered in paragraph 6.2.

PART 6
AUTOMATED INFORMATION SYSTEMS

6.1 Definition of Automated Information System

6.1.1 The advent of the Internet has given rise to new modes of commercial dealing. In particular, it is now possible to conclude a web-based contract over the Internet. Typically, this involves an individual keying in the particulars of the transaction at a Website, for example, the details of his purchase. When the individual confirms his order, the computer software running the Website (variously referred to as an "automated information system", "electronic agent" or "bot"[75]) automatically generates a response based on the information provided (e.g. confirms fulfilment of the order). On a more sophisticated level, a company may program a bot (*A*) to present other e-business companies with different sets of acceptable pricing structures. *A* can connect on the Internet with another bot (*B*) which is programmed to accept one or more of those pricing structures. Following a series of on-line security checks, *A* and *B* will electronically conclude the deal without any human intervention. In many cases, such transactions will entail the formation of contracts.[76]

6.1.2 The draft UNCITRAL Convention on Electronic Contracting defines automated information system as:

> "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".[77]

---

[75] Short for robot.

[76] The analogy with electronic data exchanges (EDI) is limited because of vital distinctions e.g. EDI assumes a highly structured form of messaging, assumes an on-going relationship based usually on an 'interchange agreement' between parties, and is usually employed between substantial business concerns. See *"Internet Law and Regulation"* edited by Graham JH Smith, Second Edition, para 10.1.1. Web contracts on the other hand may consist of informal emails (though electronic agents are likely to utilise more structured fields), may involve random once-off purchases and may occur between individuals.

[77] Article 5(f). The Canadian Uniform Electronic Commerce Act and US E-Sign Act employ the term "electronic agent". The US E-Sign Act defines "electronic agent" to mean a computer program or an electronic or other automated means used independently to initiate an action or respond to

6.1.3 This definition, based on the definition of "electronic agent" in section 2(6) of the US Uniform Electronic Transactions Act, was included in view of article 14 of the draft Convention (discussed in paragraph 6.2). A similar definition is also used in the Canadian Uniform Electronic Commerce Act.

6.1.4 The term "automated information" is used in relation to the provision discussed below.

6.1.5 This definition of "automated information system" is able to stand by itself, without the need to adopt the definition of "information system" from the UNCITRAL Convention. See discussion of definition of "information system" in paragraph 5.13.

Q15: Should the ETA adopt the definition of "automated information system" from the draft UNCITRAL Convention? (see paragraph 6.1.2)

6.2 Contractual Intention

6.2.1 The law is unclear whether automated means of communication by automated information systems can convey the intention needed to form a contract where the communication has not been reviewed by a natural person before the contract was made. Upon one view, if a computer is programmed to make or accept offers in predetermined circumstances, the intention to create legal relations exists on the part of the user of the computer.[78] An analogy may be drawn with the use of vending machines. On the other hand, it is arguable that such intention relates to the computer system, and not specific transactions. Traditional contract doctrine looks at the intention of the parties surrounding the offer and acceptance of the specific agreement in dispute.[79]

electronic records or performances in whole or in part without renew or action by an individual at the time of the action or response. The Canadian Uniform Act defines "electronic agent" in similar terms.

[78] This is the view preferred by the New Zealand Law Commission in its Report 50 on "*Electronic Commerce Part One, A Guide for the Legal and Business Community*", October 1998, paras.56-58.

[79] David Castell "Electronic Contract Formation" Juris Diction. Article accessed at http://www.jurisdicion.com/ecom3.htm.

6.2.2 With automated information systems, it is necessary to distinguish between merely functional processes, e.g. acknowledgement of receipt, and contractual responses, e.g. offer and acceptance.[80] The more sophisticated the automated system, the more difficult would be the task of linking contractual intent to the person.[81]

6.2.3 In order to remove possible doubts concerning the validity of contracts resulting from the interaction of automated information systems, the UNCITRAL Working Group is considering article 14 in the draft UNCITRAL Convention which is cast as a principle of non-discrimination along the following lines:

> "14. A contract formed by the interaction of an automated information system and a person, or by the interaction of automated information systems, shall 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.".

6.2.4 A number of jurisdictions have enacted similar provisions in their electronic transactions legislation.[82]

6.2.5 We propose to include a similar provision in the ETA to make it explicit that contracts formed by the interaction of an automated information system and an individual or by the interaction of an automated information 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.

6.2.5 The general provision proposed above would not however address all issues related to the use of automated information systems, for example, issues relating to **conflicting contract terms**, **attribution** and **single keystroke error**. These issues are complicated and, given the varied situations they involve, it is unlikely that a simple statutory solution can be found. The resolution of such issues may be more

[80] In a US case *Corinthian Pharmaceutical Systems Inc. v Lederle Laboratories* (1989) 724 F.Supp 605 (S.D.Ind.) the court dealing with an automated order taking system held that the order tracking was a merely functional acknowledgement of the order, not an acceptance.

[81] David Castell "Electronic Contract Formation" Juris Diction. Article accessed at http://www.jurisdiction.com/ecom3.htm.

[82] US E-Sign Act, section 101(h) and Canadian Uniform Electronic Commerce Act, section 21.

appropriately dealt with by general law. We include a brief explanation of the issues below.

Q16: Should the ETA adopt a provision to clarify the validity of contracts resulting from the interaction of automated information systems from the draft UNCITRAL Convention? (see paragraph 6.2.3)

6.3 Conflicting Terms

6.3.1 While an automated information system can check for pre-programmed specifics, they may not be able to recognise non-standard terms.[83] If the automated information system nevertheless concludes the order, should the user be bound by the terms? The general provision like that in the draft UNCITRAL Convention would not resolve this issue.

Q17: Can you suggest any means of resolving the issue of conflicting terms in contracts concluded by automated information systems? (see paragraph 6.3.1)

6.4 Attribution

6.4.1 The attribution provisions in article 13 of the UNCITRAL Model Law (on which section 13[84] of the ETA is based) were not designed with the range of sophisticated automated information systems available now or in the future within contemplation. Finding an acceptable solution for the attribution of electronic communication in the varied circumstances of such transactions would pose great difficulty. Given these complications, an overwhelming majority at UNCITRAL felt that the draft Convention should not address this issue. The current draft Convention on Electronic Contracting does not therefore contain any attribution provision.

6.4.2 The ETA however already has an attribution provision in section 13, based on the UNCITRAL Model Law on Electronic Commerce. It is uncertain how the attribution provisions should apply to automated information systems.

[83] e.g. an exclusion from liability unless sued within 15 days instead of the usual period under the Limitation Act.
[84] See general discussion on Attribution and section 13 in paragraph 4.4.

6.4.3. A particularly difficult question arises in the case where an automated information system responds in a manner that was not intended by the sender, either because it was inadequately or wrongly programmed, or because of malfunction of the computer system or corruption of data or the operation of a computer virus. Should an electronic communication sent by an automated information system be attributed to a human sender in such circumstances?

6.4.4 In the case of human error in programming, the sender would probably have a right of action against the programmer. Unless what was communicated was so obviously wrong that the recipient must be aware of the mistake, the offeror would probably be bound by the resulting contract.[85] The failure by the offeror to require a verification procedure may suggest that he has assumed the risk of such mistakes.[86] The existing provisions on attribution in section 13 of the ETA are consistent with this. In attributing the act of the automated information system to the person using that agent, that person would be prevented from disavowing an intention to create legal relations.[87] The proper allocation of responsibility in the case of malfunction of the automated information system or corruption or virus is however more difficult to decide.

Q18: Should section 13 of the ETA apply to contracts concluded by automated information systems? Should provisions be made to attribute communications in any specific situations involving the use of automated information systems?

6.5 **Single Keystroke Error**

6.5.1 The ease with which transactions can be concluded over the Internet highlights the need for adequate safeguards. In computer communications, it is easy to hit a wrong key when typing quickly or to click the mouse on the wrong spot on a screen, and by doing so to send a command with legal consequences (the single keystroke error). To minimise such incidents, most websites require an individual to

[85] See *Cheshire, Fifoot and Furmston's Law of Contract – Second Singapore and Malaysian Edition* (1998) p.383ff generally on doctrine of mistake, bring it to there being a concluded contract rather than a mere invitation to make an offer (see paragraph 4.2 on Article 12 of the draft UNCITRAL Convention).
[86] New Zealand Law Commission in its Report 50 paras 59-60.
[87] New Zealand Law Commission in its Report 50 para 63.

confirm the particulars of a transaction before processing it. On the other hand, where the individual does not have an opportunity to prevent or correct a material error, it would seem unfair to hold him responsible for the legal consequences that may flow from a *bona fide* mistake.

6.5.2 Under the common law doctrine of mistake which applies under Singapore law,[88] a mistake is immaterial unless it is fundamental i.e. it results in a complete difference in substance between what the mistaken party bargained for and what the contract purports. It is likely that a court would allow the apparent contract to stand unless, on the facts, it must have been obvious to the other party that the person had made a mistake.

6.5.3 Article 16 of the draft UNCITRAL Convention on Electronic Contracting contains a provision on errors in electronic communications.[89] The provision requires a party offering goods or services through an automated information system to make available to parties that use the system some technical means allowing them to identify and correct errors.

6.5.4 Additionally, the UNCITRAL Working Group is considering a provision that deals with the legal effects of errors made by a natural person communicating with an automated information system.[90] The provision (inspired by Canadian legislation[91]) makes the contract unenforceable if the person made an error and:

(a) the system did not provide the person with an opportunity to prevent or correct the error;
(b) the person notifies the other person of the error as soon as practicable when he learns of it;
(c) the person takes reasonable steps to return the goods or services received or, if instructed to do so, to destroy them;

[88] See footnote 85.
[89] It was not considered at the 42nd session of the Working Group. Comments at earlier sessions therefore still stand.
[90] It had been suggested at the Working Group that the provision might not be appropriate in the context of commercial transactions (which the Convention is intended to govern). (A/CN.9/509, paragraphs 110 and 111)
[91] Section 22 of the Canadian Uniform Electronic Commerce Act.

(d) the person has not used or received any material benefit or value from the goods or services.

6.5.5 Such a provision would balance the need for certainty in commercial relationships and the need to protect consumers from unfair trade practices. It allows individuals to avoid an electronic transaction on the basis of mistake in narrowly defined circumstances[92]. The provision is intended to supplement the common law. The provision "gives online merchants a way of giving themselves a good deal of security against allegations of mistake, and encourages good business practices in everybody's interests".[93]

Q19. Should the ETA contain a provision requiring a party offering goods or services through an automated information system to make available to parties that use the system some technical means allowing them to identify and correct errors? (See paragraph 6.5.3)

Q20. Should the ETA provide for the legal effect of a "single keystroke error"? If yes, please suggest the terms of such a provision. (See paragraph 6.5.4).

[92] A common law defence of mistake exists under Singapore and Canadian law.
[93] Annotations to the Canadian Uniform Electronic Commerce Act.

PART 7
OTHER CONTRACT ISSUES

7.1 Incorporation by Reference

7.1.1 The UNCITRAL Model Law on Electronic Commerce, article 5 *bis*, adopted by the Commission in June 1998, provides as follows:

> "Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, *but is merely referred to in that message*. [Italics added]"

7.1.2 The establishment of standards for incorporating data messages by reference into other data messages is critical to the growth of a computer-based trade infrastructure. Without the legal certainty fostered by such standards, there might be a significant risk that the application of traditional tests for determining the enforceability of terms that seek to be incorporated by reference might be ineffective when applied to corresponding electronic commerce terms because of the differences between traditional and electronic commerce mechanisms. [94]

7.1.3 Incorporation by reference is often regarded as essential to widespread use of electronic communications in commerce. It follows that practitioners should not have imposed upon them an obligation to overload their electronic communications with quantities of free text when they can take advantage of extrinsic sources of information, such as databases, code lists or glossaries, by making use of abbreviations, codes and other references to such information.[95] Standards for incorporating data messages by reference into other data messages may also be essential to the use of public key certificates, because these certificates are generally brief records with rigidly prescribed contents that are finite in size.[96] While electronic commerce relies heavily on the mechanism of incorporation by reference, the accessibility of the full text of the information being

[94] UNCITRAL Model Law on Electronic Commerce, Guide to Enactment, para 46-4.
[95] UNCITRAL Model Law on Electronic Commerce, Guide to Enactment, para 46-2.
[96] UNCITRAL Model Law on Electronic Commerce, Guide to Enactment, para 46-3.

referred to may be considerably improved by the use of electronic communications e.g. by hypertext links to URLs. [97]

7.1.4 Article 5 *bis* seeks to facilitate incorporation by reference in an electronic context by removing the uncertainty prevailing in many jurisdictions as to whether the provisions dealing with traditional incorporation by reference are applicable to incorporation by reference in an electronic environment.[98] Article 5 *bis* is not to be interpreted as creating a specific legal regime for incorporation by reference in an electronic environment or introducing more restrictive requirements with respect to incorporation by reference in electronic commerce than might already apply in paper-based trade. Rather, by establishing a principle of non-discrimination, it is to be construed as making the domestic rules applicable to incorporation by reference in a paper-based environment equally applicable to incorporation by reference for the purposes of electronic commerce. [99]

7.1.5 Article 5 *bis* is not intended to interfere with consumer-protection or other national or international law of a mandatory nature, e.g. rules protecting weaker parties in the context of contracts of adhesion[100]. That result could be achieved by validating incorporation by reference in an electronic environment "to the extent permitted by law", or by listing the rules of law that remain unaffected by article 5 *bis*.[101]

7.1.6 As there does not seem to be any significant doubt that the general principles of law relating to incorporation by reference apply in the realm of electronic transactions, **we do not think that it is necessary to adopt a provision similar to Article 5 *bis* of the UNCITRAL Model Law.**

7.1.7 A more difficult question is whether it is necessary to clarify the way in which those principles apply to specific situations involving

[97] UNCITRAL Model Law on Electronic Commerce, Guide to Enactment, para 46-5.
[98] UNCITRAL Model Law on Electronic Commerce, Guide to Enactment, para 46-6.
[99] UNCITRAL Model Law on Electronic Commerce, Guide to Enactment, para 46-7.
[100] i.e. standard term contracts.
[101] For example, in a number of jurisdictions, existing rules of mandatory law only validate incorporation by reference provided that the following three conditions are met: (a) the reference clause should be inserted in the data message; (b) the document being referred to, e.g., general terms and conditions, should actually be known to the party against whom the reference document might be relied upon; and (c) the reference document should be accepted, in addition to being known, by that party." UNCITRAL Model Law on Electronic Commerce, Guide to Enactment, para 46-7.

electronic transactions. At common law, there are 3 main modes of incorporation, namely by *signature*, by *reasonable notice* or by a *consistent course of dealing*. The existing legal principles relating to incorporation by *course of dealing* would appear to apply to electronic transactions without much modification. There has been academic comment that the presence of Internet websites may result in at least slight alteration of the rules in relation to *reasonable notice*. This would depend upon whether or not consumers are more or less likely to read terms on Internet websites. As for incorporation by signature, it has been suggested that it would conduce to flexibility if legislation provided for alteration and verification of authenticity[102].[103]

7.1.8 As it would be a difficult, and most likely impossible, task to do so exhaustively given the lack of empirical information and the many possible variations in which the issue of incorporation may arise in the context of electronic transactions, **the principles applicable to incorporation by reference in the context of electronic communications should probably be left to be decided on particular fact situations by the courts.**

Q21: Should the ETA adopt a provision stating that incorporation by reference applies in electronic transactions? If yes, please specify the terms of such a proposal. (See paragraph 7.1.1 and 7.1.6).

Q22: Should the ETA elaborate specific rules as to whether there is incorporation in particular specified circumstances? If yes, please specify the terms of such a provision. (See paragraph 7.1.8)

7.2 Provision of Originals

7.2.1 The UNCITRAL Model Law on Electronic Commerce provides for the requirement for an original to be met by an electronic functional equivalent. The functional equivalent must satisfy the twin criteria of providing a reliable assurance as to the integrity of the information

[102] See Part 3 on Recognition of Electronic Signatures.

[103] Andrew Phang and Yeo Tiong Min, "The Impact of Cyberspace on Contract Law", in Seng Kiat Boon Daniel, ed, The Impact of the Regulatory Framework on E-Commerce in Singapore (Singapore Academy of Law, 2002) 39-58.

and having the capability of being displayed to the person to whom it is to be presented.[104]

7.2.2 Many countries have adopted provisions modelled on the UNCITRAL Model Law relating to the criteria by which the requirement for originals can be satisfied by electronic documents. They have generally adopted the twin criteria of reliable assurance of integrity (or accuracy) and accessibility.[105] "Integrity" means that the information has remained complete and unaltered, apart from any changes that arise in the normal course of communication, storage or display. The standard of reliability is to be assessed in relation to the document and in the light of all the circumstances. "Accessibility" covers both the usability of the record for subsequent reference and its capability of being retained by the person to whom the record is provided. This is an extension of the requirement in the UNCITRAL Model Law which merely provides that the information must be capable of being displayed to the person.[106] The Singapore ETA does not contain any provision on originals.

[104] Article 8 provides:
(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.
(3) For the purposes of subparagraph (a) of paragraph (1):

(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 which 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.

(4) The provisions of this article do not apply to the following: [...].

[105] Canadian Uniform Electronic Commerce Act s.11, Irish Electronic Commerce Act 2000 s.17, Hong Kong Electronic Transactions Ordinance s.7. See also the US E-Sign Act s.101(d)(1) and (3). Section 32 of the New Zealand Electronic Commerce Act which relates to the "legal requirement to compare a document with an original document" however only adopts the requirement of reasonable assurance of integrity. However section 28 of the New Zealand Act relating to the requirement to provide information or to produce information in paper form adopts those criteria and could apply to the provision of originals.

[106] Hong Kong adopted the UNCITRAL formulation i.e. capability of display.

7.2.3 A primary application of article 8 is in respect of documents of title and negotiable instruments and areas of law where special requirements exist with respect to registration or notarization of "writings", e.g., family matters or the sale of real estate. These areas have however been largely excluded from the ambit of the ETA.

7.2.4 Negotiable instruments and documents of title have been excluded from the ETA as the “unique document security concerns” relating to such documents would be better dealt with through a specific legislative and technological regime, rather than by a general provision. The Singapore Bills of Exchange Act has been amended to allow for the transmission of digitised images of cheques.[107] Provisions for electronic bills of lading may be made via regulations under the Bills of Lading Act.[108] However the lack of international consensus on the elements of an electronic bill of lading is a major obstacle to its adoption. Private contractual regimes such as the Bolero Project provide an alternative means of implementation. Similar concerns would probably apply to other types of documents of title such as delivery orders, store warrants and dock warrants. Exclusions from the ETA under section 4 will be addressed in Stage II of the public consultation on Review of the ETA.

7.2.5 Article 8 of the UNCITRAL Model Law however is also intended to apply to documents which (while not negotiable or used to transfer rights or title) need to be transmitted unchanged, that is in their "original" form, so that other parties in international commerce may have confidence in their contents. In a paper-based environment, these types of document are usually only accepted if they are "original" to lessen the chance that they may be altered, which would be difficult to detect in copies. Examples of documents that might require an "original" are trade documents such as weight certificates, agricultural certificates, quality or quantity certificates, inspection reports, insurance certificates, etc. Without this functional equivalent of originality, the sale of goods using electronic commerce would be hampered since the issuers of such documents would be required to retransmit their data message each and every time the goods are sold,

[107] (Cap.23).
[108] (Cap.384) s.1(5).

or the parties would be forced to use paper documents to supplement the electronic commerce transaction. [109]

7.2.6 In the case of requirements imposed by commercial practice, we are hesitant to override established commercial practice by legislation. It may be preferable to leave private parties to agree on the acceptability of electronic equivalents if they so desire.[110]

7.2.8 Since the primary areas requiring the production of originals have been or should be dealt with by specific provisions, there remains little room for the operation of a general provision on the use of originals. Requirements imposed by commercial practice do not pose an obstacle to electronic commerce since these requirements can usually be removed by agreement between the parties.

Q23: Should the ETA include a provision on electronic originals in the context of contractual transactions? If yes, what should be the criteria for the electronic functional equivalent?

7.3 Other Issues

7.3.1 Apart from the ETA, the main sources of contract law in Singapore are case law, the Sale of Goods Act[111], the Unfair Contract Terms Act[112] and the Vienna Sales Convention[113]. In addition, the Contracts (Rights of Third Parties) Act[114] and the Consumer Protection (Fair Trading) Act 2003[115] have a bearing on consumer transactions. Much of Singapore's statutory framework pre-dates both the Internet and the rise of the computer software industry[116]. Case law (which evolves

[109] UNCITRAL Model Law, Guide to Enactment.
[110] The operation of Article 8 is limited to requirements of law, which the Guide to Enactment clarifies does not include law merchant (see paragraph 8.13). Article 8 therefore probably does not apply to such requirements imposed by commercial practice.
[111] The Sale of Goods Act (Cap.393) provides for the terms under which goods are sold and includes many provisions intended to stipulate what terms apply in the absence of clear terms in a contract of sale.
[112] The Unfair Contract Terms Act (Cap.396) regulates exclusion clauses and limitation of liability clauses in most consumer and standard form contracts.
[113] The UN Convention on Contracts for the International Sale of Goods 1980, applicable in Singapore by virtue of the Sales of Goods (United Nations Conventions) Act (Cap.283A).
[114] (Cap.53B).
[115] Act No. 27 of 2003.
[116] Singapore's Sale of Goods Act (Cap.393) re-enacts the UK Sale of Goods Act 1979 (as amended in 1996) which is in turn a consolidation of the original Sale of Goods Act 1893. Singapore's Unfair

when courts decide novel issues by analogy to decided cases) generally has not caught up with the technology. To date, very few cases involving software contracts have reached the stage of court proceedings[117] locally or in the UK[118], possibly because excessive uncertainty as to the very basis upon which a court may decide inhibits litigation[119]. Consequently some of the most basic questions concerning the application of provisions of contractual and non-contractual liability in the information technology field admit of no easy or certain answer.[120]

7.3.2 **Meaning of "goods" in the Sale of Goods Act.** The local courts have yet to consider basic issues such as whether downloadable software and digitised products are "goods" within the meaning of our Sale of Goods Act. Even if digitised products are capable of being "goods", there is the related question of whether such products are "sold" if the intellectual property rights in the software remain with the original owner as is almost invariably the case (i.e. the end user is merely granted a licence to use the software).

7.3.3 **Shrink-wrap or click-wrap contracts.** Another question is whether shrink-wrap[121] and click-wrap agreements[122] are enforceable under

---

Contract Terms Act (Cap.396) re-enacts the UK Unfair Contract Terms Act 1977. Both UK Acts were received into Singapore law through the Application of English Law Act (Cap.7A). The Consumer Protection (Fair Trading) Act 2003 does not currently address electronic commerce issues specifically.

[117] With one exception, all of the cases which have reached the stage of High Court proceedings have concerned relatively high-value contracts for software which has either been developed under the terms of a specific contract for one or a small number of clients or which has been modified extensively to suit the needs of a particular customer. To date, there have been no cases concerned with the extent of liabilities that will apply to mass-produced or standard software packages such as word processing or spreadsheet programs.

[118] Guidance is often sought from UK case law in the absence of any local ruling on a point of law. As Singapore and UK share a common legal tradition, UK court decisions have persuasive value even though they do not bind our courts.

[119] See Ian J Lloyd, Information Technology Law – Third Edition, Reed Elsevier (UK) Ltd, 2000 at p. 495

[120] *Ibid*. E.g. issues relating to offer and acceptance, time of formation of contract, shrink-wrap and click-wrap contracts, etc . See discussions in New Zealand Law Commission in its Report 50 on *"Electronic Commerce Part One, A Guide for the Legal and Business Community"*, October 1998, Chapter 3;"*Internet Law and Regulation"* edited by Graham JH Smith, Second Edition, Chapter 10; "*Computer Law"*, Colin Tapper, Fourth edition, Chapter 5.

[121] A shrink-wrap contract is essentially a contract where the vendor offers to license the use of his product (e.g. computer software) on terms that accompany the product. The licensee is deemed to have agreed to these terms through the conduct of retaining the product and using it after being given a chance to read the terms.

Singapore law. Mass-market softwares are normally sold with software licences either prominently displayed on the packaging, with a term that specifies that they become effective when the transparent wrapping is torn by the customer, or may not even be accessible at all before the software packages are sold. In the case of software sold online, a term may specify that the customer accepts the terms displayed onscreen by further clicking his mouse on a button onscreen.

7.3.4 Various legal analyses have been sought to legitimize this commercial practice but there has yet been no authoritative judicial pronouncement on the validity of this practice. The most supportable approach treats the software licence as the producer's offer to the software user, which the user accepts by the conduct of breaking the shrinkwrap or using the software or, in the case of online distribution, clicking the mouse.

7.3.5 **Privity of contract.** The sale of computer software entails the purchaser acquiring rights to both medium as well as software. The transaction is complicated by the fact that the rights are acquired against different parties – the immediate seller supplies the medium but the developer of the software supplies the licence to use the software. The more important right is of course the licence to use functional and operative software, not the right to the medium as such. The doctrine of privity of contract may pose difficulties in allowing the purchaser to seek remedies from the immediate seller for defective software. Under the Contracts (Rights of Third Parties) Act 2001,[123] such rights can be conferred on the purchaser by an appropriately worded contract or if the contract purports to benefit a third party and there is nothing to rebut the presumption that that the parties intended to give the third party a right to enforce the contract. Parties are however free to contract out of the position under the Contracts (Rights of Third Parties) Act.[124] In contrast, the US does not recognise a substantive doctrine of privity of contract.

[122] A click-wrap contract is basically an on-line shrink-wrap contract. Typically, a person is required to intimate his acceptance of terms displayed onscreen by a mouse-click.
[123] (Cap.53B). It came into force on 1 Jan 2002.
[124] See Report on the Act (LRRD No.2/2001) available at http://www.agc.gov.sg.

7.3.6 **Standard terms**[125] **and consumer protection issues.** Software is typically marketed in a "mass-market" context (i.e. software developers do not individually negotiate terms with consumers). One result of this is that such contracts will therefore be on the standard terms of the distributor rather than arrived at by negotiation with the user. Because of limitation of space, the contract terms are likely to be in fine print or embedded deep in the Web-page. [126] This also raises consumer protection issues. [127]

7.3.7 **Viral contracts.** There is also the emerging issue of viral contracts whereby software is distributed on terms which are intended to follow the software down the chain of distribution. In usual contract practice, this is achieved by assignment. The situation is more complicated in relation to software distribution online because it may not be possible to assess the risks involved as there is no immediate knowledge of potential parties to the agreement. Open source products in particular attempt to implement a system of holding creations in common by means of a viral contract.

7.3.8 Some of these issues[128] are dealt with in a model law developed by the US National Conference of Commissioners on Uniform State Laws (NCCUSL) in the **Uniform Computer Information Transactions Act (UCITA).**[129] UCITA has however encountered growing opposition from major consumer and library groups, federal and state

[125] These are referred to as "adhesion contracts" in the US.

[126] See discussion on Incorporation by Reference in paragraph 7.1.

[127] The provisions on unfair practices in the Consumer Protection (Fair Trading Act) 2003 would apply also to electronic contracts e.g. fine print.

[128] E.g. the formation of online contracts, parol evidence rule, warranties, assignments, breach (including anticipatory breach), and remedies.

[129] US Uniform Law Commissioners, "A Few Facts about… Uniform Computer Information Transactions Act", 2000. The text of UCITA and related materials are available at http://www.ucitaonline.com.

The UCITA grew out of work on Art 2B of the Uniform Commercial Code (UCC), which was intended to complement Art 2 UCC.

The model law represents the world's first and only comprehensive uniform computer information licensing law. NCCUSL states that the legislation "uses the accepted and familiar principles of contract law, setting the rules for creating electronic contracts and the use of electronic signatures for contract adoption, thereby making computer information transactions as well-grounded in the law as traditional transactions". It is premised on the view that the rules for one paradigm (manufactured goods) yield uncertainty, complexity and risk of error when applied to another (computer information) thus adding unnecessary costs to transactions. The Introduction to the UCITA reports that a recent study in the European Union found that huge expenditures were made for the legal costs associated with uncertainty of transactional and other law in Internet transactions.

consumer protection officials, state attorney-generals and certain trade and professional groups, including the American Bar Association (ABA)[130], and is unlikely to see widespread adoption.[131]. It is reported that 3 states have adopted "bomb shelter" legislation to shield their state's residents from UCITA being applied to their contracts.[132]

Q24: Should any concepts of contract law (including those highlighted above) be clarified in relation to electronic transactions? If yes, please explain the problem faced, with reference to practical examples, and propose possible solutions.

[130] UCITA was substantially amended by NCCUSL in 2002 following a review of commentary received from all parties, including recommendations of the ABA. The NCCUSL had sought a resolution from ABA's governing body approving UCITA. However, as it became evident that a clear consensus on the model law was unlikely to appear, the resolution was withdrawn on the advice of a number of ABA leaders

[131] To date, the model Act has been enacted into law only in the states of Maryland and Virginia. It was reportedly under consideration for introduction in a number of additional states in the 2003 legislative session. As at Jul 2001, legislation based on the model law had been introduced (but has not been passed to date) in 14 other states: Arizona, Delaware, District of Columbia, Hawaii, Illinois, Iowa, Louisiana, Maine, New Hampshire, New Jersey, Oklahoma, Oregon, Texas and Washington. Information from Baker & McKenzie website http://www.bmck.com/ecommerce/ucitacomp.htm.

[132] Vermont, Iowa, West Virginia and North Carolina were reported to have enacted such laws, whilst Massachusettes was considering such a measure. Library Journal article dated 6.11.2003 at www.libraryjournal.com/article/CA30372.

ANNEX A

LIST OF QUESTIONS

Q1: Should the ETA include a consent provision similar to that in the draft UNCITRAL Convention, article 8, paragraph 2 (see para 2.1.1) in the context of all contractual transactions?

Q2. Do you agree that parties should be able to agree:

(a) not to use electronic records to satisfy rules of law requiring writing, signature and retention of records;
(b) to requirements that are more stringent than those in Part II of the ETA? (See paragraph 2.4.3.)

Q3. Do you agree that parties should not be able to agree to standards that are lower than the mandatory requirements for electronic communications provided in the ETA or in other rules of law? (See paragraph 2.4.7.)

Q4. Should section 5 be replaced with specific provisions within the relevant sections making the provisions apply subject to agreement otherwise by the parties? (See paragraph 2.3.2 and 2.5.4.)

Q5. If section 5 is retained, should it be amended to adopt the language of inconsistency[133] rather than making reference to a right to vary provisions of the ETA? (See paragraph 2.5.2)

Q6. Should there be both a general consent provision and provision for variation ETA provisions by agreement of the parties (whether in section 5 or in specific provisions)?

Q7: Should the ETA be amended to adopt the provisions of article 9 of the draft UNCITRAL Convention on the recognition of electronic signatures?

Q8: Should section 8 of the ETA or the definition of "electronic signature" be amended in any way? If yes, please explain the problem addressed by the suggested amendments.

[133] See footnote 26.

Q9: Should the ETA provide when an offer and acceptance in electronic form takes effect? If yes, please suggest the terms of the necessary legislative provision to effect the change and comment whether the provision should apply only if the parties opt-in.

Q10: Should the ETA provide that proposals to enter a contract made by electronic means to the world at large are to be treated as an invitation to make offers, unless the proposal indicates that the person making the proposal intended to be bound in case of acceptance?

Q11: Should references to "declaration, demand, notice or request" be added to section 12 of the ETA for consistency with the UNCITRAL draft Convention?

Q12: Should the attribution provision in section 13 be retained? If section 13 is retained, should it be amended in any way?
(See also amendments to section 13 discussed in paragraphs 4.4.6 to 4.4.9. below)

Q13: Would there be any other implications in adopting the provisions on time and place of despatch or receipt in article 10 of the draft UNCITRAL Convention? (See paragraphs 5.5 and 5.11)

Q14: Should the ETA adopt a definition of "information system" based on the draft UNCITRAL Convention whether generally, or in relation to any specific provisions?

Q15: Should the ETA adopt the definition of "automated information system" from the draft UNCITRAL Convention? (paragraph 6.1.2)

Q16: Should the ETA adopt a provision to clarify the validity of contracts resulting from the interaction of automated information systems from the draft UNCITRAL Convention? (see paragraph 6.2.3)

Q17: Can you suggest any means of resolving the issue of conflicting terms in contracts concluded by automated information systems? (see paragraph 6.3.1)

Q18: Should section 13 of the ETA apply to contracts concluded by automated information systems? Should provisions be made to attribute communications in any specific situations involving the use of automated information systems?

Q19. Should the ETA contain a provision requiring a party offering goods or services through an automated information system to make available to parties that use the system some technical means allowing them to identify and correct errors? (See paragraph 6.5.3)

Q20. Should the ETA provide for the legal effect of a "single keystroke error"? If yes, please suggest the terms of such a provision. (See paragraph 6.5.4).

Q21: Should the ETA adopt a provision stating that incorporation by reference applies in electronic transactions? If yes, please specify the terms of such a proposal. (See paragraph 7.1.1 and 7.1.6).

Q22: Should the ETA elaborate specific rules as to whether there is incorporation in particular specified circumstances? If yes, please specify the terms of such a provision. (See paragraph 7.1.8)

Q23: Should the ETA include a provision on electronic originals in the context of contractual transactions? If yes, what should be the criteria for the electronic functional equivalent?

Q24: Should any concepts of contract law (including those highlighted above) be clarified in relation to electronic transactions? If yes, please explain the problem faced, with reference to practical examples, and propose possible solutions.

ANNEX B

LEGISLATION REFERENCES

Singapore
Electronic Transactions Act (Cap.88) (1998)
http://www.ecitizen.gov.sg/

Australia
http://www.austlii.org/
Commonwealth Electronic Transactions Act 2000
New South Wales Electronic Transactions Act 2000
http://www.legislation.nsw.gov.au/
Electronic Transactions (Victoria) Act 2000
http://www.dms.dpc.vic.gov.sg/

Canada
Uniform Electronic Commerce Act
http://www.ulcc.ca/
British Columbia Electronic Transactions Act (2001)
http://www.qp.gov.bc/
New Brunswick Electronic Transactions Act (2001)
Consultation paper: *http://www.gov.nb.cp/justice/under.htm>.Paper*
Ontario Electronic Commerce Act 2000
Manitoba Electronic Commerce and Information Act 2000

Hong Kong
Electronic Transactions Ordinance (Cap.553)
http://www.justice.gov.hk/

Ireland
Electronic Commerce Act 2000
http://irlgov.ie/bills28/acts/2000/default.htm

New Zealand
Electronic Transactions Act 2002
http://www.legislation.govt.nz/

UK
Electronic Communications Act 2000
http://www.hmso.gov.uk/

US
Electronic Signatures in Global and National Commerce Act (E-SIGN Act) (2000)
http://www.access.gpo.gov/

UNCITRAL
http://www.uncitral.org/
Model Law on Electronic Signatures (2001)
Model Law on Electronic Commerce, with Guide to Enactment (1996) and article 6*bis* (1998)

Draft Convention on Electronic Contracting
draft used for discussion at 41st session of Working Group IV,
see A/CN.9/WG.IV/WP.103

EU
http://europa.eu.int/
Directive on Electronic Signatures (Directive 1999/93/EC)
eur-lex/eh/lif/dat/1999/en-399L0093.html
Directive on Electronic Commerce (Directive 2000/31/EC)
http://europa.eu.int/eur-lex/eh/lif/dat/2000/en-300L0031.html

The Commonwealth Secretariat
Model Law on Electronic Transactions
http://www.thecommonwealth.org

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE II: EXCLUSIONS UNDER SECTION 4 OF THE ETA

(Consultation Paper)

LRRD No. 2/2004

25 June 2004

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE II: EXCLUSIONS UNDER SECTION 4 OF THE ETA

The AGC (Law Reform and Revision Division) Team for this project comprises:

Mr Charles Lim Aeng Cheng	-	Principal Senior State Counsel
Mrs Joyce Chao	-	State Counsel

The following persons have rendered invaluable assistance to the team:

Mr Lawrence Tan	-	Senior Consultant, Infocomm Development Authority of Singapore

Legal Editorial and Publication

Ms Yvette Rodrigues	-	Senior Legal Executive, LRRD
Ms Regina Tan Shea Fang	-	Legal Executive, LRRD
Ms Noraini Bte Jantan	-	Corporate Support Officer, LRRD

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE II: EXCLUSIONS UNDER SECTION 4 OF THE ETA

CONTENTS

EXECUTIVE SUMMARY OF PUBLIC CONSULTATION ON REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE II: EXCLUSIONS UNDER SECTION 4 OF THE ETA

1 The Infocomm Development Authority of Singapore and the Attorney-General's Chambers are conducting a review of the Electronic Transactions Act (ETA) and the Electronic Transactions (Certification Authority) Regulations (CA Regulations). For this purpose, a public consultation is being carried out in 3 stages dealing with electronic contracting issues, exclusions from the ETA under section 4 and secure electronic signatures and certification authorities.

2 Stage I of the Public Consultation, which concerned **Electronic Contracting Issues**, was launched on 18 February 2004 and closed on 15 April 2004. The Consultation Paper on Electronic Contracting Issues (LRRD No.1/2004) is available on the AGC website (www.agc.gov.sg, under Publications) and the IDA website (www.ida.gov.sg, under Policy and Regulation, IDA Consultation Papers). Responses to the Consultation, available on the IDA website, are currently under consideration.

3 Stage II of the Public Consultation, concerning **Exclusions from the ETA under section 4**, is being conducted in consultation with the Ministry of Law. The ETA contains provisions clarifying that electronic records are the functional equivalent of paper records and providing that an electronic record or signature satisfies any rule of law requiring writing or a signature. Section 4 of the ETA however excludes those provisions from applying to any rule of law requiring writing or signature in certain kinds of transactions, namely:

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

4 The Consultation Paper reviews the rationale for these exclusions and developments affecting them, and seeks feedback whether any of these exclusions should be modified or deleted.

5 The issues are described in greater detail below:

Effect and Rationale of Section 4 (Part 2)

Section 4 prevents Parts II and IV of the ETA (containing provisions clarifying that electronic records are the functional equivalent of paper records) from applying to any rule of law requiring writing or signature in certain kinds of transactions. This Paper discusses, generally, the rationale for excluding those transactions. Views are sought whether any changes should be made to the exclusions under section 4.

Wills (Part 3)

No change to the exclusion of wills is proposed. The advantages of electronic wills are outweighed by the potential disadvantages.

Negotiable Instruments (Part 4)

No change to the exclusion of negotiable instruments is proposed. If provisions are to be made for electronic negotiable instruments, we propose that specific legislation may be made to address the complex issues raised and special safeguards required for the use of electronic negotiable instruments. Provisions on documents used in carriage of goods (including negotiable instruments) are however under consideration (see Part 9).

Indentures (Part 5)

The adequacy of electronic equivalents of writing, sealing, signing, attestation and delivery are discussed. It is tentatively proposed to adopt a provision to allow secure electronic signatures (or perhaps only secure digital signatures) to satisfy the requirement for the sealing of deeds.

Trusts (Part 6)

The declaration of trusts, with the exception of constructive and resulting trusts, is currently excluded. It is proposed to limit the exclusion to testamentary trusts and trusts relating to land.

Powers of Attorney (Part 7)

The advantages of electronic powers of attorney appear to be outweighed by their disadvantages. Nevertheless some jurisdictions limit their exclusion only to certain types of powers of attorney. Views are therefore sought on whether the exclusion of powers of attorney should be amended. It is proposed however that powers of attorney used in the transfer of land should continue to be excluded.

Transfers of Immovable Property (Part 8)

Comments are sought as to whether the scope of exclusion of land transactions should be restricted so as to allow certain classes of persons to enter electronic transactions relating to the transfer of land, or to allow certain kinds of land transactions to be effected by electronic contracts. The wider implementation of an e-conveyancing system goes beyond the scope of the current consultation.

Documents of Title (Part 9)

No change to the exclusion of documents of title is proposed. If provisions are to be made for electronic documents of title, we propose that specific legislation may be made to address the complex issues raised and special safeguards required for the use of electronic documents of title. Feedback is sought whether to adopt general provisions on documents used in carriage of goods (including documents of title and negotiable instruments) based on provisions in the UNCITRAL Model Law on Electronic Commerce.

Other Issues (Part 10)

Views are sought whether any other changes should be made to section 4. In particular, feedback is sought whether the ambit of any exclusions should be narrowed or whether any classes of persons should be exempted from any exclusions or whether any other transactions should be added to the existing exclusions. Further, we also seek comments whether clarification is necessary as to the application of the ETA to any transactions or specific legislation.

CONSULTATION PAPER

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE II: EXCLUSIONS FROM THE ETA UNDER SECTION 4

PART I INTRODUCTION

1.1 This Consultation Paper on **Exclusions from the ETA under section 4** forms Stage II of a Joint IDA-AGC[1] Public Consultation on the Review of the Electronic Transactions Act. Stage II of this Consultation is being conducted in consultation with the Ministry of Law. This Consultation Paper is intended to solicit the views of industry and business, professionals, the public and Government Ministries and agencies, in order to inform the Government in its review of the ETA.

1.2 With the enactment of the Electronic Transactions Act (Cap.88) in 1998, Singapore became the first country in the world to enact electronic transactions legislation based on the UNCITRAL Model Law on Electronic Commerce. Since then, numerous other countries have adopted electronic commerce legislation based on the UNCITRAL model.[2]

1.3 In view of these developments overseas and internationally, the Ministry of Information, Communications and the Arts (MITA), the Infocomm Development Authority of Singapore (IDA) and the Attorney-General's Chambers (AGC) are undertaking a joint review of the Electronic Transactions Act in 3 stages. Stage I of the Public Consultation concerning Electronic Contracting Issues was launched on 18 February 2004 and closed on 15 April 2004.[3] Stage III, which

---

1 Infocomm Development Authority of Singapore – Attorney-General's Chambers. Stage II of the Public Consultation is being conducted in consultation with the Ministry of Law.

2 See Annex A for list of recent legislation on electronic transactions and useful websites.

3 The Consultation Paper on Electronic Contracting Issues (LRRD No.1/2004) is available on the AGC website (www.agc.gov.sg, under Publications) and the IDA website (www.ida.gov.sg, under Policy and Regulation, IDA Consultation Papers). Responses to the Consultation, available on the IDA website, are currently under consideration.

will follow in the coming months, will deal with Secure Electronic Signatures, Certification Authorities and e-Government.

- Please send your feedback on this Consultation to the Law Reform and Revision Division of the Attorney-General's Chambers, marked **"Re: Exclusions from the ETA under section 4"**

  - via e-mail, at agc_lrrd@agc.gov.sg;
  - by post (a diskette containing a soft copy would be appreciated) to "**Law Reform and Revision Division, Attorney-General's Chambers, 1 Coleman Street, #05-04 The Adelphi, Singapore 179803**"; or
  - via fax, at **6332 4700.**

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

- The closing date for this Consultation is **25th August 2004**.

- A soft copy of the Consultation paper may be downloaded from http://www.ida.gov.sg/idaweb/pnr/index.jsp or http://www.agc.gov.sg (under Publications).

- In accordance with the standard practice of IDA, responses to this Consultation (including your name and your personal/company particulars) will be posted on the IDA website. Your response may also be quoted or referred to in subsequent publications or made available to third parties. Any part of the response which is considered confidential must be clearly marked and placed as an annex to the comments raised.

- If you need any clarifications, please contact:

  - **Mr Lawrence Tan** via e-mail at lawrence_tan@ida.gov.sg; or
  - **Mrs Joyce Chao** via e-mail at agc_lrrd@agc.gov.sg.

- The Consultation will be carried out in 3 stages. This Consultation on Exclusions from the ETA under Section 4 forms Stage II.

PART 2
EFFECT AND RATIONALE OF SECTION 4

2.1 Effect of Section 4

2.1.1 Parts II and IV of the ETA contain provisions clarifying that electronic records are the functional equivalent of paper records. In particular, sections 7 and 8 provide, respectively, that an electronic record or signature satisfies any rule of law requiring writing or a signature.

2.1.2 Section 4 of the ETA however excludes those provisions from applying to any rule of law requiring writing or signature in certain kinds of transactions, namely:

(a) the creation or execution of a will;

(b) negotiable instruments[4];

(c) the creation, performance or enforcement of an indenture[5], a declaration of trust or power of attorney[6], with the exception of constructive and resulting trusts;

(d) any contract for the sale or other disposition of immovable property[7], or any interest in such property;

---

4 A cheque, promissory note, bill of exchange, security or any document representing money payable which can be transferred to another by handing it over (delivery) and/or endorsing it (signing one's name on the back either with no instructions or directing it to another, such as "pay to the order of ABC").

5 An indenture is usually a deed made between two or more parties, and sealed by the parties e.g. a conveyance, lease, mortgage, settlement etc. Formerly it was usual to write the copies in duplicate (or triplicate, etc, as the case may be) on the same parchment or paper, and to divide it by cutting it through in a wavy line. The parts could then be fitted together to prove their genuineness. Afterwards only indenting was used, every deed to which there was more than one party being indented with a wavy line at the top.

6 A power of attorney is a formal instrument by which one person empowers another person to represent him or act in his place for certain purposes. It is usually executed in the form of a deed poll (i.e. a deed made by only one party) and attested by two witnesses.

7 i.e. land. Immovable property includes land, benefits that arise out of land and things attached to the earth or permanently fastened to anything attached to the earth: Interpretation Act (Cap.1) s.2.

(e) the conveyance of immovable property[8] for the transfer of any interest in immovable property; and

(f) documents of title[9].

2.1.3 The effect of section 4 is that, in such excluded transactions, one cannot rely on the provisions in the ETA that enable electronic records and signatures to satisfy legal requirements for writing and signature.[10] For example, sections 6 and 7 of the Civil Law Act[11] impose legal requirements for writing and signature in the case of certain land transactions and for trusts respectively.

2.1.4 **The exclusion does not however operate where there are no form requirements.** In such cases, there is no need to rely on the provisions of Part II or IV of the ETA to validate transactions. In most contractual situations, the law imposes no form requirements. A contract can generally be concluded by any means intimating an offer and acceptance. In recognition of this, the provision on formation and validity of contracts in section 11 of the ETA is couched in terms of an avoidance of doubt provision.

2.1.5 **Even where legal form requirements apply, exclusion under section 4 of the ETA may not necessarily prevent such transactions from being done electronically.** Electronic records or signatures could still possibly satisfy the legal requirements without reliance on the provisions of the ETA. It would be a matter for legal interpretation whether an electronic form satisfies a particular legal requirement for writing or signature. Some legislative provisions, by reason of their detailed specifications, would clearly exclude the use of electronic means even if the ETA were applicable. For example, the Wills Act arguably does not contemplate the creation or execution of

---

8 See footnote 7

9 This is a document used in the course of commerce as proof of the possession and control of goods and the transfer of which, by mercantile custom long recognized as law, gives the transferee, or enables the transferee to complete, the right of property in the goods described in and represented by the document of title e.g. bills of lading, delivery orders, store warrants and dock warrants, etc. (*Oxford Companion to Law*, David Walker, 1980)

10 In particular sections 7 and 8 of the ETA. Examples of legal requirements for writing and signature are found in sections 6 and 7 of the Civil Law Act. Also notices required under the Hire Purchase Act (Cap.125), and notice of general meeting under the Land Titles (Strata) Act (Cap.158).

11 Cap.43.

wills in electronic form because it refers to a will being signed at the foot or end thereof.[12] Similarly, the use of electronic forms would necessarily be excluded where legislation requires that certain records must be indicated in "ink" or issued "under the hand of" someone.[13] It is also generally accepted that because the Bills of Exchange Act includes a number of paper-based concepts, it requires bills of exchange to be in paper form.[14] Provisions that merely refer to the need for a record or notice without prescribing their form are however more likely to be interpreted to allow the use of electronic forms.

2.1.6 The UK Law Commission holds the view that the requirement for writing may (without the need for any enabling legislation) be satisfied by e-mail or web transactions, and that signature requirements can be satisfied by digital signatures, scanned manuscript signatures,[15] the typing of a name or initials, or even clicking on a web-site button, although they recognise that there is a lack of consensus on these issues.[16]

2.1.7 Such an approach gives rise to uncertainty as to whether electronic forms may be used in a particular case. Case law or commercial practice could possibly develop to put such issues beyond doubt, but these take time and tend to be limited to particular facts. The ETA provisions seek to avoid such uncertainties.

2.2 Rationale for the Exclusions

2.2.1 The original rationale for excluding these transactions was that e-commerce was at an infant stage and international developments in

[12] (Cap.352) s.6(2) Every will shall be signed at the foot or end thereof by the testator, or by some other person in his presence and by his direction, and the signature shall be made or acknowledged by the testator as the signature to his will or codicil in the presence of two or more witnesses present at the same time, and those witnesses shall subscribe the will in the presence of the testator, but no form of attestation shall be necessary.

[13] For example, Companies Act (Cap.50), s.40 (requiring alterations to be indicated in ink on copies of memorandum and articles issued to members); Road Traffic (Driving Instructors and Driving Schools) Rules, rule 15 (requiring driving instructors to make entries in their record in ink); Land Titles (Strata) Act (Cap.158), s.17 (requiring an instrument of proxy to be under the hand of the appointer).

[14] UK Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions* (December 2001), para.9.6, available at www.lawcom.gov.uk.

[15] This is not considered an electronic signature as it serves no authentication purpose.

[16] UK Law Commission, Electronic Commerce: Formal Requirements in Commercial Transactions (December 2001), Part 3, available at www.lawcom.gov.uk.

this area were still evolving. As such, it was felt that the provisions of the ETA should not go so far as to require recognition of all electronic signatures and electronic documents in place of physical forms[17]. With the significant advances in information technology (including technological controls against fraud) and rapid growth in its use, these exclusions need to be reconsidered.

2.2.2 Other more enduring reasons for exclusion are:

(a) the excluded transactions require more detailed rules, or more safeguards for their users, than can be established by a general purpose statute like the ETA;[18]

(b) the excluded transactions should be conducted through conventional means because of their solemnity, significance, or the need for certain formalities for execution, or the likelihood of technological obsolescence because such documents will be needed[19] for a long time in the future;[20] and

(c) it is considered that an appropriate level of technology and established process are not yet widely available to allow these transactions to be included, and that the public interest in the transactions is large enough to disallow people from taking the associated risks in the event of potential lapses[21].

2.2.3 Internationally, the following trends may be observed:

(a) the following transactions are almost **universally excluded**: wills, testamentary trusts, enduring powers of attorney and transfers of land generally;

---

17 Electronic Transactions Bill, Parliamentary Debates 1998, Column 254.

18 For example, electronic bills of lading, which are currently excluded under section 4 of the ETA. Singapore re-enacted the UK Carriage of Goods by Sea Act 1992 as the Bills of Lading Act, allowing for the authorisation of electronic bills of lading by regulation. No such regulations have been made in the UK or Singapore to date.

19 After a long passage of time, the technology with which the document was first created is likely to become obsolete and it may become difficult or impossible to access the document with new technology. To ensure continued accessibility of the old documents, it would be necessary to monitor changes in technology and to periodically invest time and expense to convert old documents to keep up with technology. Technology used to authenticate may also be no longer available or secure.

20 Wills are the classic example.

21 For example, high value transactions such as the conveyance of immovable property.

(b) the following transactions are **commonly excluded**: negotiable instruments, documents of title, and other powers of attorney and trusts; and

(c) most jurisdictions also provide for other specific exclusions such as affidavits and other sworn declarations, consumer protection notices, court proceedings, and specific Acts or provisions within an Act, usually relating to these areas.[22]

See the comparative table of excluded transactions at Annex B.

2.2.4 In contrast, the recent New Brunswick Electronic Transactions Act does not exclude any of the above areas.[23] The New Brunswick Department of Justice was of the view that exclusions were either superfluous or undesirable. Given that the Act does not force an electronic version of any document on anyone [24], they felt that nothing was really to be gained from 'excluding' them from the Act. Furthermore, inclusion or exclusion of a document in the Act does not itself mean that the document can or cannot be prepared electronically. All it means is that the particular rules set out in the Act do not apply.[25]

2.2.5 An additional point affecting the ambit of electronic transaction legislation is that some jurisdictions limit certain provisions of their Acts to listed legislation. In Singapore's ETA, the provisions relating to electronic records and signatures apply to the requirements of "a rule of law" (which includes both rules in written law and common law).[26] By contrast, similar provisions in the New Zealand ETA are

---

22 The Australian Electronic Transactions Regulations 2000 excludes listed legislation from certain provisions in the Electronic Transactions Act 1999. The listed legislation includes, amongst others, the Corporations Act 1989, Corporations Law, Cheques Act 1986, the Bills of Exchange Act, provisions relating to tax, insurance and banking.

23 Exclusion Regulation - Electronic Transactions Act (Regulation 2002-24) only excludes a small number of Acts.

24 Nothing in the Act requires anyone to use or to accept information in electronic form: section 6(1), which is common to the UECA.

25 New Brunswick Department of Justice, Law Reform Notes, Number 15, September 2001. Their Consultation Paper on the Electronic Transactions Act is available at http://www.gov.nb.ca/justice/index.htm.

26 The meaning intended in the UNCITRAL Model Law, on which the Singapore ETA is based, is instructive. The Guide to Enactment of the UNCITRAL Model Law states that the words "the law" are to be understood as encompassing not only statutory or regulatory law but also

restricted in their application to requirements in "enactments" and would therefore apply only to requirements imposed by statute.[27]

2.2.6 A final point to note is that the ambit of the express exclusions in legislation could also depend upon whether the legislation is framed broadly as electronic transaction legislation or whether it is restricted to electronic commerce. In the case of electronic commerce legislation, it would not be necessary to expressly exclude clearly non-commercial transactions, such as legal requirements as to wills, affidavits and the delivery of Government services, since these would already by definition be excluded. Nevertheless, in practice, those jurisdictions that restrict their legislation to electronic commerce have taken a cautious approach by expressly excluding even non-commercial transactions.[28]

---

judicially-created law and other procedural law, including common law. However, "the law", as used in the Model Law, is not meant to include areas of law that have not become part of the law of a State and are sometimes, somewhat imprecisely, referred to by expressions such as "lex mercatoria" or "law merchant". The definition of "rule of law" in the ETA merely states that it includes written law, which in turn is defined in the Interpretation Act (Cap.1) to mean "the Constitution and all previous Constitutions having application to Singapore and all Acts, Ordinances and enactments by whatever name called and subsidiary legislation made thereunder for the time being in force in Singapore". In its ordinary meaning, the term would also include common law.

[27] s.15(2) of New Zealand ETA. Ministry of Economic Development policy analyst Andrew McCallum, who played a dominant role in shepherding the legislation into being over four years, reportedly observed that the act applies a lot less broadly than many people think as it pertains only to statutory requirements in laws and regulations imposed by government agencies. Communications concerning private arrangements between businesses are still a matter for common law, which the act does not change. Likewise, the requirement for parties to give consent to receiving documents in electronic form only applies to statutory matters. In private dealings, parties may assume that electronic communications will be valid unless another party to the deal specifically says they are not. See http://www.itworldcanada.com.

[28] The US E-Sign Act restricts the definition of "transactions" to an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including (A) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods or intangibles, (ii) services, and (iii) any combination thereof; and (B) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.

The Uniform Law Commission of Canada, in its introduction to the Uniform Electronic Commerce Act (UECA), states that the UECA (despite its name) applies beyond the scope of "commerce" to almost any legal relationship that may require documentation.

The New Zealand Law Commission had originally restricted their recommended legislation to "trade" related transactions as it would avoid the need to list individually many such transactions which should be excluded from the application of the Act. The Government however finally decided to apply the Electronic Transactions Act to all transactions (including those relating to the delivery of Government services) unless specifically excluded by the Act.

2.3 Approach to Exclusions

2.3.1 The approach adopted in this Paper is to favour a wide application of the ETA provisions rendering electronic records the functional equivalent of paper records[29], in furtherance of the purpose enunciated in section 3(b) of the ETA: 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. Such functional equivalence provisions should, in principle, be allowed to apply unless there are overriding reasons why they should not apply in a particular context.

2.3.2 Legislation cannot keep up with the pace of technological change and therefore should not put obstacles in the way of the development and adoption of practical and commercially viable electronic means as they become available. The lack of an existing electronic means of effecting an electronic equivalent of a paper transaction under current technology should not, by itself, dictate that such a transaction must be excluded under section 4.

2.3.3 Continued exclusion under section 4 of the ETA may however be justified if there are overriding concerns of public policy, such as the continued need to protect the public or certain sectors of the public. Modern technology is complex and lack of understanding of technology may open the uninformed or the unwary to unexpected pitfalls in the use of technology.

2.3.4 The existing exclusions under section 4 are examined in turn in the following Parts of this Paper. In some cases, we propose that the existing exclusions should be narrowed to allow more electronic transactions to benefit from the functional equivalence provisions in the ETA.

(New Zealand Law Commission Report 68, *Electronic Commerce: Part Three – Remaining Issues*, December 2000, paragraph 9.)

[29] In Parts II and IV of the ETA.

PART 3
WILLS

3.1 **No change is proposed to the exclusion of wills in the ETA**. This category has been universally excluded in other jurisdictions, as well as the Commonwealth Model Law on Electronic Transactions[30]. The advantages of using electronic wills, as compared with paper wills, are small and they are counterbalanced by significant disadvantages.[31]

3.2 The Uniform Law Conference of Canada (ULCC) considered the issue of electronic wills.[32] The discussion paper noted that the formalities required for wills were intended to ensure that only authentic expressions of testators' intentions are recognised by law for the purposes of probate and to serve administrative efficiency. Electronic wills would offer no significant advantages in terms of convenience or cost of preparation, ease or security of storage, durability and accessibility.

3.3 It was highlighted that electronic wills are likely to be created by individuals i.e. non-business entities acting through computer systems which may not be secure. It would also be difficult to achieve an acceptable level of reliability with electronic wills because of lapse of time[33], the lack of current monitoring of authenticity[34], the lack of secure electronic equipment[35], and the lack of the testator's testimony[36].

3.4 In any case, it is likely that a will in electronic form will eventually have to be put in paper form, with some form of verification, to satisfy

---

30 Report of the Commonwealth Expert Working Group on Legal Aspects of Information Technology and the Related Law of Evidence (London 26-30 Jun, 2000). See comparative table of excluded transactions in Annex B.

31 Notably, it is still the practice to require CPF and insurance beneficiary nominations (which perform a similar function to a will) to be made on paper, with the signature of the person nominating.

32 Their discussion paper and resolutions at the 2001 Annual Meeting are available at http://www.ulcc.ca/en/poam2/

33 A will only takes effect after the death of the testator which, usually, occurs many years after the making of the will. There is a risk that the will may no longer be readable by that time due to technological obsolescence.

34 It may be impossible, without such current monitoring, to ascertain authenticity after the testator has died.

35 There is no certainty that the document has not been tampered with.

36 Because wills take effect only after the death of the testator.

third parties who are required to act in accordance with it. There are also uncertainties as to the meaning of 'original' in relation to an electronic will. Further, if the recognition of electronic wills would create a risk that a non-authentic record in a person's computer will be accepted as a person's will and hence supersede an earlier executed paper will, prudent and knowledgeable computer-owners would feel some compulsion to adopt security measures that would not otherwise have been necessary.

Q.1 Do you agree that electronic wills should continue to be excluded from the application of the ETA? If you think electronic wills should be recognised, please justify and suggest how they may work in practice.

3.5 **Dispensing power in Wills Act**. While the Uniform Law Commission of Canada decided to retain the exclusion of wills from the Uniform Electronic Commerce Act, they also resolved to prepare statutory provisions to amend the Uniform Wills Act to allow courts to recognise electronic wills in appropriate cases by giving them the power to dispense with strict compliance with formalities. The exclusion of wills under the ETA does not prevent other legislation, e.g. the Wills Act, from making provision for them.

3.6 The Canadian Uniform Wills Act s.19 gives a court power "notwithstanding a lack of compliance with all the formalities of execution" imposed by the Act, to declare effective a "document" which is "intended by a deceased to constitute a will" and which "embodies the testamentary intention of the deceased". In the Quebec case of *Rioux v Columbe* (1996) 19 ETR (2d) 201 (Que.S.C.), such a dispensing power was used to admit an electronic record to probate. The facts of the case were however highly exceptional in that the creation of the record was almost contemporaneous with the testator's death and she left directions in her own writing as to where the record was to be found.[37]

3.7 The Singapore Wills Act (Cap.352) does not contain a provision to dispense with compliance with formalities (except in the case of

[37] The testator committed suicide and a note beside her body gave directions to an envelope containing a computer disk marked "this is my will/Jacqueline de Rioux/(date)".

military personnel or seamen). The Singapore Wills Act[38] requires a will to be in writing and signed at the end by the testator in the presence of 2 witnesses who subscribe the will (i.e. sign at the bottom) in the testator's presence. The removal of the exclusion of the creation and execution of wills by section 4 by itself would not enable a will to be made electronically. The requirements for signing at the end of the page and for signing in the presence of 2 witnesses do not easily translate to the electronic medium.

3.8 It would appear that a provision allowing a court to dispense with formalities for a will would be exercised only in highly exceptional cases. Indeed it may not serve public policy to be seen to facilitate the making of a will in precipitous circumstances such as that in the case of *Rioux v Columbe*.

Q.2 Should the Wills Act be amended to facilitate the use of electronic wills in exceptional cases? If yes, please suggest what circumstances such a provision may be used in and the amendments that should be made.

[38] Cap. 352, section 6. Other provisions relate to signature to validate alterations etc (s.16) and writing to revoke a will (s.15).

PART 4
NEGOTIABLE INSTRUMENTS

4.1 A negotiable instrument includes a cheque, promissory note, bill of exchange, security or any document representing money payable which can be transferred to another by handing it over (delivery) and/or endorsing it (signing one's name on the back either with no instructions or directing it to another, such as "pay to the order of ABC"). In commercial practice, negotiable instruments provide a convenient method of transferring the right to payment from one person to another by delivery of a document, without the complexities of effecting an assignment of the right.

4.2 The Bills of Exchange Act[39] governs certain kinds of negotiable instruments, including cheques[40]. By its definition in the Act, a bill of exchange must be in writing and signed by the person giving it.[41] The exclusion of negotiable instruments by section 4 prevents reliance on Parts II and IV of the ETA to satisfy these requirements for writing and signature in order to use negotiable instruments in electronic form. Although it is possible to replicate the functions of a bill of exchange electronically by way of a series of promises to pay, they would not provide the protection afforded by the Bills of Exchange Act to bona fide purchasers for value.

4.3 Cheques are one of the most commonly used forms of bills of exchange. An **electronic cheque (or check) system** has been developed by the Financial Security Technology Consortium, a US banker's organisation. The Electronic Check reportedly performs the payment and other financial functions of paper checks, by using

---

39 Cap 23.

40 A cheque is defined as a bill of exchange drawn on a banker payable on demand.

41 A bill of exchange is defined as an unconditional order in writing, addressed by one person to another, signed by the person giving it, requiring the person to whom it is addressed to pay on demand or at a fixed or determinable future time a sum certain in money to, or to the order of, a specified person, or to bearer. It is generally accepted that because the Bills of Exchange Act includes a number of paper-based concepts, it requires bills of exchange to be in paper form. UK Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions* (December 2001), para.9.6, available at www.lawcom.gov.uk.

cryptographic signatures and secure messaging over the Internet,[42] and satisfies the legal requirements for negotiable instruments.[43]

4.4 Currently, there are no plans for an e-cheques initiative in Singapore.[44] In practice, most cheques are crossed and therefore not negotiable. The widespread availability of fund debit facilities at point of sale, such as NETS and Cashcard facilities, possibly satisfies most business and consumer requirements.

---

[42] Phase I involving payment by the US Treasury of Department of Defence contractors was successfully completed in 2000. Phase II involved trial participation by a broader range of participants. For legal and technical details of the electronic check project see "The Electronic Check Architecture" by Milton M. Anderson, available at http://fstc.org. Echecks provide for authorisation, instruction, and transaction (like paper checks) and additionally authentication. Every aspect of the payment transaction can be automatically processed by any party, independently. Echecks are signed using a smartcard and PIN to unlock the electronic checkbook. Payer signatures and endorsements are applied as digital signatures. Multiple signatures are supported and can be mandated in account restrictions. Signatures can optionally cover any attachments to the echeck, but attachments can be removed without invalidating the signature.

Confidentiality and security of transport are provided by other electronic security measures such as secure email and secure Web sessions. It allows duplicates but there is duplicate detection to ensure that the paying bank pays only once. It employs a 3-level certification authority hierarchy, with banks authoritative for checking accounts and a central bank or government agency authoritative as to which banks may operate.

[43] UCC Section 3-104. Form of Negotiable Instruments. "(1) Any writing to be a negotiable instrument within this article must (a) be signed by the maker or drawer; and (b) contain an unconditional promise or order to pay a sum certain in money and no other promise, … (c) be payable on demand or at a definite time; and (d) be payable to order or to bearer." The Federal Evidence Regulations R 1001(1) provides that writing includes electronic recording. UCC Section 1-201(39) provides that sign includes any symbol executed or adopted by a party with present intention to authenticate a writing.

These provisions are similar to the provisions of Singapore's Bills of Exchange Act (Cap.23), read with the definition of "sign" and section 7 (on the requirement for writing) in the ETA.

[44] The various initiatives introduced by NETS (Network for Electronic Transfers Pte Ltd) do not constitute negotiable instruments. In the US, a variety of electronic payment methods are also referred to as 'electronic checks'. However, these payment methods are not truly 'cheques' and do not constitute negotiable instruments. For example, electronic check conversion is a process in which a paper check is used as a source of information – for the check number, payer's account number and financial institution. The information is then used to make a one-time electronic payment from the payer's account – an electronic fund transfer. The service was developed to reduce the costs associated with accepting checks at the point of sale and to expedite the settlement of funds into the store's account through the use of the Automated Clearing House network. See glossary of terms is available at http://ecc.nacha.org. Information brochure on "Electronic Check Conversion" is available from the Board of Governors of the Federal Reserve System at http://www.federal reserve.gov/pubs/checkconv/checkconv.pdf.

4.5 The UK Law Commission noted in December 2001 that they were not aware of any demand to create an electronic equivalent of a bill of exchange with negotiable status. They pointed out that if such demand did arise, reform should be approached internationally so as to maintain uniformity of the laws on bills of exchange world-wide.[45]

4.6 **No change is proposed to the exclusion of negotiable instruments**. This category has commonly been excluded as negotiable instruments raise specific legal issues relating to transferability and negotiability.[46] These issues require special rules and special technology. In view of the complexity of these issues, we feel that **any provision for electronic negotiable instruments should be made by introducing new legislation or amending existing legislation[47], as necessary, in conjunction with the relevant agencies, rather than by removing the exclusion from the ETA**. For example, provisions have already been made for cheque truncation by amendments in the Bills of Exchange Act.[48]

Q.3	Do you agree that negotiable instruments should continue to be excluded from the application of the ETA?

4.7 However, please consider further the discussion in Part 9 on documents used in Carriage of Goods, which potentially include negotiable instruments.[49]

---

45 UK Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions* (December 2001), para.9.7, available at www.lawcom.gov.uk.

46 The Commonwealth Model Law on Electronic Transactions excludes negotiable instruments because of such "unique document" security concerns: Report of the Commonwealth Expert Working Group on Legal Aspects of Information Technology and the Related Law of Evidence (London 26-30 Jun, 2000). The New Zealand ETA also excludes it.

47 E.g. Bills of Exchange Act (Cap.23)

48 For the purpose of establishing a Cheque Truncation System, amendments were made to the Bills of Exchange Act in September 2002 to (a) provide banks an alternative means of presenting cheques by transmitting electronic images and payment information of the cheque, and (b) recognise the rights of holders of Image Return Documents (IRDs), which are documents that banks issue instead of returning the original cheque when a cheque is dishonoured.

49 Please see paragraph 9.8.

PART 5
INDENTURES

5.1 An indenture is a deed entered between 2 or more persons.[50] At common law, there is a legal requirement for deeds to be made on parchment (i.e. paper) and for the sealing of deeds. In practice, deeds are also almost always attested even though there is no legal requirement for it. Additionally, deeds are not regarded to be legally binding until they have been delivered to the other party.

5.2 Historically, the purpose of sealing was to provide authentication as to the identity of the maker of the deed. In the context of widespread illiteracy, a seal provided a substitute for a signature.[51] The process of affixing a seal also serves to add solemnity to the occasion to underline the legally binding nature of the transaction. This is of particular significance since deeds provide an exception to the doctrine of consideration.[52]

5.3 In England, the requirement for parchment has been abolished. The requirement for sealing in the case of individuals has been replaced by a requirement for the signature of the person executing the deed and the attestation of 2 witnesses. In the case of companies, a common seal is no longer required and a deed may be executed by the signature of certain officers of the company. Similar amendments are being considered in Singapore to abolish the requirements for parchment and sealing of deeds under a proposed Instruments (Formalities) Bill.[53]

---

50 See footnote 5.

51 White Paper on "Electronic Signatures: Understand the Past to Develop the Future" by McCullagh, Little and Caelli, especially pages 13-15. Available at http://spyrus.com/content/information_resource_center/white_papers/Electronic_Signatures.pdf.

52 The rule of law which requires that in order to have a legally binding agreement, a benefit must have been conferred on the promisor. The Contracts (Rights of Third Parties) Act (Cap. 53B) enables parties to an agreement to confer benefits on third parties but it does not affect the need for consideration as between the parties to the agreement. See LRRD Report on the Contracts (Rights of Third Parties) Act (LRRD No 2/2001) available at http://www.agc.gov.sg.

53 See LRRD Report No.1/2001 (Revised w.e.f. 1st October 2001) on "The Instruments (Formalities) Bill 2001" available at http://www.agc.gov.sg. These amendments are based on provisions in the UK Law of Property (Miscellaneous Provisions) Act 1989 and the draft Instruments (Formalities) Bill (proposed by the UK Law Commission in their Report No.253 on "The Execution of Deeds and Documents By or On Behalf of Bodies Corporate"). Further amendments to the proposed Bill are being considered and a Supplementary Report will be published at a later date.

5.4 The requirements of signing and sealing, attestation (i.e. witnessing) and delivery are considered in more detail in the following paragraphs. Some jurisdictions now have legislative provisions allowing for electronic equivalents of sealing and attestation.

Q.4 Should the creation, performance or enforcement of an indenture continue to be excluded from the application of the ETA?

5.5 Signature or Seal

5.5.1 Signing or sealing may serve many purposes, for example, to provide evidence of the identity of the signor, that the signor agreed to be bound by the agreement and that he did so voluntarily, that the document is final and complete, or that the information has not been altered after signing.[54] They may also caution the signor and indicate the intent to act in a legally binding manner.

5.5.2 The ancient seal may in modern times be replicated by the private key value that will be used to digitally sign an electronic document.[55] In the context of electronic transactions, secure electronic signatures can provide the necessary assurance of reliability. The application of secure digital signatures (i.e. electronic signatures based on PKI infrastructure) would ensure authenticity of the signature, assurance of the identity of the signor and integrity of the document.

5.5.3 There are specific provisions for secure electronic signatures, with appropriate certification, to be used in place of a seal in Ireland.[56] The Canadian Department of Justice recommended that global rules should contain a provision that any requirement for a personal seal be satisfied if the document is signed using a secure electronic signature.[57]

---

[54] See Sneddon "Legislating to Facilitate Electronic Signatures and Records: Exceptions, Standards and the Impact of the Statute Book" (especially Part 2.II on "Policy Objectives of Writing and Signature Requirements) University of NSW Law Journal available at http:/law.unsw.edu.au/publications/journals/unswlj/index.html.

[55] *Ibid*, p.14.

[56] Irish Electronic Commerce Act 2000, section 16.

[57] Consultation Paper on Facilitating Electronic Commerce: Statutes, Signatures and Evidence, Canadian Ministry of Justice, available at http://canada.justice.gc.ca/n/cons/facilt7.html.

5.5.4 Notably, the e-Conveyancing[58] initiatives in a number of countries also contemplate the use of electronic documents and signatures in land transactions involving deeds. The UK model envisages execution of deeds by solicitors on behalf of their clients via an Intranet. The Victorian model envisages the use of secure digital signature technology via Internet with digital cards issued by a Certification Authority.

5.5.5 **We tentatively propose to adopt a provision in the ETA to allow secure electronic signatures (or perhaps only secure digital signatures[59]) to satisfy the requirement for sealing of deeds.** Contracts (including indentures) for the sale or disposition or conveyance or transfer of immovable property are discussed separately in Part 8.

Q.5 Should Singapore adopt a provision in the ETA to allow secure electronic signatures (or only secure digital signatures) to satisfy the requirement for sealing?

Q.6 If you answered yes to Q.5, should any class of transactions be excluded from the provision allowing electronic signatures (or secure digital signatures) to satisfy the requirement for sealing e.g. land transactions?[60]

5.6 Attestation

5.6.1 The purpose of attestation is to preserve evidence of the signing. The witness, if cross-examined on the circumstances surrounding the signing, can give such knowledge as is within his knowledge.[61]

5.6.2 It has been argued that traditional witnessing processes are not wholly adaptable to the process of electronically signing documents. There is no assurance that the image on the screen is in fact the document to which the electronic signature will be affixed. All that the witness and the signor can see is a human readable representation on the computer

[58] See paragraph 8.9 on e-conveyancing.

[59] Secure digital signature is defined in s.20 of the ETA. The term "digital signature" is defined in relation to PKI (public key infrastructure) technology.

[60] On land transactions, see Part 8.

[61] White Paper on "Electronic Signatures: Understand the Past to Develop the Future", especially pages 15-18. See footnote 51.

screen of what is allegedly in memory. When the witness sees the signor pressing the keyboard, the witness will not know with certainty what is actually happening. It would be possible to ensure that the screen display corresponds to the contents of the computer memory and that the signor's keystrokes correspond to his intentions only if the computer has been evaluated to effect a trusted path by trusted evaluation criteria. It has been suggested that the witness would have to verify that the document has been electronically signed by first using the signor's public key to verify the initial signing and then also to electronically sign the document himself. The software which affixes the witness' signature must both note the witness as an attester and not as the primary signor and affix his signature in a manner that embodies the whole document including the signature of the signor. [62]

5.6.3 A Certification Authority would be able to perform a similar function to the attesting witness by certifying that the private key belongs to the person purporting to sign the deed. If the signor uses a secure digital signature without an attesting witness, it would still be possible to verify the authenticity of the signature, the identity of the person to whom the signature belongs, the integrity of the document, and probably even the date and time of signing. In this sense, a secure digital signature is superior to an ordinary hand-written signature. The advantages of having, in addition, an actual witness to attest a secure digital signature would probably be minimal unless, exceptionally, the voluntariness of the signing was in question.[63]

5.6.4 The New Zealand ETA provides that a legal requirement for a signature or seal to be witnessed is met by the *witness'* electronic signature, without specifying the technology to be used.[64]

---

62 *Ibid*, p.18

63 See views in the context of land transactions in Part 8, para. 8.3(b).

64 NZ Electronic Transactions Bill, section 23.
"23.(1) Subject to subsection (2), a legal requirement for a signature or seal to be witnessed is met by means of a witness' electronic signature if, -
(a) in the case of the witnessing of a signature, the signature to be witnessed is an electronic signature that complies with section 22; and
(b) in the case of the witnessing of a signature or a seal, the electronic signature of the witness –
(i) adequately identifies the witness and adequately indicates that the signature or seal has been witnessed; and
(ii) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the witness' signature is required.

5.6.5 In the context of e-conveyancing, the majority of respondents in a consultation by the UK Lord Chancellor's Department were of the view that attestation was inappropriate for electronic conveyancing documents because authorisation or certification takes the place of attestation.[65]

Q.7 Should the ETA enable a secure electronic signature (or secure digital signature) to satisfy the attestation requirement, i.e. signing of a document by its maker using such a signature need not be witnessed by another person?[66]

Q.8 Should the ETA provide that a legal requirement for a signature or seal to be witnessed is met by the *witness'* electronic signature?[67]

Q.9 If you answered yes to Q.7 or 13, should any class of transactions be excluded from the provision e.g. land transactions?[68]

5.7 Delivery

5.7.1 Additionally, a deed is not binding on the signatory until it has been delivered. However, the deed need not be physically delivered provided that the intention of the party to be bound by the obligations in the deed can be established. It has been suggested that since delivery is a question of fact to be determined in the circumstances of each case, the same should apply to electronic deeds.[69]

5.7.2 In the context of e-conveyancing, most respondents to the UK Lord Chancellor's consultation preferred that electronic deeds should take effect on the date and at the time specified by the parties since traditional concepts of delivery do not translate well to the Internet.[70] Some respondents however felt that clarifications were needed in

(2) A legal requirement for a signature or seal to be witnessed, if that signature or seal relates to information legally required to be given to a person, is met by means of a witness' electronic signature only if that person consents to receiving the witness' electronic signature."

65 See paragraph 8.9.3(b).

66 See discussion in paragraphs 5.6.1 and 5.6.3.

67 E.g. NZ Electronic Transactions Act, see footnote 64.

68 On land transactions, see Part 8.

69 White Paper on "Electronic Signatures: Understand the Past to Develop the Future", p.14-15. See footnote 51.

70 See Part 8.

relation to withdrawal from a transaction and alteration of the effective date or time of an electronic deed or of a minor term therein.

Q.10 When should an electronic indenture take effect?

Q.11 What should be the requirements for withdrawal from or amendment of an electronic indenture?

PART 6
TRUSTS

6.1 **We are of the view that the declaration of testamentary trusts should continue to be excluded under section 4.** This is for consistency with the position on wills since testamentary trusts must comply with the requirements of the Wills Act.[71] As discussed in Part 3, the advantages of allowing testamentary instruments to be created electronically are few compared to the possible pitfalls of doing so.

6.2 We recognise however that the same objections may not apply to other kinds of trust. Laws governing the formation of trusts contain few or no requirements for paper, writing or signatures. Constructive and resulting trusts are already excepted from the exclusion under section 4. A resulting trust in favour of the settlor is created automatically when an express trust fails. Where the courts impose a trust on parties, e.g. to prevent fraud, there is a constructive trust.[72] Trusts may also be implied. Implied trusts should probably be similarly excepted from section 4.

6.3 **Trusts of land** may however require special consideration.[73] There can be an express, implied, resulting or constructive trust of land. An express trust may be created either by (1) transferring legal title to a third person as a trustee or (2) the owner simply declaring himself a trustee for the beneficiary.

6.4 The transfer of legal title to land to a third person as trustee would have to be done in the appropriate manner i.e. by deed in English for unregistered land[74] or by registered transfer under the Land Titles

---

71 (Cap.66). See Part 3 on Wills.

72 E.g. the doctrine in *Rochefoucauld v Boustead [1897] 1 Ch 196, that the Statute of Frauds cannot be used as "engine of fraud"*.

73 See generally Tan Sook Yee *"Principles of Singapore Land Law"*, 2nd edition, 2001, Butterworths, Chapter 7 on Trusts. The pre-1826 law of strict settlement of land, being common law, is part of the law of Singapore. The Singapore Settled Estates Act (Cap.293) governs transactions involving settled estates, defined as "all immovable property … which are subject to a settlement" and "settlement" is defined as "any statute, deed, agreement, will or other instrument … under which any immovable property stands limited to or in trust for any person or persons by way of succession." The Act enables the Court, in certain limited circumstances, to order sale of settled land.

74 Conveyancing and Law of Property Act (Cap.61) s.53

Act[75] for registered land. Such transfers would fall within the exclusion of transfers of immovable property discussed in Part 8.

6.5 Where the owner declares himself a trustee, the trust must be evidenced in writing or it would be unenforceable.[76] Nevertheless, where a trust is not evidenced in writing, the courts will allow parol evidence of the trust to be admitted so that the statute cannot be used as "an engine of fraud".[77] Therefore, even if land transactions via electronic records continue to be excluded under section 4, the court could in appropriate cases uphold the declaration of trust on the basis of evidence provided by the electronic record.

6.6 The requirement for writing and signature for a declaration of trust respecting immovable property or any interest in such property under section 7(1) of the Civil Law Act is only for purposes of evidence and enforceability. It also does not affect the creation of resulting, implied or constructive trusts.

6.7 If sections 7 and 8 of the ETA were applied to the interpretation of section 7 of the Civil Law Act, an electronic record would satisfy the requirement for writing in section 7 of the Civil Law Act if the information contained in the record is accessible so as to be usable for subsequent reference and an electronic signature would satisfy the requirement for signature. Such a result would not prejudice the protection provided by section 7 of the Civil Law Act.

6.8 **Arguably however, a declaration of trust by the owner over land by electronic means should continue to be excluded, for consistency with the fact that a transfer to a third party as trustee would be excluded[78] and with our proposal in Part 8 to continue to exclude transfers of land.** Similarly, should an actual transfer of land by an owner fail because it purported to be effected by electronic

---

75 Cap.157

76 Civil Law Act (Cap.43) s.7. Under the Land Titles Act (Cap.157), the beneficiary can protect his interests by lodging a caveat under s.115 of that Act. Under the Registration of Deeds Act (Cap.269), the trust document can be registered if it is a deed. In any case, a caveat can be registered in respect of a trust: sections 8, 9.

77 The doctrine in *Rochefoucauld v Boustead* [1897] 1 Ch 196. See footnote 72

78 See para 6.4.

means, a resulting trust should not be imposed on the owner as this would avoid the safeguards intended for the owner.[79]

Q.12 Do you agree that section 4 should exclude testamentary trusts i.e. the ETA should not apply to testamentary trusts?

Q.13 Do you agree that section 4 should exclude trusts in relation to land i.e. the ETA should not apply to trusts for land?

Q.14 Do you agree that Parts II and IV of the ETA should be allowed to apply to implied trusts, in addition to constructive and resulting trusts (which are currently allowed)?

Q.15 Do you agree that Parts II and IV of the ETA should be allowed to apply to trusts (other than testamentary trusts and trusts in relation to land) created electronically? If the ETA is amended to enable non-testamentary trusts to be made electronically, what special requirements, if any, should apply to the creation of such trusts?

[79] See reasons for excluding land transfers discussed in Part 8, namely the need to protect unsophisticated homeowners from unwittingly parting with their homes.

PART 7
POWERS OF ATTORNEY

7.1 Section 4 excludes Parts II and IV of the ETA from facilitating the creation, performance or enforcement of powers of attorney by electronic means. Powers of attorney have been excluded to varying degrees in the electronic transactions legislation of other jurisdictions. New Zealand (like Singapore) has a complete exclusion[80], whereas some other jurisdictions restrict their exclusions to particular kinds of powers of attorney. Ireland only excludes enduring powers of attorney.[81] Canada has excluded powers of attorney with respect to financial affairs and personal care[82]. Some Canadian states exclude enduring powers of attorney as there are formality issues.[83] In contrast, New Brunswick has not excluded powers of attorney on the basis that powers of attorney are simply a form of agency contract and agency contracts in general are not excluded.[84]

7.2 It has been pointed out that the few advantages of making powers of attorney electronically are outweighed by the disadvantages.[85] Since the purpose of a power of attorney is to show it to third parties to establish the power of the attorney to alter the grantor's legal relationships, it is highly likely that the power of attorney will have to be put in paper form (with proper authentication) at an early stage, thus negativing any advantages of permitting the use of the electronic form.[86] If powers of attorney are not excluded, there is a risk that people might make them electronically in ignorance of the practical limits on their use.

---

80 New Zealand Electronic Transactions Act 2002.

81 Irish Electronic Commerce Act 2000, s.10(1)(a)(iii).

82 UECA section 2(3)(c).

83 An Alberta Law Reform Institute Report on Electronic Wills and Powers of Attorney was discussed at the 2001 Annual Meeting of the Uniform Law Conference of Canada (ULCC), the Report, which discouraged the use of electronic wills and powers of attorney, was received by the ULCC but the ULCC did not make any resolution on the issue of powers of attorney.

84 New Brunswick Department of Justice Consultation Paper on the Electronic Transactions Act is available at http://www.gov.nb.ca/justice/index.htm.

85 See footnote 83.

86 If a requirement for consent for use of electronic records is adopted (see Consultation Paper on Electronic Contracting Issues LRRD No.1/2004, available at www.agc.gov.sg, under Publications), there would be a problem of obtaining consent to the use of the power of attorney from all the third parties who are affected by it. The inconvenience may well be enough to discourage people from making electronic powers of attorney.

7.3 The Conveyancing and Law of Property Act[87] provides for instruments creating a power of attorney to be deposited in the Registry of the Supreme Court. On a sale under a contract providing for the execution of the conveyance by an attorney under a power of attorney, the purchaser is entitled to require that the power of attorney be so deposited.[88] The Registrar of Titles and Deeds may require such deposit of a power of attorney upon execution of an assurance or caveat[89] (or lodgement for registration of an instrument executed by an attorney)[90] by an attorney. Similarly, under the Trustees Act, a power of attorney delegating trusts during an absence of the trustee abroad is required to be deposited with the Registry of the Supreme Court.[91] Such deposit, which must be accompanied by affidavit or other evidence of the execution of the power of attorney, is intended to provide verification of the execution of the power of attorney. In the event that electronic powers of attorney are permitted, these existing paper-based procedures would have to be revamped to allow for the deposit of electronic instruments.

7.4 In practice, powers of attorney most often relate to land transactions. It would therefore be consistent with the exclusion of conveyances to exclude them.[92] The high value of such transactions justifies the extra precautionary measures to be taken.

7.5 Further, under common law, a power of attorney which empowers the execution of documents under seal must itself be made under seal. This requirement for sealing would prevent such a power of attorney from being made electronically, subject to provision for an electronic equivalent for sealing.[93] However, an amendment is currently being considered to abolish this requirement.[94]

7.6 Reference was made to enduring powers of attorney above. These are powers of attorney which continue to be effective despite the intervening mental incapacity of the donor of the power of attorney.

87 (Cap.61) s.48.
88 (Cap.61) s.8. A mortgagor has a similar right on the execution of a reconveyance or transfer or discharge of a mortgage by an attorney under a power of attorney.
89 Registration of Deeds Act (Cap.269) s.10.
90 Land Titles Act (Cap.157) s.147.
91 (Cap. 337) s.27
92 See Part 8.
93 On sealing requirement, see Part 5, para. 5.5.
94 See footnote 53.

Under general law, powers of attorney would cease upon the mental incapacity of their donor. In many jurisdictions, legislation has been promulgated to make it possible for persons to create powers of attorney in contemplation of their becoming mentally incapacitated. It is widely recognised that the creation of such powers of attorney require special safeguards to prevent abuse of powers by attorneys. A major consideration is that after becoming mentally incapacitated, the original donor would no longer be in a position to verify the execution of the power of attorney or to check on the exercise of the powers by the attorney. The exclusion of enduring powers of attorney from being made electronically is understandable in view of the analogy with wills. Further the formalities and safeguards imposed often do not lend themselves easily to being carried out by electronic means. There is currently no provision in Singapore law for enduring powers of attorney.

Q.16 Should electronic powers of attorney continue to be excluded from the application of the ETA? If you think electronic powers of attorney should be permitted, please explain why they should be permitted and how they may work in practice.

Q.17 Do you agree that powers of attorney used in relation to the disposition of land should continue to be excluded from the application of the ETA?

PART 8
TRANSFERS OF IMMOVABLE PROPERTY (i.e. LAND/REAL ESTATE)

8.1 Section 4 excludes Parts II and IV of the ETA from applying to the sale, disposition, conveyance or transfer of immovable property[95]. The main obstacles to land transactions being carried out electronically are the various requirements for writing, signature or deed in the context of land transactions.

8.2 The Conveyancing and Law of Property Act (CLPA)[96] provides that a conveyance of any estate or interest in land other than a lease for a period not exceeding 7 years at a rack rent shall be void at law unless it is by deed in the English language. As discussed in Part 5, the requirement for a deed need not be an obstacle to adopting electronic means. This is because electronic equivalents for signing, sealing and attestation exist. Further, there is an initiative to abolish the requirement for sealing of deeds.

8.3 Even where a deed or writing is not required to effect a transaction (for example, in the case of leases for a term of less than 7 years, or an option to purchase land), the Civil Law Act[97] (CLA) prevents contracts for the sale or other disposition of immovable property, or any interest in such property, from being enforced unless they are evidenced in writing and signed. The rationale for this requirement of the CLA is the prevention of fraud. However, courts have consistently allowed parol evidence to be admitted in the absence of signature or writing so that the statute cannot be used as "an engine of fraud".[98] Therefore, even if land transactions via electronic records continue to be excluded under section 4, the court could in appropriate cases uphold the transaction on the basis of evidence provided by the electronic record.

8.4 Various other disabilities flow from the lack of writing or deed in the context of land transactions. Section 6 of the CLPA provides for general words in a conveyance to transfer all land and buildings and

---

95 For simplicity, the term "land" is used interchangeably with references to "immovable property" in the rest of this Part.

96 Cap.61, section 53

97 Cap.43, section 6(d)

98 The doctrine in *Rochefoucauld v Boustead* [1897] 1 Ch 196.

rights appertaining to the land conveyed. Section 7 of the CLPA provides for covenants for title to be implied in a conveyance. Section 55 of the CLPA makes it unnecessary in a deed relating to land to add words of limitation to heirs when the intention is to give the absolute interest to a person and his heirs general. A transfer of land that is not effected by a conveyance or a deed will not benefit from these deeming provisions.

8.5 One of the main rationale for excluding electronic land transactions is the **protection of unsophisticated parties**. The exclusion avoids the danger that uninformed homeowners may be tricked into unwittingly parting with their property at undervalue through a clickwrap contract. The typical homeowner is inexperienced when it comes to home sales and is therefore vulnerable to being duped into a poor bargain. This argument takes on even greater importance in land scarce Singapore where property values are high. Further there is the difficulty of authenticating the identity of the contracting party.

8.6 On the other hand, sophisticated landowners such as corporations or statutory boards, and buyers or tenants of their property, could possibly benefit from the ease and convenience of being able to carry out certain land transactions electronically. An obvious example would be in the case of high volume or repetitive standard term transactions by property developers or statutory boards.[99] The possibility of effecting the renewal of commercial leases may be useful to institutional owners and their tenants. In this case, the danger of the parties being duped into an unintended transaction is minimal since both parties are already familiar with the property in question and the value of the lease.

8.7 **Technological obsolescence** is another concern which is relevant in the case of long term transactions and title documents. For example, if an option to purchase land granted by electronic means is to be exercised many years after the initial grant, the electronic record may no longer be accessible when that time comes to exercise the option. In the case of title documents, Land Registries which provide electronic registration of title will presumably be able to ensure timely conversion of records. Large corporations or statutory boards may also have the resources to convert their records. However, it is less certain

[99] E.g. the Housing Development Board (HDB) and Jurong Town Corporation (JTC).

whether private parties using electronic records in relation to non-registrable transactions will have the knowledge or ability to preserve their records in an appropriate manner.

8.8 **This category has been excluded from electronic transactions legislation of most other jurisdictions, but to varying degrees. Canada and New Zealand exclude only those instruments that require registration. Ireland excludes conveyancing but excepts contracts.** We seek feedback on whether the exclusion in section 4 of the ETA should be finetuned.

Q.18 Should any classes of persons be excluded from the operation of section 4(1)(d) or (e) of the ETA i.e. to enable them to enter electronic contracts for the sale or other disposition of land, or any interest in land? If yes, please specify in relation to which kinds of transactions, and propose any additional safeguards that may be necessary.

Q.19 Should any classes of land transactions be excluded from the operation of section 4(1)(d) or (e) of the ETA i.e. to enable such transactions to be carried out electronically? If yes, please specify any additional safeguards that may be necessary.

8.9 **E-conveyancing**

8.9.1 Singapore has already implemented an Electronic Lodgement System (ELS)[100] which enables documents to be lodged online with the Registrar of Titles.[101] ELS does not however extend to e-marketing of properties, online execution of options to purchase, sale and purchase

[100] Amendments were made to the Land Titles Act to provide a legislative framework for ELS in 2002. Under the ELS, the entire process within the purview of the Registrar of Titles has been computerised. Documents are lodged online with the Registrar, and registered on-line through a back-end IT system resulting in the updating of the electronic land register. In the case of documents that pass title, pertinent details of such documents are submitted to the Registrar electronically under a priority booking system within ELS, however hard copies of such documents must still be presented to the Registrar within the same lodgement day. The lodgement system is available via Internet. Digital cards, employing public and private key infrastructure, issued to authorised users are used to authenticate identity to ensure non-repudiation of transactions.

[101] A number of other jurisdictions have also introduced electronic lodgement systems e.g. New Zealand's Land*online* (see http://www/landonline.govt.nz), the Australian State of Victoria (see Report on "Electronic Conveyancing Victoria" (ECV) prepared by the Department of Natural Resources and Environment of Melbourne, Victoria, Australia), and the UK Land Registry.

agreements and other relevant deeds. It also does not cater for electronic exchange of funds (which would obviate the need for cashier's orders for legal completion).

8.9.2 An e-Conveyancing system currently under study in the UK envisages a completely electronic conveyancing process, including all contract documents used in the course of the transaction and electronic funds transfer.[102] In the US, on-line real estate transactions have already reportedly been carried out via on-line "signing rooms".[103]

8.9.3 Responses to a consultation conducted by the UK Lord Chancellor's Department[104] indicated that a vast majority of respondents agreed that electronic conveyancing documents[105] should be permissible, subject to implementation of a secure system against fraud. Particular issues discussed included the:

(a) *operative date and time of electronic documents*. Respondents were generally in favour of the operative time and date being stipulated in the electronic documents themselves, but some felt that further clarifications were needed in relation to withdrawal from the transaction and alteration of the effective date and time or minor terms;

(b) *requirement for witnessing of documents*. The Chancery Bar Association proposed that the requirement for witnessing a document should not be abandoned as witnessing provides a valuable function as giving evidence not only that the person has executed the document, but also where and when it was executed. The majority of respondents however agreed that attestation was inappropriate for electronic conveyancing

[102] See Lord Chancellor's Department Consultation Paper on "Electronic Conveyancing – A draft order under section 8 of the Electronic Transactions Act 2000" available at http://www.lcd.gov.uk/consult/general/e.conv.htm, and UK Land Registry's Consultation Paper and Report available at http://www.landregistry.gov.uk/e-conveyancing.

[103] A virtual, electronic room in which documents can be securely posted, edited and signed by parties to the transaction. Most of the transactions have centred on mortgages. See http://realtytimes.com/rtnews/rtcpages/20011003_paperless.htm, also 20000531 and 20000706. Also http://www.nchomeloan.com/Press%20Release/paperless.htm and http://wwww.emergis.com/en/newsroom/newsreleases/2003/feb24.asp.

[104] The Lord Chancellor's Department Consultation Response dated December 2001 available at http://www.lcd.gov.uk/consult/general/e-convresp.htm.

[105] For a general discussion on the application of the ETA to Indentures, and more particularly sealing, attestation, and delivery of deed, please see Part 5.

documents. The most common reason given was that authentication or certification of the electronic signature took the place of attestation. A number of respondents felt that there should be an added safeguard requiring the electronic signature to be affixed by a regulated professional. A small minority however thought that attestation is vital and its removal would be an erosion of fundamental principles;

(c) *need for a secure repository* for dematerialised documents not held at the Land Registry; and

(d) *preservation of the distinction between contract and deed*. Some felt that it was useful to preserve this distinction (e.g. for limitation purposes, and warranties and indemnities).

8.9.4 Respondents also identified a range of practical issues including:

(a) the difficulty of combining paper and electronic documents in a single transaction or chain of transactions;

(b) the need to provide proper assurance of an agent's authorisation where the agent signed a document electronically on behalf of the principal;

(c) the possibility that standard forms may not be suitable for complex transactions;

(d) the need to consider indemnity insurance issues; and

(e) electronic stamp duty (in particular how documents could be adjudicated).

8.9.5 The issues relating to an e-conveyancing system are complex and fall beyond the scope of the current consultation. **In our view an e-conveyancing system, if adopted, cannot be implemented merely by amendment of the ETA but will require amendments to other relevant statutes,** e.g. the Conveyancing and Law of Property Act[106]

[106] Cap.61.

and Land Titles Act[107], to ensure that the necessary safeguards are put in place to support electronic submissions and conveyancing.

[107] Cap.157.

PART 9
DOCUMENTS OF TITLE

9.1 Section 4 excludes Parts II and IV of the ETA from applying to documents of title. A document of title enables the person in possession of it to deal with property described in it as if he were the owner. They are used to prove ownership of property and may be deposited to provide security for mortgages or loans.

9.2 The most common type of document of title is the **bill of lading**. A bill of lading is a document of title transferable by endorsement and delivery, giving the holder the right to sue on it.[108] Provision for electronic bills of lading can be made via regulations under the Bills of Lading Act[109]. To date no such regulations have been made.

9.3 Various contractual schemes have used electronic contracts in place of traditional paper bills of lading. Seadocs, launched in 1983, was a hybrid scheme which retained the paper bill of lading, but it was deposited with a third party, with the right to its possession being dictated by electronic communications. The International Maritime Committee (CMI) Rules for Electronic Bills of Lading, issued in 1990, rely on a series of attornments[110] by the carrier to each new holder of the "electronic bill". Finally, the Bolero scheme[111], launched in 1999, is based upon a multilateral contract in the form of a Rule Book binding all participants. It also relies upon attornments[112] by the carrier, giving contractual effect to them by way of novation and a central Title Registry. These are not true equivalents of the paper bill of lading. They require the involvement of the carrier or registrar on

---

[108] It is not a negotiable instrument so that the transferee obtains no better title than the transferor has. Carriage of Goods by Sea Act 1924. Osborn's Concise Law Dictionary.

[109] Cap.384, section 1(5).

[110] For meaning of attornment, see footnote 113.

[111] A Bolero Bill of Lading is the "functional equivalent of a conventional bill of lading" but its legal basis is the Bolero Rulebook which is adopted contractually. Authentication of messages is drawn from the user's digital signature. The Bolero system acts as a postbox which checks on the authenticity of the digital signatures it receives and passes on messages. It also includes a title registry comprising an electronic database of information relating to Bolero bills of lading. It works only where all the parties are members of the Bolero Association. If a party wishes to sell cargo to a non-member, it will be necessary to switch to paper transactions; thereafter, the paper bill cannot re-enter the Bolero system. For more information on Bolero project see articles at http://www.elbornes.com/articles/bolero.htm, http://maritimelegal.com/article.htm, and http://www.fedpress.aust.com/Word/BurnettChap2.doc.

[112] For meaning of attornment, see footnote 113.

each transfer, achieving the same result as paper bills of lading by means of direct attornment[113] by the carrier, or by the registrar on the carrier's behalf, to a new 'holder', together with a direct contract between them incorporating the terms of the original contract of carriage.[114]

9.4 At present, there is no true electronic equivalent of a paper bill of lading. Nor does there seem to be any market demand for it. It remains to be seen whether technology of the future will provide the commercial world with a true electronic equivalent of the paper bill of lading.[115] The obstacle is a lack of international consensus on the elements of an electronic bill of lading. International consensus is essential as bills of lading are used in cross-border transactions.

9.5 Other examples of documents of title are delivery orders (issued by the owner of goods and addressed to the keeper of the warehouse where they are stored), and store warrants and dock warrants (by which a custodier acknowledges that he holds goods and undertakes to deliver them to a person named in the order). A dock warrant is a document of title issued by a dock company stating that certain goods therein mentioned are deliverable to a person named therein or his assigns by endorsement.[116]

9.6 The Commonwealth Expert Working Group noted that the "use of electronic bills of lading would give rise to the same "unique document" security concerns that lead most countries to presently exclude negotiable instruments[117] from their electronic transactions legislation" (e.g. issues of multiple copies and originals, and authenticity).[118]

---

113 A bailee's acknowledgment that he will hold the goods on behalf of someone other than the bailer (Blacks Law Dictionary, 7th ed).

114 UK Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions*, December 2001, Part 4.

115 UK Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions*, December 2001, para.4.8.

116 Osborn's Concise Law Dictionary, Seventh Edition, by Roger Bird (Sweet & Maxwell 1983).

117 See Part 4 on Negotiable Instruments.

118 Report of the Commonwealth Expert Working Group on Legal Aspects of Information Technology and the Related Law of Evidence (London 26-30 Jun, 2000). The Commonwealth Model Law on Electronic Transactions excludes Documents of Title. Similarly, the NZ Electronic Transactions Act (s.14(2)(d), referring to the First Schedule, Part 3) also excludes bills of lading.

9.7 **No change to the exclusion of documents of title is proposed**. It would be more appropriate for provisions for electronic forms of documents of title to be made in specific legislation dealing with those types of documents of title as they would require special rules, e.g. the Bills of Lading Act.

Q.20 Do you agree that electronic documents of title should continue to be excluded from the application of Parts II and IV of the ETA?

Q.21 Should Singapore enact any legislation to facilitate the use of electronic documents of title? If yes, please specify what kinds of documents of title, how they may work in practice and what legislative provisions will be required.

9.8 Carriage of Goods

9.8.1 The UN Model Law on Electronic Commerce[119] contains a Part relating to contracts of carriage of goods and transport documents. In preparing these provisions, UNCITRAL noted that carriage of goods was the context in which electronic communications were most likely to be used and in which a legal framework facilitating the use of such communications was most urgently needed.

9.8.2 The provisions, which apply to both negotiable and non-negotiable documents, would encompass bills of lading and negotiable instruments used in relation to carriage of goods. They provide for actions in connection with, or in pursuance of, a contract of carriage of goods carried out by one or more data messages to satisfy legal requirements for such actions to be carried out in writing or using a paper document. The reference to "one or more data messages" is intended to reflect the fact that, in the context of the transfer of rights through data messages, some of the functions traditionally performed through a single transmission of a paper bill of lading would necessarily imply the transmission of more than one data message.

9.8.3 The provisions also introduce a requirement of the guarantee of singularity in order to satisfy unique document requirements. The electronic procedures must ensure that it is not possible for more than one person (except in the case where title to goods are jointly held) to

[119] Articles 16 and 17, and Guide to enactment, paragraphs 108 to 122.

lay claim to the right at any one time and that there is reasonable assurance that the same data message cannot be multiplied and that no two media can be simultaneously used for the same purpose. The provisions also seek to address the situation where the use of data messages have to be replaced by paper documents.

9.8.4 Further, the provisions seek to ensure that laws such as the Hague and Hague-Visby Rules are not excluded merely by the use of data messages instead of paper documents.

9.8.5 The Canadian Uniform Electronic Commerce Act adopts these provisions from UN Model Law on Electronic Commerce. Although negotiable instruments and documents of title are excluded from Canadian legislation based on the Uniform Electronic Commerce Act[120], the application of the provisions on Contracts for Carriage of Goods to such documents has been preserved.

9.8.6 Such provisions are presumably intended to give a proactive boost to the growth of international trade by facilitating the adoption of electronic communications. However, it is recognised that, in the context of international trade, for a scheme of electronic communications to be viable there needs to be widespread acceptance of a similar legislative regime by one's trading partners. Currently there does not seem to be widespread adoption of such provisions. Nevertheless there does not seem to be any harm in adopting such legislation in anticipation of the growth of international consensus on the issue.

9.8.7 Alternatively, it may be felt that instead of having such general provisions on documents used in carriage of goods, more specific legislation (possibly under some other Act) is required. Nevertheless, the existence of general provisions on the subject would not prevent the adoption of more specific provisions in future, should the need arise.

[120] Manitoba Electronic Commerce and Information Bill C-31, Part 4; Ontario Electronic Commerce Act 2000, s.23. These provisions are based on the UNCITRAL Model Law on Electronic Commerce.

Q.22 Should Singapore enact legislation based on chapter 1 of Part 2 of the UN Model Law on Electronic Commerce[121] relating to documents used in carriage of goods?

[121] Chapter 1 of Part 2 of the UNCITRAL Model Law on Electronic Commerce:

"*Article 16. Actions related to contracts of carriage of goods*

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

(a) (i) furnishing the marks, number, quantity or weight of goods;
(ii) stating or declaring the nature or value of goods;
(iii) issuing a receipt for goods;
(iv) confirming that goods have been loaded;

(b) (i) notifying a person of terms and conditions of the contract;
(ii) giving instructions to a carrier;

(c) (i) claiming delivery of goods;
(ii) authorizing release of goods;
(iii) giving notice of loss of, or damage to, goods;

(d) giving any other notice or statement in connection with the performance of the contract;

(e) undertaking to deliver goods to a named person or a person authorized to claim delivery;

(f) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;

(g) acquiring or transferring rights and obligations under the contract.

Article 17. Transport documents

(1) Subject to paragraph (3), where the law requires that any action referred to in article 16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

(4) For the purposes of paragraph (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(5) Where one or more data messages are used to effect any action in subparagraphs (f) and (g) of article 16, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

(6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.

(7) The provisions of this article do not apply to the following: [...].".

PART 10
OTHER ISSUES

10.1 In the preceding Parts of this consultation paper, we have discussed each existing exclusion under section 4 of the ETA in turn. In some cases it may be felt that an existing exclusion can be completely removed because the rationale for the exclusion no longer applies. In other cases, it may be felt that the categories need to be finetuned by narrowing certain excluded transactions or, perhaps, by limiting the operation of the exclusions only to parties who are likely to need their protection. For example, should the exclusion for the creation of trusts be limited only to testamentary trusts? Should corporations and statutory boards be allowed to sell land electronically since they are less likely to require protection from the pitfalls of improper use of electronic transactions? We have included general questions below[122] to seek any feedback that may not have been discussed in the earlier Parts of this Paper. [123]

10.2 **We also seek views on whether any other transactions should be added to the exclusions under section 4.**[124] Notably, the electronic transactions legislation of some jurisdictions have excluded listed legislation and certain kinds of transactions not currently excluded under section 4 of the Singapore ETA. These excluded legislation and transactions relate broadly to:

(a) affidavits and other sworn documents;

(b) warrants to enter, seize or search;

(c) court documents and proceedings; and

(d) consumer protection notices.

10.3 We do not think that specific provision needs to be made for the types of documents referred to in paragraph 10.2 (a), (b) and (c) because the requirements for such documents are usually specified in legislation

---

[122] See questions 1 to 3.

[123] Section 4(1) of the Singapore ETA can be modified by order of the Minister for Communications, Information and the Arts.

[124] See question 2.

and would come under the scrutiny of the courts. In most cases their form is already governed by rules relating to court administration. In addition, they would often come within the purview of some other Government agency, in which case the discussion in paragraph 10.9 below would be relevant.

10.4 Some jurisdictions[125] exclude the provision of information required by consumer protection legislation from their electronic transactions legislation because of concerns that consumers may be given inadequate notice of such information if electronic means are used. Canada and Ireland however do not exclude consumer protection legislation.

10.5 Many jurisdictions have specific legislation imposing requirements on the use of electronic communications in relation to consumer transactions. For example, in relation to the legal requirement for information to be provided to consumers in writing, the US E-sign Act requires traders to obtain the consent of the consumer to use electronic records and inform the consumer of his right to withdraw his consent and to keep the consumer informed in relation to procedures, technical requirements and fees for such withdrawal.[126] European jurisdictions and Canadian provinces impose notice requirements on distance selling in their consumer protection legislation.

10.6 Some examples of consumer notices required under Singapore law are:

(a) the Hire-Purchase Act which renders a hire-purchase agreement unenforceable if it is not in writing. The agreement must be signed and served on the hirer. There are also requirements for certain notices to be given to the hirer and specification as to the size of type and legibility of prescribed documents. [127]

(b) the consumer information notice provided under the Consumer Protection (Fair Trading) (Cancellation of Contracts)

[125] A general exclusion in the New Zealand ETA, and a more limited exclusion in the US E-Sign Act (relating to specified transactions such as cancellation of utilities, foreclosure etc). Australia excludes the ETA only in relation to specific provisions in relevant legislation, such as the Trade Practices Act.

[126] US E-Sign Act s.103.

[127] Cap.125, s.3, 4, 5.

Regulations.[128] To be effective, a consumer information notice must be in a prescribed form and must be "brought to the attention" of the consumer.

10.7 Bearing in mind that the ETA is intended to promote the use of electronic commerce, the preferable approach would be to limit exclusions from the ETA as far as possible. Additional protective measures can be added in relevant legislation where it is felt that special safeguards are required, for example in relation to consumer protection. It can be made clear that the ETA does not affect such additional safeguards.[129]

10.8 **At the same time we also seek feedback whether the application of the ETA is uncertain in respect of any class of transactions**,[130] for example because of any specifications relating to the form of certain transactions (or the lack thereof) make it uncertain whether they may be done electronically. (Please refer to the discussion in paragraphs 2.1.5 to 2.1.7 above.)

10.9 In most cases this does not pose a practical difficulty since form requirements in legislative provisions usually relate to official forms required by Government agencies and the ETA already allows such agencies to use electronic forms notwithstanding anything to the contrary in any written law. Further, nothing in the ETA compels a Government agency to accept or issue any document in the form of electronic records. Therefore reliance cannot be placed on any provision of the ETA to deem that an electronic record satisfies form requirements, such as writing or signature, as against a Government agency, unless the Government agency decides to do so. Further,

---

[128] G.N. No. S620/2003.

[129] A provision modelled , for example, on section 9(4) of the ETA may be expanded to include the situation:

"9(4) Nothing in this section shall —

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

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

[130] See question 25.

Government agencies may make specifications with respect to the use of electronic records for such purposes.[131]

Q.23 Should any class of parties or transactions be excluded from the operation of section 4 of the ETA? If yes, please explain.

Q.24 Should any transactions be added to the exclusions under section 4 of the ETA? If yes, please explain.

Q.25 Do the form requirements in any legislation need to be clarified as to whether or not they may be satisfied by electronic means? If yes, please specify and explain the difficulty posed by the provision.

[131] ETA s.47.

ANNEX A

LEGISLATION REFERENCES

Singapore
Electronic Transactions Act (Cap.88) (1998)
http://www.ecitizen.gov.sg/

Australia
http://www.austlii.org/
Commonwealth Electronic Transactions Act 2000
New South Wales Electronic Transactions Act 2000
http://www.legislation.nsw.gov.au/
Electronic Transactions (Victoria) Act 2000
http://www.dms.dpc.vic.gov.sg/

Canada
Uniform Electronic Commerce Act
http://www.ulcc.ca/
British Columbia Electronic Transactions Act (2001)
http://www.qp.gov.bc/
New Brunswick Electronic Transactions Act (2001)
Consultation paper: *http://www.gov.nb.cp/justice/under.htm>.Paper*
Ontario Electronic Commerce Act 2000
Manitoba Electronic Commerce and Information Act 2000

Hong Kong
Electronic Transactions Ordinance (Cap.553)
http://www.justice.gov.hk/

Ireland
Electronic Commerce Act 2000
http://irlgov.ie/bills28/acts/2000/default.htm

New Zealand
Electronic Transactions Act 2002
http://www.legislation.govt.nz/

UK
Electronic Communications Act 2000
http://www.hmso.gov.uk/

US
Electronic Signatures in Global and National Commerce Act (E-SIGN Act) (2000)
http://www.access.gpo.gov/

UNCITRAL
http://www.uncitral.org/
Model Law on Electronic Signatures (2001)
Model Law on Electronic Commerce, with Guide to Enactment (1996) and article 6*bis* (1998)
Draft Convention on Electronic Contracting
draft used for discussion at 43rd session of Working Group IV, see A/CN.9/WG.IV/WP.108

EU
http://europa.eu.int/
Directive on Electronic Signatures (Directive 1999/93/EC)
eur-lex/eh/lif/dat/1999/en-399L0093.html
Directive on Electronic Commerce (Directive 2000/31/EC)
http://europa.eu.int/eur-lex/eh/lif/dat/2000/en-300L0031.html

The Commonwealth Secretariat
Model Law on Electronic Transactions
http://www.thecommonwealth.org

ANNEX B

Comparative Table of Excluded Transactions

Excluded transaction	Canadian Uniform Electronic Commerce Act s.2	New Zealand Electronic Transactions Act 2002, First Schedule, Part 3 (unless otherwise stated)	Irish Electronic Commerce Act 2000, s.10	US E-Sign Act s.103	Commonwealth Model Law (* listed as possible exclusions)	Australian Electronic Transactions Act 1999, exclusions under ET Regulations 2000
Wills	+	+	+	+	+	-
Negotiable instruments	+ except Part 3 (Carriage of Goods)	+	-	-	+	+ by exclusion of Bills of Exchange Act 1999 and Cheques Act 1986.
Indentures	-	Requirement for signature or seal to be witnessed met by means of witness' electronic signature (s.23)	Requirement for signature to be witnessed met if signature to be witnessed and signature of witness are advanced electronic signatures (s.14) Requirement for seal met by advanced electronic signature, based on a qualified certificate. (s.16)	-	-	-
Trusts	+ created by wills or codicils to wills	Testamentary instruments	+	Testamentary trusts	*	-
Powers of attorney	+ in respect of financial affairs or personal care of	+ and enduring powers of attorney	Enduring powers of attorney	-	*	-

	individual					
Land transfers	+ that require registration to be effective against third parties	Instruments or documents presented to Land Registry	Yes, except contracts (whether or not under seal) for the creation acquisition or disposal of interests in real property.	-	+	-
Documents of title	+ except Part 3 (Carriage of Goods)	Bills of lading	-	-	+	-
Others	-	Affidavits, statutory or sworn declarations	Affidavits, statutory or sworn declarations	Requirement for signatures or records o be notarized, verified or made under oath mat by electronic signature		Statutory Declarations Act 1959
	-	Notices to be given to public/ in writing in person or by registered post/ to be attached or displayed.	-	-	-	
	-	Warrant to enter/ search/ seize	-	-	-	
	-	Consumer protection information	-	Cancellation of utilities, health benefits, product failure, foreclosure etc. Note provision on consumer disclosures: s.101(c)	*	Trade practices Act 1974,certain sections.
	-	Mental health notices/ certificates	-	-	-	

	-	-	-	UCC except s 1 107, 1 206, Articles 2 and 2A	-	Corporations Act 1989, Corporations Law and subordinate legislation thereunder
	-	-	-	Adoption, divorce, family law	* documents relating to marriage	
	-	Ship registration instruments	-	-	-	
	-	Enactments relating to certain courts First Schedule, Part 4	Court procedures	Court proceedings	-	
	-	Listed Acts First Schedule, Part 1, 2	List Acts (s.11)	-	-	Other listed legislation

+ excluded.
- not excluded.

ANNEX C

LIST OF QUESTIONS

Q.1 Do you agree that electronic wills should continue to be excluded from the application of the ETA? If you think electronic wills should be recognised, please justify and suggest how they may work in practice.

Q.2 Should the Wills Act be amended to facilitate the use of electronic wills in exceptional cases? If yes, please suggest what circumstances such a provision may be used in and the amendments that should be made.

Q.3 Do you agree that negotiable instruments should continue to be excluded from the application of the ETA?

Q.4 Should the creation, performance or enforcement of an indenture continue to be excluded from the application of the ETA?

Q.5 Should Singapore adopt a provision in the ETA to allow secure electronic signatures (or only secure digital signatures) to satisfy the requirement for sealing?

Q.6 If you answered yes to Q.5, should any class of transactions be excluded from the provision allowing electronic signatures (or secure digital signatures) to satisfy the requirement for sealing e.g. land transactions?

Q.7 Should the ETA enable a secure electronic signature (or secure digital signature) to satisfy the attestation requirement, i.e. signing of a document by its maker using such a signature need not be witnessed by another person?

Q.8 Should the ETA provide that a legal requirement for a signature or seal to be witnessed is met by the *witness'* electronic signature?

Q.9 If you answered yes to Q.7 or 13, should any class of transactions be excluded from the provision e.g. land transactions?

Q.10 When should an electronic indenture take effect?

Q.11 What should be the requirements for withdrawal from or amendment of an electronic indenture?

Q.12 Do you agree that section 4 should exclude testamentary trusts i.e. the ETA should not apply to testamentary trusts?

Q.13 Do you agree that section 4 should exclude trusts in relation to land i.e. the ETA should not apply to trusts for land?

Q.14 Do you agree that Parts II and IV of the ETA should be allowed to apply to implied trusts, in addition to constructive and resulting trusts (which are currently allowed)?

Q.15 Do you agree that Parts II and IV of the ETA should be allowed to apply to trusts (other than testamentary trusts and trusts in relation to land) created electronically? If the ETA is amended to enable non-testamentary trusts to be made electronically, what special requirements, if any, should apply to the creation of such trusts?

Q.16 Should electronic powers of attorney continue to be excluded from the application of the ETA? If you think electronic powers of attorney should be permitted, please explain why they should be permitted and how they may work in practice.

Q.17 Do you agree that powers of attorney used in relation to the disposition of land should continue to be excluded from the application of the ETA?

Q.18 Should any classes of persons be excluded from the operation of section 4(1)(d) or (e) of the ETA i.e. to enable them to enter electronic contracts for the sale or other disposition of land, or any interest in land? If yes, please specify in relation to which kinds of transactions, and propose any additional safeguards that may be necessary.

Q.19 Should any classes of land transactions be excluded from the operation of section 4(1)(d) or (e) of the ETA i.e. to enable such transactions to be carried out electronically? If yes, please specify any additional safeguards that may be necessary.

Q.20 Do you agree that electronic documents of title should continue to be excluded from the application of Parts II and IV of the ETA?

Q.21 Should Singapore enact any legislation to facilitate the use of electronic documents of title? If yes, please specify what kinds of documents of title, how they may work in practice and what legislative provisions will be required.

Q.22 Should Singapore enact legislation based on chapter 1 of Part 2 of the UN Model Law on Electronic Commerce relating to documents used in carriage of goods?

Q.23 Should any class of parties or transactions be excluded from the operation of section 4 of the ETA? If yes, please explain.

Q.24 Should any transactions be added to the exclusions under section 4 of the ETA? If yes, please explain.

Q.25 Do the form requirements in any legislation need to be clarified as to whether or not they may be satisfied by electronic means? If yes, please specify and explain the difficulty posed by the provision.

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE III: REMAINING ISSUES

(Consultation Paper)

LRRD No. 1/2005

22 June 2005

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE III: REMAINING ISSUES

CONTENTS

EXECUTIVE SUMMARY OF PUBLIC CONSULTATION ON REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE III: REMAINING ISSUES

1 The Infocomm Development Authority of Singapore and the Attorney-General's Chambers are conducting a review of the Electronic Transactions Act (ETA) and the Electronic Transactions (Certification Authority) Regulations (CA Regulations). For this purpose, a public consultation is being carried out in 3 stages dealing with electronic contracting issues, exclusions from the ETA under section 4 and other remaining issues including secure electronic signatures and certification authorities.

2 Stage I of the Public Consultation, which concerned **Electronic Contracting Issues**, was launched on 18 February 2004 and closed on 15 April 2004. Stage II of the Public Consultation, concerning **Exclusions from the ETA under section 4**, was launched on 25 June 2004 and closed on 25 September 2004. The Consultation Paper on Electronic Contracting Issues (LRRD No.1/2004) and the Consultation Paper on Exclusions from the ETA under section 4 (LRRD No.2/2004) are available on the AGC website (www.agc.gov.sg, under Publications) and the IDA website (www.ida.gov.sg, under Policy and Regulation, IDA Consultation Papers). Responses to the Consultations, available on the IDA website, are under consideration.

3 Stage III of the consultation concerns the following issues:

- Regulation of Certification Authorities
- Exemption from Liability for Internet Service Providers
- Electronic Government
- UNCITRAL Electronic Contracts Convention and Related Issues

Regulation of Certification Authorities (CAs) (Part 2)

4 IDA conducted a study comparing Singapore's CA regime under the ETA and Electronic Transactions (Certification Authorities) Regulations

with regimes in other countries. To keep the ETA up to date with developments in the CA and security solutions industry, IDA proposes to:

- Remove PKI specific references from the ETA to promote a technology neutral approach to the regulation of CAs and the authentication and security solutions market.

- Replace the voluntary licensing scheme for CAs with a voluntary accreditation scheme.

- Remove financial criteria for accreditation of CAs i.e. requirements for a banker's guarantee, insurance coverage and minimum paid-up capital.

- Reduce application fees and licensing fees for accreditation.

- Increase the duration of accreditation from 1 year to 2 years.

- Limit audit requirement to relevant security guidelines.

Exemption from Liability for Service Providers (Part 3)

5 This Part contains a survey of international developments in the exemption from liability for network service providers. The extension of section 10 of the ETA, which provides for the exemption from liability for network service providers in Singapore, to cater to the emergence of new Internet services such as content hosting services and information location tools is discussed. It is proposed that this may be done by adopting a wide definition of "network service provider" and removing the reference to "provides access" in section 10. No change is proposed to the existing exceptions in section 10(2) i.e. we do not propose to adopt any new notice and take down regime.

Electronic Government (Part 4)

6 The goal of the e-Government Action Plan II is to serve the public best with infocommunications technology by integrating services to deliver seamless and speedy service through a single point of access. Novel legal issues arise from such integration initiatives e.g. the use of combined forms, the involvement of intermediaries (including private entities) in the delivery

of Government services, the production and retention of information in electronic form and the acceptance of electronic originals.

7 Amendments are proposed to make section 47, the central provision in the ETA on Government use of electronic records, more comprehensive. Amendments are also proposed to section 9 (retention of electronic records) to provide, as a default position subject to express opt-out, that Government agencies will accept the retention of documents in electronic form. A new section 9A (on the acceptance of electronic originals) is also proposed. (A related discussion on the provision of electronic originals is also found in Part 5.) These last 2 provisions also apply generally to non-Government transactions.

UNCITRAL Electronic Contracts Convention and Related Issues (Part 5)

8 The UNCITRAL Convention on the Use of Electronic Communications in International Contracts is expected to be finalised by UNCITRAL in July 2005. We discuss the implications of various changes that have been made to the draft Convention since our previous consultation on the subject in February 2004. We seek feedback on the impact of adopting the provisions of the Convention for domestic, as well as international, contracts and for other transactions.

CONSULTATION PAPER

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE III: REMAINING ISSUES

PART I
INTRODUCTION

1.1 This Consultation Paper, which forms Stage III of a Joint IDA-AGC[1] Public Consultation on the Review of the Electronic Transactions Act, is intended to solicit the views of industry and business, professionals, the public and Government Ministries and agencies, in order to inform the Government in its review of the ETA.

1.2 This Consultation Paper on Remaining Issues concerns the following:

- Regulation of Certification Authorities
- Exemption from Liability for Internet Service Providers
- Electronic Government
- UNCITRAL Electronic Contracts Convention and Related Issues.

1.3 With the enactment of the Electronic Transactions Act (Cap.88) in 1998, Singapore became the first country in the world to enact electronic transactions legislation based on the UNCITRAL Model Law on Electronic Commerce. Since then, numerous other countries have adopted electronic commerce legislation based on the UNCITRAL model.[2]

1.4 In view of these developments overseas and internationally, the Ministry of Information, Communications and the Arts (MICA)[3], the Infocomm Development Authority of Singapore (IDA) and the

[1] Infocomm Development Authority of Singapore – Attorney-General's Chambers.
[2] See Annex D for list of recent legislation on electronic transactions and useful websites.
[3] The Ministry was previously known as MITA.

Attorney-General's Chambers (AGC) are undertaking a joint review of the Electronic Transactions Act in 3 stages. Stage I of the Public Consultation concerning Electronic Contracting Issues was launched on 18 February 2004 and closed on 15 April 2004. Stage II, relating to Exclusions from the ETA under section 4, was conducted between 25 June and 25 September 2004. Stage III forms the final Consultation Paper in this series. [4]

1.5 The ETA and related subsidiary legislation and Singapore's position with regard to the UNCITRAL Electronic Contracts Convention will be reviewed based on feedback from all 3 stages of the Joint IDA-AGC Public Consultation on the Review of the Electronic Transactions Act. Draft amendments to the ETA and related legislation will subsequently be prepared and exposed for public comment.

- Please send your feedback on this Consultation to the Law Reform and Revision Division of the Attorney-General's Chambers, marked **"Re: ETA Remaining Issues"**

  - via e-mail, at agc_lrrd@agc.gov.sg;
  - by post (a diskette containing a soft copy would be appreciated) to "**Law Reform and Revision Division, Attorney-General's Chambers, 1 Coleman Street, #05-04 The Adelphi, Singapore 179803**"; or
  - via fax, at **6332 4700.**

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

- The closing date for this Consultation is **17 August 2005**.

- A soft copy of the Consultation paper may be downloaded from http://www.ida.gov.sg/idaweb/pnr/index.jsp (under Consultation Papers) or http://www.agc.gov.sg (under Publications).

[4] The Consultation Paper on Electronic Contracting Issues (LRRD No.1/2004) and the Consultation Paper on Exclusions from the ETA under section 4 (LRRD No.2/2004) are available on the AGC website (www.agc.gov.sg, under Publications) and the IDA website (www.ida.gov.sg, under Policy and Regulation, IDA Consultation Papers). Responses to these Consultations, available on the IDA website, are under consideration.

- In accordance with the standard practice of IDA, responses to this Consultation (including your name and your personal/company particulars) will be posted on the IDA website. Your response may also be quoted or referred to in subsequent publications or made available to third parties. Any part of the response which is considered confidential must be clearly marked and placed as an annex to the comments raised.

- If you need any clarifications, please contact:

  - **Ms Evelyn Goh** via e-mail at evelyn_goh@ida.gov.sg; or
  - **Mrs Joyce Chao** via e-mail at agc_lrrd@agc.gov.sg.

- The Public Consultation on the Review of the ETA has been carried out in 3 stages. This Consultation on Remaining Issues forms Stage III.

PART 2
REGULATION OF CERTIFICATION AUTHORITIES

2.1 The Electronic Transactions Act ("ETA") and the Electronic Transactions (Certification Authority) Regulations ("ETR") provide a legal framework to facilitate the establishment of trusted certification authority ("CA") services in Singapore, serving both the domestic and international markets. The goal is to establish Singapore as a trusted hub for e-commerce, with its wide range of security products and services, by providing a legal foundation that is up to date with technological developments.

2.2 Having achieved the initial target of providing a basic legal framework and secure public key infrastructure ("PKI") for trusted e-commerce transactions, the focus now is to maintain the market relevance of the ETA and ETR to international developments in this area. With the emergence of a more mature PKI market and the availability of new alternative security solutions, the existing framework of the ETA and ETR, which seeks to create trust by imposing stringent requirements for licensing CAs, may be inappropriate in today's context.

2.3 This Part discusses changes to the ETA and the ETR to facilitate further development of the CA, authentication and security solutions market. IDA proposes that Singapore should move away from ensuring the business viability of CAs through stringent financial requirements. Instead, users should be allowed to make their own commercial decisions on the level of security and risk that they are prepared to accept. The revised CA framework aims to encourage CAs to be "accredited"[5] so long as the security guidelines stipulated by IDA are met.

2.4 Although the ETA is generally technology neutral, provisions relating to digital signature in Part V of the ETA are predicated on PKI technology.[6] In this Part, we discuss ways in which the ETA and ETR can be expanded to facilitate a wider coverage of all authentication technologies and solutions.

---

[5] See paragraph 2.7.

[6] PKI technology is one of the many asymmetrical algorithms used in secured e-commerce transactions and e-communication.

2.5 The following issues are discussed in this Part:

- amendments in the ETA (and ETR) to ensure technology neutrality (Part 2.6)
- change in CA licensing regime from voluntary licensing to voluntary accreditation (Part 2.7)
- removal of all financial requirements (e.g. banker's guarantee, insurance and paid-up capital) (paragraphs 2.8.1 to 2.8.11)
- reduction of the application fee for accreditation (paragraphs 2.8.12 to 2.8.16)
- increase in the term of the accreditation from 1 year to 2 years (Part 2.9)
- limitation of audit requirement to compliance with relevant security guidelines (Part 2.10)

2.6 Technology Neutral Approach

2.6.1 Like most international legislation on e-commerce[7], the ETA is generally drafted to be technology neutral. However, some of its provisions are tied to the definition of secure digital signature, which is PKI specific.

2.6.2 PKI is one of the most secure authentication architectures in terms of reliability and non-repudiation attributes. Hence, the ETA and ETR, which were intended to be the benchmark for the integrity and security of authentication services offered by CAs in e-commerce transactions, are based on the highest level of secure authentication architecture – PKI.

2.6.3 To ensure that the ETA will accord the same benefits to other new and developing technologies like biometrics, IDA proposes to remove technology specific details from the ETA[8] and leave such details to regulations to be made under the ETA.

[7] UNCITRAL Model Law on Electronic Commerce 1996 and Electronic Signatures 2001, European Commission E-Commerce Directive 2000/31/EC.

[8] In particular, from Part VI (which defines secure digital signatures and the presumptions regarding certificates and unreliable digital signature), Part VII (which describes the general duties relating to digital signatures), Part VIII (which describes the duties of Certification Authorities) and Part IX (which describes the duties of subscribers). Part V defines what constitutes secure electronic records and signatures and their related presumptions.

2.6.4 By allowing the primary legislation[9] to remain technology neutral and leaving the specific details to the regulations, the law will be able to accord new authentication technologies the same benefits as those currently enjoyed by PKI quickly and conveniently by enacting new regulations.

Q1.	Do you have any comments on the proposal to move technology specific details in the ETA[10] to the ETR?

2.7 Voluntary Licensing / Accreditation

2.7.1 Most international economies have adopted voluntary schemes[11] for the licensing or accreditation of CAs as it is more conducive to the growth of the industry. Accreditation, in particular, is used in a number of countries e.g. Australia, Japan, and Taiwan.

2.7.2 **IDA proposes to replace the current "licensing" of CAs with an "accreditation" framework.** This will better represent the voluntary nature of our CA framework. The term "licensing" is misleading as it connotes that permission must be obtained in order to operate any CA business.

Q2.	Do you have any comments on the proposal to replace the current "licensing" approach with an "accreditation" approach in the ETA and ETR? (See Annex A)

2.8 Financial Criteria and Fees

2.8.1 IDA has received industry feedback that the financial requirements to obtain a licence from the Controller of Certification Authorities ("CCA") are too stringent. In addition, the cost of an annual security audit, required under the security guidelines, is a disincentive to

[9] i.e. the ETA.
[10] i.e. Parts VI, VII, VIII and IX.
[11] The voluntary scheme provides for an opt-in scheme for CAs to be certified. Most countries that are major players in e-commerce (e.g. UK, USA, and Australia) have adopted voluntary schemes. EU's E-signature Directive prohibits its member states from imposing mandatory licensing of CAs.

applying for the CA licence (or yearly renewal), given the small CA/PKI business market in Singapore[12].

2.8.2 A study on international practices conducted by IDA[13] found that the financial requirements in the ETR are more stringent than those in other countries. Singapore's licence application fees were found to be relatively high, with an additional requirement for a banker's guarantee. These might contribute to the high barrier to entry for companies contemplating accreditation as a CA in Singapore.

2.8.3 Taking into consideration the small market size for PKI in Singapore, IDA proposes the following amendments to the existing fees and financial criteria[14].

Banker's Guarantee

2.8.4 The requirement for a $1 million banker's guarantee in the current ETR[15] was intended to increase public confidence in the adoption of the then relatively new e-commerce market, by providing a 'safety cushion' for users in the event of termination of their CA service provider.

2.8.5 However, as the technology and CA experience has matured, the requirement for a banker's guarantee is no longer necessary. First, users of CA services are usually business users who are able to make their own commercial risk assessment before engaging the services of a CA. Second, a banker's guarantee of $1 million in the small CA/PKI market in Singapore[16] is a barrier to entry.

2.8.6 IDA proposes to remove the requirement for a $1 million banker's guarantee[17].

[12] The CA/PKI business market in Singapore is presently estimated around $4 million based on a study of the Singapore PKI and Infocomm Security Market conducted by Ernst and Young in October 2004.
[13] As part of this review, IDA studied the CA Regulations and Framework of regimes from USA, UK, Australia, EU, Japan, South Korea and Hong Kong.
[14] ETR, regulations 6 and 7. See Annex A.
[15] ETR, regulation 7(1)(d). See Annex A.
[16] See footnote 12.
[17] See footnote 15.

Insurance Requirement

2.8.7 It is a good risk mitigation practice for CAs to obtain insurance coverage for errors and omissions as these are inherent CA risks[18]. However, this should be a commercial decision for each CA rather than being imposed by law. Most countries do not have such an insurance requirement.

2.8.8 IDA proposes to remove the current insurance requirement in the ETR.[19]

Paid-up Capital Requirement

2.8.9 Under the current CA licensing scheme, IDA requires applicants to prove their financial health by having sufficient paid-up capital and available financing of not less than $5 million at the time of application.

2.8.10 IDA is of the view that the capacity of a CA to set up a secured CA service data center and to have sufficient funds to continue its operations should not be scrutinised by IDA. Instead, potential clients of a CA should make their own commercial assessment of the financial health of the CA as with any other business contract.

2.8.11 IDA recommends the removal of the current paid up capital requirement in the ETR.[20]

Application Fee & Annual Licence Fee

2.8.12 Currently, CAs must pay a $5,000 application fee on every grant or renewal of a licence to be a licensed CA[21]. In addition, the CA is required to pay a $1,000 fee for each year the licence is granted. A $1,000 fee is also payable for each year the licence is renewed. In other words, a CA must pay a total of $6,000 every year that it is licensed.

[18] Including risks related to system integration, impersonation, performance delays, and delays in maintenance of the Certificate Revocation List (CRLs), key compromise, security breach and fraud.
[19] ETR, regulation 7(1)(b). See Annex A.
[20] ETR, regulation 7(1)(c). See Annex A.
[21] ETR, regulation 6(1). See Annex A.

2.8.13 The application fee of $5,000 under the existing CA licensing scheme is relatively high compared to other countries. Some countries, such as Canada and Australia, do not require any application fees from CAs.

2.8.14 IDA proposes to reduce the application fee of $5,000 to a one time fee of $1,000 to cover the administrative cost of processing the accreditation application.

2.8.15 Instead of an annual fee of $1,000 upon the grant of accreditation and subsequent renewals, with the proposal to grant accreditation and renewals for periods of 2 years at a time[22], IDA proposes that the fee for each 2 year period should remain at $1,000.

2.8.16 The total fee payable by a CA will therefore be reduced to $2,000 for the first application for a CA accreditation and $1,000 subsequently for every 2 years of renewal and accreditation.

Q3.	Do you have any comments on the proposed amendments to the financial criteria and fees for CA accreditation?

2.9 Term of Accreditation

2.9.1 CAs are currently required to conduct a security audit prior to their initial application for licensing and before each application for renewal of their licence. Since the current licence duration is 1 year, CAs are required to conduct a security audit annually.

2.9.2 Based on industry feedback that the cost of an annual security audit is a disincentive when applying for the CA licence (or its renewal), especially given the small CA/PKI business market in Singapore, **IDA proposes to increase the term of accreditation of CAs (and renewal thereof) from 1 year to 2 years.**

Q4.	Do you have any comments on the proposed increase in the accreditation duration from 1 year to 2 years?

[22] See paragraph 2.9.

2.10 Operational Criteria & Auditing Requirements

2.10.1 In order to obtain or renew their licence, CAs are required to undergo security audits to ensure that they meet the level of integrity, security and service established under the ETR and IDA security guidelines.

2.10.2 The ETR requires an applicant for a CA licence to provide an independent audit certifying its full compliance with the ETA, the ETR and the terms of its licence.

2.10.3 IDA is of the view that while the audit should check the CA's compliance with the relevant security guidelines, a comprehensive audit on the CA's compliance with the ETA, ETR and licence conditions is unnecessary. IDA proposes to remove this requirement and to limit the audit requirements to relevant security guidelines[23].

Q5.	Do you have any comments on the proposed amendments to limit the audit requirement to relevant security guidelines?[24]

[23] The removal of this requirement does not reduce IDA's ability to enforce the legislations should there be any incident of breach.

[24] i.e. removing the auditing requirement in regulation 10(1)(b) (relating to compliance with licence conditions) and (d) (relating to provisions of the ETA and ETR)

PART 3
EXEMPTION FROM LIABILITY FOR INTERNET SERVICE PROVIDERS[25]

3.1 Existing Section 10

3.1.1 The Singapore government recognises the importance of network service providers in providing information infrastructure and content and maintains that it is essential for the growth of a national information infrastructure that the exposure of network service providers to the risks of liabilities for third party content be managed. For example, an ISP should not be held liable for objectionable content or defamatory statements on the thousands of web sites that are accessed daily, and over which the ISP has no control[26]. The government also realises the impracticality in having network service providers check all content for which they merely provide access.[27]

3.1.2 Section 10 of the ETA,[28] which has been on the statute book since 1998, provides that a network service provider is not subject to criminal or civil liability for third party material for which the provider merely provides access. This section does not, however, affect the obligations of a network service provider under any licensing or other regulatory regime established under the law such as the class licensing scheme and Internet Code of Practice administered by the Media Development Authority of Singapore (MDA).[29] It also

---

[25] In this Part, the term "internet service provider" is used to refer to person providing services on the Internet such as Internet service providers (ISPs), content hosts (e.g. website hosts, bulletin board service providers, etc) and providers of information location tools (e.g. search engine operators).

[26] IDA, Salient Features of Electronic Transactions Act 1998, available at http://www.ida.gov.sg (Accessed on 3 May 2005).

[27] IDA, Electronic Transactions Act, 1 May 2002, available at http://www.ida.gov.sg (Accessed on 3 May 2005).

[28] The Explanatory Statement to the Bill stated:
"Clause 10 provides that a network service provider is not subject to criminal or civil liability for third-party material in the form of electronic records to which the provider merely provides access. The protection under this clause will not apply if the provider does something more than merely providing access to the third-party material. The clause, however, will not affect the obligations of a network service provider as such under any licensing or other regulatory regime established under any written law. The clause will also not affect any obligation founded on contract or any obligation imposed under any written law or by a court to remove, block or deny access to any material."

[29] Under the Class Licence Conditions, an ISP or relevant Internet Content Provider (ICP) has to remove or prohibit the broadcast of programmes included in its service if MDA informs the ISP or ICP that the broadcast of the programme is contrary to an applicable Code of Practice or the

does not affect any obligations founded on contract or any obligations imposed under any written law or by a court to remove, block or deny access to any material[30].

3.1.3 Section 10 of the ETA was amended by the Electronic Transactions (Amendment) Act 2004[31] to carve out liability under the Copyright Act (Cap.63) in respect of infringement of copyright or unauthorised use of any performance, the protection period of which has not expired. These amendments were made in conjunction with the Copyright (Amendment) Act 2004. The Copyright Act, as amended by the Copyright (Amendment) Act 2004 provides defences for network service providers in respect of such infringement, based on

programme is against the public interest, public order or national harmony or offends against good taste or decency.

Under the Internet Code of Practice, an ISP or relevant ICP has to use its best efforts to ensure that prohibited material is not broadcast via the Internet to users in Singapore. An ICP is to deny access to material considered by MDA to be prohibited material if directed to do so by MDA. MDA has asserted its authority to block access sparingly and has blocked 100 "mainly mass impact pornographic sites" that children could easily access. (See L.S. Malakoff, *Are You Mommy, Or My Big Brother? Comparing Internet Censorship In Singapore And the United States, 8 Pac Rim L. L Polly 423* at 443; D. Boey, "Code Of Practice For The Net Revised", Business Times, 23 October 1997, Singapore at Home & Abroad, at page 2.)

Under the Code, prohibited material is material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws. The following factors are taken into account in considering what is prohibited material:

- whether the material depicts nudity or genitalia in a manner calculated to titillate;
- whether the material promotes sexual violence or sexual activity involving coercion or non-consent of any kind;
- whether the material depicts a person or persons clearly engaged in explicit sexual activity;
- whether the material depicts a person who is, or appears to be, under 16 years of age in sexual activity, in a sexually provocative manner or in any other offensive manner;
- whether the material advocates homosexuality or lesbianism, or depicts or promotes incest, paedophilia, bestiality and necrophilia;
- whether the material depicts detailed or relished acts of extreme violence or cruelty;
- whether the material glorifies, incites or endorses ethnic, racial or religious hatred, strife or intolerance.

A further factor that is considered is whether the material has intrinsic medical, scientific, artistic or educational value. MDA has the power to impose sanctions, including fines, on ISPs and ICPs who contravene the Code of Practice.

Information on legislation and guidelines relating to the Internet administered by MDA are available at http://www.mda.gov.sg/wms.www/devnpolicies.aspx?sid=161. The Class Licence Conditions and Internet Code of Practice may be viewed online there. (date accessed: 9 May 2005).

[30] E.g. pursuant to an injunction issued by a court on the application of an affected party.

[31] Act No. 54 of 2004

the model in the US Digital Millenium Copyright Act (DMCA)[32]. Consequently, the only defences available to a network service provider in respect of copyright and unauthorised use of performances are the defences in the Copyright Act. The Copyright (Amendment) Bill 2005[33] seeks, amongst other things, to make minor modifications to the copyright regime applicable to network service providers. Section 10 of the ETA continues to apply to network service providers in respect of all other areas, except for the exclusions in section 10(2).

3.1.4 Section 10 of the ETA, as amended with effect from 1 Jan 2005, reads:

Liability of network service providers

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

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

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

(2) Nothing in this section shall affect —

(a) any obligation founded on contract;

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

(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

[32] Title 17, Chapter 5, §512, referred to as the Online Copyright Infringement Liability Limitation Act.
[33] Bill No. 12 of 2005, introduced in Parliament on 17 May 2005.

(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.

3.2 New Internet Services

3.2.1 It is timely to review section 10 as the Internet has continued to evolve rapidly over the years. The variety of services and volume of content provided over the Internet has ballooned. Today new internet services are provided by means of various new technologies by a wide range of players employing different business models. Services are not limited to the provision of access to the Internet by telecommunication or broadcasting network operators[34] via their networks. It is necessary to consider whether the immunities under section 10 of the ETA should be extended to these new Internet technologies, players and activities and how the provision needs to be amended for this purpose.

3.2.2 **Content hosting services** have emerged whereby the content host may only provide storage for content on their servers and access via the Internet for such content, without providing or operating any networks of their own.[35] Commercially, content hosting usually involves the provision of computer systems with multiple web or file-transfer sites, each site with its own disk storage space and access to software facilities to add, remove and maintain the site contents. It may also provide associated system and network hardware and software to allow Internet access and specialised server software to allow Internet users to transfer copies of files stored on the system to

[34] e.g. SingTel, Starhub and M1
[35] e.g. Alta Vista.

their own computers, to view temporarily with browsers or to store on their own devices.[36] This includes personal homepages, websites, internet providers, message boards etc. Often, the content host does not play any role in creating or providing the content that it hosts. Such content may be provided by third parties without direct intervention by the content host. Hosting such content could potentially give rise to liability arising from illegal activities initiated by third parties. Liability can arise in respect of a wide variety of areas such as patents, trademarks, defamation, confidentiality, privacy, or illegal and harmful content, besides copyright.

3.2.3 The growth of services relating to Internet **information location tools** such as search engine service providers[37] is another development on the Internet. Information location tool providers carry out two main activities to help users find information on the Internet, namely, upon request by an Internet user, identifying and indexing new websites and displaying a list of links to websites where certain information is located.[38] Such service providers could face legal liability as a result of providing links to websites with infringing or illegal content insofar as they might be alleged to know the existence of the infringing or illegal material. Potential liability relating to copyright, trademark and competition violations may also arise in respect of particular linking techniques such as deep-linking[39], in-lining[40] and inclusion of certain material in links[41].[42]

3.2.4 A further new feature on the Internet comprises **aggregators**. These

[36] *"Who Is An Internet Content Host Or An Internet Service Provider (And How Is The ABA Going To Notify Them)?"* Internet Society of Australia. http://www.isoc-au.org.au/Regulation/WhoisISP.html accessed on 28 Apr 2005.
[37] e.g. Google.
[38] Esprit Project 27028 Electronic Legal Issues Platform (ECLIP) Deliverable 2.1.4 bis On-Line Intermediary Liability Issues: Comparing EU and U.S. Legal Frameworks Rosa Julia-Barcelo, accessed at europa.eu.int/ISPO/legal/en/lab/991216/liability.doc on 4 May 2005.
[39] Deep-linking consists of linking to some place other then the top level of the linked page (i.e. homepage). It may, in addition to possible copyright infringement arising from modification of copyright material, be alleged to create confusion as to the identity of the site owner or cause loss of advertising revenue by by-passing advertisements.
[40] In-lining, rather than directing the user to another website, instructs the Web browser to bring the linked image or text to the user from another website. It will automatically merge the image from the source website onto the other website. This may cause confusion as to the origin and ownership of the image.
[41] The inclusion of abstracts, famous words such as titles or trademarks, or pictures from another Website, might give rise to liability for violation of copyright or trademark laws.
[42] Esprit Project 27028, see footnote 38

are websites which provide links to a variety of sites so that, say, a user can read the headlines from multiple news sites conveniently on one page. Such aggregators link a wide variety of "upstream content" over which they may not have technical control to remove, depending on how their software code is implemented. Similarly, price comparison sites generate links to a wide variety of sites ranked by factors such as price and availability and are an important feature of the Internet in promoting consumer choice.[43]

3.2.5 Beyond these, the **P2P** (peer-to-peer) filesharing paradigm has evolved in ingenious ways since Napster. *Napster* provided filesharing services by routing user requests for a particular song or other work via a centralised index maintained by Napster. The user could then download the requested song or work directly from the location. Napster made no copies of files on its own servers. Following the Napster lawsuit, the default approach is now to employ a decentralized index. This is used by P2P services such as *Kazaa* and *Grokster*. A variation of this approach is to have a number of computers ("supernodes") act as servers hosting sub-indexes, thereby speeding up search times. *BitTorrent* demonstrates P2P services in its latest form. In this case, a particular file is not just downloaded by one user from just one other identified host or user. Instead, it is fetched from any other user who is sharing that file and the file is split into parts, each of which can be transferred independently. This improves transfer speeds enormously. *Freenet* loosely resembles *BitTorrent* in that files are downloaded and uploaded in small chunks from multiple sources, rather than as a whole, but further it encrypts files so that even a host sharing a file (or chunk thereof) cannot identify what file is being uploaded or stored.[44] These different technological configurations affect legal considerations as to knowledge and liability for unlawful content transferred via these methods.

3.2.6 The difficulties posed by the development of P2P intermediaries has been stated as follows:

[43] *Online Intermediaries and Liability for Copyright Infringement*, Charlotte Waelde and Lillian Edwards, World Intellectual Property Organization (WIPO) Seminar on Copyright and Internet Intermediaries, Geneva, 18 Apr 2005 page 24. This paper gives a comprehensive overview and analysis of international legal developments in respect of Internet intermediary liability and relevant technological developments. The seminar papers from the WIPO Seminar are available at www.wipo.int/meetings/2005/wipo_iis/en/program.html. (Accessed on 3 May 2005.)
[44] See *Online Intermediaries and Liability for Copyright Infringement*, page 7-9, see footnote 43.

> "Some form of immunity scheme for lawful P2P intermediaries may not only seem to be desirable but also essential if technological development is to continue. Yet given the essential value-neutrality of technologies, it is hard to see how a liability regime for "unlawful" and not "publicly beneficial" P2P intermediaries can be devised, except one wholly based on the intention of the service provider, such as the "active inducement" draft statutes we have seen introduced in the US. Legislation solely based on intent, however, may be difficult to prosecute and enforce."[45] [46]

3.3 Legislative Approaches to ISP Liability

3.3.1 Globally, there are 3 different approaches to service provider liability: first, the total liability approach, whereby intermediaries are treated as equally liable as content providers for unlawful content; second, the self regulation/total immunity approach; and third, the limitation of liability/notification and takedown approach. [47]

3.3.2 The first approach has not found support in the West as it "has usually been regarded as both practically unworkable, and dangerously likely to impede freedom of speech".[48]

---

[45] See *Online Intermediaries and Liability for Copyright Infringement*, page 59, see footnote 43.

[46] The **On-Line Criminal Liability Standardization Bill** introduced in the US Congress in 2002 is an example of an "active inducement" statute. The Bill seeks to amend the Federal Criminal Code to provide that no interactive computer service provider shall be liable for an offence arising from transmitting, storing, distributing or otherwise making available material provided by another person. The immunity is lost if the defendant intended that the service be used in the commission of the offence. The Bill provides that if the provider does not have such intent unless (a) an employee or agent has such intent and (b) the conduct constituting the offence was authorized, requested, commanded, performed, or tolerated by one or more members of the board of directors or a high managerial agent acting for the benefit of the provider within the scope of his office or employment. The Bill has been referred to the House Subcommittee on Crime.
"ISP Giants Support New Liability Bill" Katherine Balpataky, 18 Mar 2002, WebHost Industry Review, accessed at www.thewhir.com/features/isp031802.cfm on 27 Apr 2005, pointed out that the passage of the Bill could however take years and that further Congressional support remained to be seen.

[47] *Online Intermediaries and Liability for Copyright Infringement*, p.19–22, see footnote 43.

[48] In China, a form of strict liability is imposed on ISPs who are enjoined to refrain from "producing, posting or disseminating pernicious information that may jeopardize state security and disrupt social stability, contravene laws and regulations and spread superstition and obscenity". *Liability of Online Information Providers – Towards a Global Solution*, Chris Reed, (2003) 17(3) Int Rev LCT. Reference found in *Online Intermediaries and Liability for Copyright Infringement*, p.19, see footnote 43, which notes that access prevention provisions which would have a similar effect were dropped from the draft Australian Broadcasting Services Amendment (On Line Services) Act 1999 in the face of strong public and ISP community opposition to such an approach.

3.3.3 The second approach was based upon the expectation that service providers would for "commercial reasons, naturally take on an editorial and filtering role, so long as they are given protection from the risk of being seen as publishers, distributors or the like".

3.3.4 Section 230 of the **US Communications Decency Act**[49] is regarded as an example of the second approach. This provision has been interpreted by the courts to provide wide-ranging immunity for ISPs, however its precise scope is still being developed by the courts. It does not apply to federal criminal liability and intellectual property law.[50]

3.3.5 It has been noted, however, that this expectation of self-regulation has not altogether come to pass. "Intermediaries left to their own devices do not see content filtering as a core business activity, and will only largely remove illegal content on notice, both for fear of legal sanctions and as a matter of good public relations".[51]

3.3.6 Recent international developments in the US and Europe, namely the **US Digital Millenium Copyright Act (DMCA)**[52] and the **European E-Commerce Directive**[53] (2000/31/EC) and national laws

[49] Section 230 provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".
[50] The US Court of Appeals for the Fourth Circuit held in *Zeran v America Online Inc.* 958 F.Supp. 1124 (1997) that "Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium ... Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, keep government interference in the medium to the minimum." In *Kathleen R. v City of Livermore*, the California Court of Appeals found on Mar 2001 that the immunity provisions in the CDA applied to claims for injunctive relief as wells as damage claims, even though claims for equitable relief and for waste of taxpayer funds might not readily be characterized as "tort" claims. *Legal Liability for Internet Service Providers Under the Communications Decency Act*, Edmund B. (Peter) Burke, accessed on 26 Apr 2005 at www.gigalaw.com/articles/2001-all/burke-2001-05-all.html.
[51] *Online Intermediaries and Liability for Copyright Infringement*, p.20-22, 59, see footnote 43.
[52] See footnote 32
[53] The **European E-Commerce Directive** (2000/31/EC) adopted by the European Commission deals, amongst other things, with the criminal and civil liability of e-commerce intermediary service providers. It provides for protective measures in respect of "mere conduit", caching and hosting services. These protections do not however "affect the possibility of a court or administrative authority, in accordance with Member States' legal systems, requiring the service provider to terminate or prevent an infringement" and in the case of hosting services, additionally allows, Member States to create procedures to "govern the removal or disabling of access to information" *Emerging Patterns of E-Commerce Governance in Europe – the European Union's Directive on E-Commerce* George Christou and Seamus Simpson, paper prepared for 32nd Telecommunication

implementing the Directive, have tended to take the third approach. [54] An emerging consensus can be discerned on what functions of service providers need to be protected.[55] There is however an on-going debate as to when and the extent to which service providers should be required to proactively remove, disable unlawful content.[56] Even more controversial are provisions that require service providers to proactively monitor unlawful content or to identify persons responsible for providing such content.[57]

3.3.7 Some legislation on service provider liability have taken a liability-specific (i.e. vertical) approach e.g. **UK's Defamation Act 1996**[58]

Policy Research Conference: Communication, Information and Internet Policy, George Mason University Law School, Arlington, Virginia, US, Oct 1-3, 2004. (Accessed at http://web.si.umich.edu/tprc/papers/2004/297/chris-simpTPRC04(final).pdf on 4 May 2005). This paper outlines the salient features of the legislation enacted by Finland, UK and Germany. If an activity does not qualify for exemption under the Directive, it does not mean that the service provider is automatically liable as the service provider may avail itself of other defences available under existing law.

The main areas in which they differ concern the circumstances requiring service providers to remove or disable content. The implementation deadline was 17 Jan 2002. As the liability standard set out in the Directive is a maximum standard, Member States can decide to impose less cumbersome liability criterion. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP published in Computer Law Review International discusses the provisions enacted or proposed by Belgium, Finland, France, Germany, Luxembourg, Norway, Spain, Sweden. (Accessed at www.softic.or.jp/symposium/open_materials/10th/en/vinje2-en.pdf on 4 May 2005).

[54] Some other articles on such legislation: *Online Information Provider Liability for Copyright Infringement: Potential Pitfalls and Solutions*, Michael L. Siegel, 4 Va.J.L. & Tech.7, accessed on 26 Apr 2005 at www.vjolt.net/vol4/issue/v4i2a7-siegel.html; *Internet service provider liability for subscriber copyright infringement, enterprise liability, and the First Amendment*, Alfred Yen, Georgetown Law Journal accessed on 26 Apr 2005 at www.findarticles.com/p/articles/mi_qa3805/is_200006/ai_n8880509/print; *On the Service Provider Liability for Illegal Content*, Sanna Heikkinen, article in T-110.501 Seminar on Network Security 2001 ISBN 951-22-5807-2, accessed on 26 Apr 2005 at www.tml.hut.fi/Studies/T-110.501/2001/papers/index.html; *Liability Immunity for Internet Service Providers – How Is It Working?*, Heidi Pearlman Salow, Journal of Technology Law & Policy, Vol 6, Issue 1, accessed on 26 Apr 2005 at http://grove.ufi.edu/~techlaw/vol6/issue1/Pearlman.html.

[55] These relate to transitory communication or mere conduit activities, caching and hosting. Many jurisdictions also include information location services. See Part 3.5 below.

[56] See discussion at Part 3.6.

[57] See discussion at Part 3.9.

[58] UK's Defamation Act 1996 was an early precursor to legislation providing protection for service providers. Section 1 of the UK Defamation Act 1996 (so far as relevant) reads:

"(1) In defamation proceedings a person has a defence if he shows that —

(a) he was not the author, editor or publisher of the statement complained of,

(b) he took reasonable care in relation to its publication, and

(c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

[(2) omitted.]

which relates to liability for defamation, and the US DMCA and Singapore Copyright Act which are confined to liability under those Acts. Alternatively, legislation may take a horizontal approach that applies generally in respect of all unlawful content or activities. This is the approach adopted by the EC Directive and section 10 of the Singapore ETA (except for the carve out for liability under the Copyright Act).

3.3.8 It has been questioned whether the assumptions underlying the need for service provider immunity still hold true today. A paper[59] presented at the WIPO Seminar on Copyright and Intermediaries held in Geneva on 16 April 2005 stated:

> "ISP immunity ... was based on the perception of ISPs as beleaguered defendants, facing unlimited risk as a result of hosting or providing access to limitless amounts of content over which they had little of no control. This led to a need for immunities to safeguard the public interest in a healthy Internet access market. But since then, a number of factors have altered."

3.3.9 The paper[60] proceeds to point out that "the online media industry has become more mainstreamed, and thus perhaps less in need of special protections to survive". It also asserts that "the expectation that intermediaries would naturally be driven by market forces to remove and block illegal content has not altogether come to pass. Intermediaries left to their own devices do not see content filtering as a core business activity, and will only largely remove illegal content on notice, both for fear of legal sanctions and as a matter of good

(3)A person shall not be considered the author, editor or publisher of a statement if he is only involved —
[(a) omitted.]
(c) in processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form;
[(d) omitted.]
(e) as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.
(4) In a case not within paragraphs (a) to (e) the court may have regard to those provisions by way of analogy in deciding whether a person is to be considered the author, editor or publisher of a statement.".

[59] *Online Intermediaries and Liability for Copyright Infringement*, page 59, see footnote 43.
[60] *Online Intermediaries and Liability for Copyright Infringement*, page 59, see footnote43.

public relations; but ... even NTD[61] regimes are extremely problematic when considering the public interest and the public domain".

3.4 Issues

"Network service provider"

3.4.1 Section 10 of the ETA currently uses the term "network service provider". This term is not defined in the ETA. The reference to "network" may arguably cause the term to be interpreted to exclude those service providers that do not operate telecommunications or broadcasting networks. As noted in Part 3.2, service providers may provide services such as content hosting or information location tools without operating or providing access to networks.

3.4.2 The Copyright Act[62] contains a wide definition of the term "network service provider":

> "network service provider" —
>
> (*a*) for the purposes of section 193B[63], means a person who provides services relating to, or provides connections for, the transmission or routing of data; and
>
> (*b*) for the purposes of this Part (other than section 193B), means a person who provides, or operates facilities for, online services or network access and includes a person referred to in paragraph (*a*),
>
> but does not include such person or class of persons as the Minister may prescribe.

3.4.3 The term "service provider" is used in the US DMCA. In relation to transitory digital network communications, it is defined to mean an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material sent or received. Otherwise, it means a

[61] i.e. Notice and Takedown

[62] (Cap.63) section 193A. This section also defines "routing" (which is used in the definition) as "directing or choosing the means or routes for the transmission of data".

[63] Section 193B of the Copyright Act relates to immunity in relation to transmission, routing and provision of connections.

provider of online services or network access, or the operator of facilities therefore, including an entity described above.

3.4.4 These broad definitions appear to embrace traditional ISPs, search engines, bulletin board system operators, and even auction web sites.[64] The District Court in the *Aimster* case[65] found that Aimster, a P2P filesharing service provider,[66] did fall within the definition of an Internet service provider but held that it did not qualify under the various safe harbour provisions in the US DMCA, namely, transitory communication[67], caching[68] or information location tools[69].

3.4.5 The EC Directive applies to "information society services providers" or "intermediary service providers" which are defined by reference to the term "information society service". This is defined as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service".

3.4.6 The EC Directive covers not only the traditional ISP sector, but also a much wider range of actors who are involved in selling goods or services online (e.g. e-commerce sites such as Amazon and Ebay), offering online information or search tools for revenue (e.g. Google, MSN, LexisNexis or Westlaw); and "pure" telecommunications, cable and mobile communications companies offering network access services. The requirement that the service be offered "at the individual request of the recipient" however means that TV and radio broadcasters do not fall within the remit of the EC Directive, although

[64] *Online Intermediaries and Liability for Copyright Infringement*, p.11, see footnote 43.
[65] *Re Aimster* 334 F.3d 643.
[66] See description of P2P filesharing services at paragraph 3.2.5.
[67] The Aimster system worked by allowing users to communicate and transfer files via privately created networks. Thus information transferred between individual users, but did not pass through Aimster's system. *Online Intermediaries and Liability for Copyright Infringement*, p.40, see footnote 43.
[68] The Court held this provision was not applicable. *Online Intermediaries and Liability for Copyright Infringement*, p.40, see footnote 43.
[69] The Court considered that Aimster did not meet the conditions under this safe harbor because, in order to apply, a service provider cannot have actual knowledge of the infringing material or activity, or, in the absence of actual knowledge, the service provider cannot be aware of facts or circumstances from which the infringing activity is apparent. If they did have such knowledge they must take steps to remove or disable access to the material. Aimster had taken no such steps. *Online Intermediaries and Liability for Copyright Infringement*, p.40, see footnote 43.

sites which offer on-demand services such as video-on-demand are included. Certain relationships are excluded from the EC Directive as not provided wholly "at a distance". However, even if a service is provided free of charge, this does not mean that the service provider falls outside the EC Directive if the service broadly forms "an economic activity".[70]

3.4.7 The UK Electronic Commerce (EC Directive) Regulations 2002 (the UK Regulations) use the term "service provider", defined to mean a person providing an information society service. "Information society service" is defined by reference to the EC Directive.

3.4.8 As it is the intention to protect service providers in relation to content hosting or information location tools whether or not they operate or provide access to networks, the term "network service provider" should be defined in the ETA to clarify the matter. The following definition, derived from that in the Copyright Act, is proposed for discussion:

> "network service provider" means a person who provides, or operates facilities for, online services or network access and includes a person who provides services relating to, or provides connections for, the transmission or routing of data, but does not include such person or class of persons as the Minister may prescribe.[71]

3.4.9 The reference to "online services" would extend beyond traditional ISPs, search engines and bulletin board system operators, to auction web sites and even the selling of goods and services online.[72] Would such a definition extend the immunity under section 10 too widely? (See further discussion in paragraphs 3.4.15 to 3.4.22 below.)

[70] *Online Intermediaries and Liability for Copyright Infringement*, p.11, 12, see footnote 43. Recital 18 of the EC Directive clarifies. For example, it seems an employer is not an "information service provider" in terms of his employment relationship with his workers; and a doctor is not a provider of such a service so long as his advice even partially requires a "physical examination of the patient". Questions arise whether a university can avail itself of the immunity provisions if it provides personal workspace to students, if it primarily fulfils its role of providing educational services by face-to-face education rather than distance learning.

[71] We do not think that it is necessary to adopt the definition of "routing" from the Copyright Act as the term is sufficiently clear. See footnote 62.

[72] See paragraph 3.4.4.

"To which he merely provides access"

3.4.10 The words "to which he merely provides access" in section 10(1) includes caching since "provides access" is defined to mean, in relation to third-party material, 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.[73]

3.4.11 It may also arguably extend to linking whether by hyperlinking, search engine or P2P software.[74]

3.4.12 It does not however seem to extend to permanent storage or hosting (as opposed to caching).[75] Apart from traditional content hosting services, such as website hosting, bulletin boards, etc., this may also affect information location tools services which, as is common practice for search engines, cache previously retrieved material more or less permanently. This aids users in locating information in future as the material may subsequently be moved or removed from the original site.

3.4.13 One way to extend section 10 to apply to storage and hosting functions is to add express references to those functions in section 10. However, given the fast rate of evolution of Internet technology and practices, it would be hard to find language that would encapsulate all present and future functions that should be included.

3.4.14 **A simpler approach is to remove the limiting words "to which he merely provides access".** If this approach is taken and the words "to which he merely provides access" in section 10(1) are deleted, then the definition of "provides access" in section 10(3) should also be deleted as a consequential amendment. This means however that section 10 will no longer be limited to the functions mentioned in that definition i.e. providing access to material and automatic or temporary storage of material. This again raises the issue whether section 10 will

[73] Section 10(3) of the ETA.
[74] See footnote 73
[75] *Online Intermediaries and Liability for Copyright Infringement*, p.21, see footnote 43 and footnote 64 in that article. "Singapore provides total immunity to intermediary service providers but only in relation to transmission and caching liability, not, crucially, hosting."

apply too widely. (See discussion in paragraphs 3.4.15 to 3.4.22 below.)

"Third party material"

3.4.15 The reference to "third party material" in section 10(1) limits the extent of the immunity that may be claimed under section 10 to that in respect of material from "a person over whom the provider has no effective control". For example, a business selling goods or services online, cannot claim immunity under section 10 in respect of misrepresentations that it has itself made online.

3.4.16 A question arises, however, in respect of a retailer offering a product for sale online that provides a link to the manufacturer's website containing misrepresentations or misleading information concerning the product offered for sale by the retailer. Should the retailer be immune in respect of liability arising from information appearing in the manufacturer's website? Liability may conceivably arise, say, under the Consumer Protection (Fair Trading) Act[76] if a consumer reads the information via the link and is thereby misled. If section 10 applies to the retailer, he will enjoy immunity in this situation because the misleading information was third party material, presuming that the manufacturer is a person over whom the provider has no effective control. Another question may arise whether, by deliberately linking to the manufacturer's website, the retailer has adopted the information so that it ceases to be "third party material", in which case, the immunity may not apply.

3.4.17 The case of information linked by an aggregator may give rise to similar issues. An aggregator, unlike a pure search engine, may have deliberately chosen to link information from a specific website. Should a news aggregator be liable for, say, defamatory remarks appearing in newspaper articles displayed via the aggregator? Under the UK Defamation Act, such an aggregator would have to show that "he took reasonable care in relation to its publication, and he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement". There are no such conditions in section 10 of the ETA.

[76] Cap.52A.

Regulatory schemes

3.4.18 In the US DMCA and the EC Directive, as well as the Singapore Copyright Act, the effect of the wide definitions of the terms "service providers", "information society services providers" and "network service providers" respectively is limited by the fact that the immunity granted by those legislation relates to specific functions (i.e. transitory communications, caching, hosting and additionally in the case of Singapore and US copyright legislation, information location tools)[77] and are conditional upon the obligation to remove or disable access to information in certain circumstances (i.e. upon obtaining certain knowledge or notice)[78].

3.4.19 In the case of section 10 of the ETA, the Class Licensing Scheme may serve a similar function. The obligations of a network service provider under the Class Licensing Scheme are preserved by section 10(2).[79] Under this scheme, MDA[80] has powers to issue takedown and blocking orders and internet service providers are required to comply with an Internet Code of Conduct.[81]

3.4.20 Section 10(2) of the ETA also preserves obligations "imposed under any written law or by a court to remove, block or deny access to any material".[82] A service provider would therefore have to comply with a court order or other direction made under written law requiring such removal, blocking or denial of access to material. Presumably, it is not intended that the immunity granted in section 10(1) against "civil and criminal liability" should extinguish or affect the right of the court to grant injunctive relief. In the example in paragraph 3.4.16, the court would therefore be able grant an injunction under section 9 of the Consumer Protection (Fair Trading) Act (based on the fact that there has been an unfair practice) ordering the removal of the link to the misleading content, although other remedies under that Act (such as a claim for damages) would not be available against the retailer.

[77] See further discussion of categorisation of functions in Part 3.5.
[78] See further discussion on knowledge requirements and takedown regimes in Part 3.6.
[79] Section 10(2)(b) "Nothing in this section shall affect ...(b) the obligation of a network service provider as such under a licensing or other regulatory regime established under any written law".
[80] Media Development Authority of Singapore.
[81] See footnote 29.
[82] Section 10(2)(c) "Nothing in this section shall affect ...(c) any obligation imposed under any written law or by a court to remove, block or deny access to any material".

3.4.21 Notably, the immunities under the UK Regulations[83] apply only to liability for "damages and other pecuniary remedy or for any criminal sanction". This allows injunctive relief to be sought against the service provider. Similarly, the safe harbour provisions under Singapore and US copyright laws apply only to prevent a court from granting monetary relief or making any order for infringement of copyright against the network service provider.

3.4.22 Notwithstanding the apparent width of the application of section 10 if it is amended in the manner proposed in paragraphs 3.4.8 and 3.4.14, the limitation to "third party material"[84] and the preservation of controls under the Class Licensing Scheme[85] and obligations to comply with orders to remove, block or disable access to material,[86] may provide an adequate balance.

Q6.	Is it necessary to clarify the meaning of "network service provider". Do you agree with the proposed definition of "network service provider"? (See definition proposed for discussion in paragraph 3.4.8)
Q7.	Do you agree with the proposed deletion of the words "to which he merely provides access" in section 10(1) of the ETA? (See paragraph 3.4.14)
Q8.	If section 10 of the ETA is amended as proposed in paragraphs 3.4.8 and 3.4.14, do you think any further safeguards are necessary? In particular, would the protection given under section 10 be too wide? (See paragraph 3.4.22). If yes, please elaborate with specific reference to the kinds of liability from which network service providers should not be exempted.

3.5 Alternative Approaches

Categorisation of protected functions

3.5.1 Both the EC Directive and the US DMCA define the various functions

[83] Electronic Commerce (EC Directive) Regulations 2002.
[84] See paragraphs 3.4.15 to 3.4.17.
[85] See paragraph 3.4.19.
[86] See paragraph 3.4.20.

in respect of which service providers can obtain immunity from liability. Their categorization of transmission, caching and hosting functions are markedly similar. The EC Directive does not, however, include any provision on information location tools.

3.5.2 ***Transmission, routing and provision of connections.*** This relates to the function of providing communications networks for transitory traffic. There is a consensus that service providers should not be liable for the content of traffic passing through their networks, as long as the material is handled automatically by their systems and the service provider does not store, control or modify the material.

3.5.3 The Singapore Copyright Act, based on the US DMCA, refers to "the transmission or routing by the network service provider of, or the provision of connections by the network service provider for, an electronic copy of the material through the network service provider's primary network". Immunity is subject to the conditions that (a) the transmission was initiated by or at the direction of a person other than the network service provider; (b) the transmission is carried out through an automatic technical process without any selection of the electronic copy of the material by the network service provider; (c) the network service provider does not select the recipients of the electronic copy of the material except as an automatic response to the request of another person; and (d) the network service provider does not make any substantive modification (other than any modification made as part of a technical process) to the content during the transmission through the primary network. [87] The Act also extends to transient storage by the network service provider of an electronic copy of the material in the course of such transmission, routing or provision of connections.[88]

3.5.4 The UK Regulations[89] implementing the EC Directive, have similar provisions on the "mere conduit" function. It applies to the "transmission in a communication network of information provided by a recipient of the services or the provision of access to a communication network" and includes intermediate and transient storage of information (a) which takes place for the sole purpose of

[87] (Cap.63) section 193B.
[88] (Cap.63) section 193C(1)(b).
[89] Electronic Commerce (EC Directive) Regulations 2002, regulation 17.

carrying out the transmission and (b) where the information is not stored for any period longer than is necessary for the transmission. The conditions are that the service provider (a) did not initiate the transmission, (b) did not select the transmission and (c) did not select or modify the information contained in the transmission.

3.5.5 Provisions on takedown notices do not apply to these functions since the passage of the material in question is, by definition, transitory.

3.5.6 ***Caching*** refers to the storing of Web files for later reuse so that they can be accessed more quickly by the end-user. Many service providers maintain "proxy servers" that store pages copied from the Web. When a user requests a page stored on a proxy, the service provider delivers the page quickly from the proxy rather than using the Web server to retrieve the page from the Internet.

3.5.7 The Singapore Copyright Act describes system caching as the making of a copy of material on the network service provider's primary network from another electronic copy of the material made available on a network (referred to as the originating network) through an automatic process in response to an action by a user of the primary network and in order to facilitate efficient access to the material by that user or other users.[90] The conditions for the "safe harbour" to apply are that the network service provider does not make any substantive modification (other than any modification made as part of a technical process) to the content of the cached copy of the material during the transmission of the cached copy of the material to users of the primary network or another network. In addition, the network service provider must comply with a takedown regime and any prescribed conditions relating to access to the cached copy of the material by users of the primary network or another network; the refreshing, reloading or updating of the cached copy of the material; and non-interference with technology used at the originating network to obtain information about the use of any material on the originating network, being technology that is consistent with industry standards in Singapore.

[90] (Cap.63) section 193C(1)(a).

3.5.8 The UK Regulations[91] describe caching as "automatic, intermediate and temporary storage where that storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request". The conditions are similar to those mentioned in the preceding paragraph except that, instead of a formal takedown regime adopted by those copyright laws, service provider must act "expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.[92]

3.5.9 ***Storage of third party material.*** This is one aspect of content hosting.[93] (See description of content hosting activities in paragraph 3.2.2).

3.5.10 The Singapore Copyright Act[94] protects "storage, at the direction of a user of the network service provider's primary network, of an electronic copy of the material on the primary network. The conditions to be satisfied are that the service provider does not receive any financial benefit directly attributable to the copyright infringement if the provider has the right and ability to control the infringing activity. The service provider must remove or disable access to the material if it acquires actual knowledge of the infringement or knowledge of facts or circumstances which would lead inevitably to

[91] Electronic Commerce (EC Directive) Regulations 2002, regulation 18
[92] Electronic Commerce (EC Directive) Regulations 2002, regulation 17.
" ... the service provider -
(i) does not modify the information;
(ii) complies with conditions on access to the information;
(iii) complies with any rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
(iv) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
(v) acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement."
[93] See description of content hosting in paragraph 3.2.2 above.
[94] (Cap.63) section 193D(1)(a).

the conclusion that the copyright in the material has been infringed,[95] or pursuant to provisions for takedown notices. There are also provisions to restore material pursuant to counter notices.

3.5.11 The UK Regulations[96] provide immunity in respect of "storage of information provided by a recipient of the service" who "was not acting under the authority or the control of the service provider" if it "does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful" or "upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information".

3.5.12 ***Information location tools.*** This refers to the referral or linkage to an online location where third party material is accessible e.g. via a search engine. (See description of information location tools in paragraphs 3.2.3 to 3.2.5 above).

3.5.13 The Singapore Copyright Act[97], modeled on the US DMCA, protects "the network service provider referring or linking a user of any network to an online location on a network (referred to ... as the originating network), being a location at which an electronic copy of the material is made available, by the use of an information location tool such as a hyperlink or directory, or an information location service such as a search engine". The conditions for immunity are the same as those for content hosting. (See paragraph 3.5.10 above.) The legislative history of the DMCA explicitly recognises that constructive knowledge should not be imputed to a human compiled directory provider "simply because the provider viewed an infringing site during the course of assembling the directory" and only if information location tool providers turn a blind eye to "red flags" of obvious infringements will they not qualify for safe harbour.[98]

[95] The Copyright (Amendment) Bill (Bill No. 12 of 2005), introduced on 17 May 2005, amends section 193D(3) to widen the court's discretion to determine whether a network service provider should be treated as having the requisite knowledge.
[96] Electronic Commerce (EC Directive) Regulations 2002, regulation 19.
[97] (Cap.63) section 193D(1)(b).
[98] Esprit Project 27028, page 22, see footnote 38.

3.5.14 The European Directive however contains no provision on information location tools and instead placed this issue under a "re-examination procedure", i.e. the European Commission allows itself a period of 3 years following adoption of the EC Directive to re-evaluate the importance of addressing the scope of liability of information location tool providers and hyperlink providers. According to the Esprit report, the reason given is that Member States laws' (and courts) are unlikely to render information location tool providers liable for mere provision of links to infringing sites, as the lack of case law on this topic demonstrates. The Esprit report however points out that a review of copyright statutes, general liability rules, and recent case law may lead to a different conclusion.[99]

3.5.15 A number of European Member States have already included immunity for information location tools under their national laws.[100]

3.6 Obligation to Remove or Disable Material

3.6.1 As noted above, the immunities for the provision of caching,[101] hosting[102] and information location tool services[103] are conditional upon compliance with the obligation to remove or disable material in certain circumstances. These circumstances may relate to the service provider's knowledge of certain matters or receipt of notice in a specific form.

3.6.2 ***Obligation to takedown upon knowledge.***[104] Knowledge requirements vary according to the function being performed by the service provider. In the case of caching, the UK Regulations[105] require the service provider to remove content if it has actual knowledge that offending content has been removed at the original source, or access to it there has been disabled, or that such removal or disablement has been ordered by a court or administrative authority. In contrast, in

[99] Esprit Project 27028, page 22, see footnote 38.
[100] eg. Spain's 2001 draft Bill, Article 17, deals with linking in a manner similar to the DMCA. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[101] See paragraphs 3.5.6 to 3.5.8.
[102] See paragraph 3.5.10.
[103] See paragraph 3.5.13.
[104] The German working draft of 1 Dec 2000 adopted the "actual knowledge" or with regard to claims for damages "awareness of facts or circumstances" (constructive knowledge). *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[105] Electronic Commerce (EC Directive) Regulations 2002, regulation 17.

relation to hosting,[106] a service provider must remove content if it acquires actual knowledge of the unlawful activity or content and is aware of facts or circumstances from which the illegality of the activity or content should have been apparent. The obligation to remove, in this case, arises from actual knowledge as well as knowledge that the service provider ought to have known based on the facts or circumstances actually known to it (i.e. constructive knowledge). The UK Regulations have not prescribed procedures for takedown notices, relying instead on codes of conduct and the creation of voluntary measures, with the Department of Trade and Industry retaining an oversight role.

3.6.3 The scheme under the Singapore Copyright Act is modeled on the US DMCA regime. In the case of hosting and referral services, it imposes an obligation to takedown material upon actual or constructive knowledge (similar to the UK Regulations[107] in respect of hosting services) or upon prescribed notice under a takedown regime. In the case of caching, however, the service provider is not required to remove content unless it has received notice in the prescribed form[108] in the takedown regime.

3.6.4 One criticism of imposing a duty on service providers to remove or disable material upon acquiring knowledge is the "chilling effect" it has upon freedom of expression. Service providers "are likely to takedown material upon receipt of almost any type of notice, even if later that notice proves to have been unfounded, and they are likely to include provisions in their user's agreements permitting them to remove material at their discretion. Freedom of expression will thereby be controlled by host service providers and bulletin board operators who would understandably prefer to shut a site down or eliminate certain content than expose themselves to liability".[109]

3.6.5 The requirement to act "expeditiously" has also been criticised for being too vague. It is pointed out that service providers might need to take legal or other advice to determine whether they have "actual knowledge" of illegal activities or materials in some instances, e.g. in

[106] Electronic Commerce (EC Directive) Regulations 2002, regulation 19.
[107] Electronic Commerce (EC Directive) Regulations 2002.
[108] The Copyright (Amendment) Bill (Bill No. 12 of 2005) seeks to clarify that the notice may be "substantially in accordance with" the prescribed form.
[109] Esprit Project 27028, see footnote 38.

relation to defamation or confidentiality, difficult issues of law may arise which can only be determined with certainty by a court of law. In such cases, it may not be appropriate to expect a service provider to evaluate the validity of complaints in order to decide whether to comply with a notice to takedown certain material.[110]

3.6.6 In an attempt to address such criticism, the UK Regulations[111] provide guidance in determining when a service provider has actual knowledge via a non-exhaustive list of criteria. Although the UK Regulations do not adopt a prescribed notice and takedown regime, whether a service provider has received a notice in accordance with contact details provided by the service provider and the details given in such a notice are circumstances that are to be taken into account to determine if the service provider has actual knowledge.[112]

3.6.7 **Notice and takedown regime.** An alternative to the "knowledge approach" is to adopt a regime whereby service providers have no obligation to remove material unless and until they receive formal notice in a prescribed form requiring them to do so. This approach takes the guesswork out of determining whether and when service providers must takedown material.

[110] Norway consulted on 2 proposals. The first proposal limits liability for hosting services if the service provider expeditiously removes or blocks access to content if it (a) is made aware that the court or a public authority has prohibited the making of content (b) has been notified in accordance with the notice and takedown regime or (c) has actual knowledge that the content is illegal "under intellectual property, child pornography, or racism law". The proposal states there may be areas in respect of which it is inappropriate to apply a knowledge test as it involves difficult legal evaluations e.g. defamation, hence the proposed limitation to specified areas of law. The second alternative excludes the knowledge test. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.

[111] Electronic Commerce (EC Directive) Regulations 2002.

[112] Electronic Commerce (EC Directive) Regulations 2002, regulation 22.

"**Notice for the purposes of actual knowledge**

22. In determining whether a service provider has actual knowledge for the purposes of regulations 18(b)(v) and 19(a)(i), a court shall take into account all matters which appear to it in the particular circumstances to be relevant and, among other things, shall have regard to -

(a) whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c), and

(b) the extent to which any notice includes –

(i) the full name and address of the sender of the notice;

(ii) details of the location of the information in question; and

(iii) details of the unlawful nature of the activity or information in question."

3.6.8 There are various ways of implementing such an approach. Under the Singapore Copyright Act[113], service providers can be certain that they are protected by the "safe harbour" provisions so long as they comply with prescribed procedures under the takedown regime. The notices must be purportedly made by the owner of the copyright in the material or under his authority, state certain prescribed matters, and be given to the service provider's designated representative.[114]

3.6.9 This method is, however, still hotly debated internationally. One concern is it that service providers will not be adequately proactive in taking down unlawful material even though they may have actual knowledge of it. It may be considered appropriate in certain contexts, for public policy reasons, to impose obligations on service providers to exercise greater vigilance, e.g., in respect of certain types of material such as illegal pornographic material (especially child pornography) or hate speech.[115] It was suggested that Sweden did not implement the notice and takedown regime probably because of explicit concern that such a regime would limit the ways in which an intermediary can become aware of illegal material and take it down, and that a notice and take-down regime might be difficult to combine with their existing laws on criminal liability of electronic bulletin boards which imposes criminal liability on operators of electronic bulletin boards who intentionally or grossly negligently fail to takedown certain material.[116]

3.6.10 An opposing criticism is that service providers will be too quick to takedown material upon receipt of a notice as they will have no regard whether the notice is reasonably justified.

3.6.11 The takedown regime under the Singapore Copyright Act[117] attempts to balance these issues by requiring the service provider to expeditiously take reasonable steps to notify the person who made

[113] Modeled on the US DMCA.
[114] Norway and Sweden also adopt notice and takedown regimes modeled on the US DMCA provisions. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[115] Finland's draft proposal in 2001 required service providers to remove material on their own initiative upon obtaining knowledge in relation to certain criminal matters e.g. child pornography. *On the Service Provider Liability for Illegal Content* Sanna Heikkinen accessed at www.tml.hut.fi/Studies/T-110.501/papers/index.html on 27 Apr 2005. Also *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[116] *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[117] Modeled on the US DMCA provisions.

available the material and restore such material to the network (subject to technical and practical feasibility) if that person submits a counter notice in the prescribed form,[118] unless the owner of the copyright in the material has, before the restoration, commenced proceedings to prevent such restoration.

3.6.12 Another way of addressing the concern that takedown notices can be, and have been, made without proper justification is to have a centralised authority to evaluate and convey demands for material to be taken down to service providers.

3.6.13 In the area of child pornography, a non-governmental "quango", the Internet Watch Foundation[119], has existed in the UK since 1996 to provide a means by which the ISP industry as a whole can receive notice and directions as to whether allegedly illegal content complained about by the public should be taken down. This enables takedown requests to be scrutinised rather than possibly simply complied with by individual service providers lacking time and legal resources. It is also to some extent transparent, as statistics are issued about the types of complaints and action taken. On the other hand, the Rightswatch project funded by the EC from 2002-2003 failed to gain support because of a lack of consensus between the interests of the various stakeholders in the market. This has been suggested to be a "strong indication of the obstacles to agreement among stakeholders on voluntary NTD[120] regimes, absent statutory underpinnings".[121]

3.6.14 Other models somewhere between NTD[122] and a full court hearing are possible. In Belgium, takedown of content by an ISP must be authorized not by a full court but by a state prosecutor. In Italy and Spain, EC Directive-based regulations demand that "a competent body" determine the legality of disputed content. In the UK, the Publisher's Association, have proposed a scheme whereby as soon as "takedown" is opposed by the provider of the disputed content, the

[118] The Copyright (Amendment) Bill (Bill No. 12 of 2005) seeks to clarify that the notice may be "substantially in accordance with" the prescribed form.

[119] See http://www.iwf.org.uk, accessed on 17 May 2005. It has recently also begun to scrutinize racist and hate speech material.

[120] i.e. Notice to Takedown.

[121] *Online Intermediaries and Liability for Copyright Infringement*, p.32 – 34, see footnote 43.

[122] See footnote 120.

matter must mandatorily go to the courts and the content meanwhile remain in the public view.[123]

3.6.15 The Oxford PCMLP-IAPCODE[124] research identifies a number of essential requirements for a self regulatory dispute resolution system to work effectively and in the public interest in the digital media/content area. The Study recommends that such schemes should amongst other things, be beneficial to consumers; accessible to members of the public; independent from interference by interested parties; adequately funded and staffed; provide effective and credible sanctions; provide for auditing and review by the relevant independent regulatory authority; be publicly accountable; and provide for an independent appeals mechanism.[125] The Oxford research suggests[126] that the way forward may lie with codes of conduct developed by relevant industry bodies accredited by the relevant independent regulatory authority for that industry sector. [127]

3.6.16 **Takedown only in compliance with order of court or regulatory authority.** Another way is to leave the administration of such demands to a judicial or regulatory authority. In this case, the service provider only has to act in compliance with orders of the court or relevant authority. This approach provides certainty for the service provider and assurance that demands to takedown material are justified.

3.6.17 One possible consequence of limiting compliance to orders from a court or regulatory authority is that service providers would have no incentive to be proactive. The problems with placing obligations upon service providers to remove material proactively have, however, been pointed out above.

---

[123] *Online Intermediaries and Liability for Copyright Infringement*, p.32 – 34, see footnote 43. Article refers to oral presentation by Publishers Association representative, Not-Con, London, June 5, 2004.

[124] Oxford PCMLP-IAPCODE "Self regulation of digital media converging onto the Internet: Industry codes of conduct in sectoral analysis" available at http://pcmlp.socleg.ox.ac.uk/execsummary.pdf, accessed on 19 May 2005.

[125] Oxford PMCLP-IAPCODE, para 12.1, see footnote 124.

[126] Oxford PMCLP-IAPCODE, section 12: Watching the Watchdogs: Accreditation of Self-regulatory Codes and Institutions, see footnote 124.

[127] Referenced from *Online Intermediaries and Liability for Copyright Infringement*, p.32 – 34, see footnote 43.

3.6.18 Another consequence is that private parties will have to incur legal costs in seeking a court order against the service provider before such material will be removed. It seems justifiable that the service provider should not bear the cost of obtaining a court order since section 10 is intended to protect service providers from civil liability and the obligation to takedown arguably arises only when the service provider is aware of the court order. The party seeking removal of the material may, in any case, be able to recover the costs incurred from the party liable for providing the material. It remains to be seen how a Singapore court might decide such an issue. The considerations of the UK Court of Appeal in the case outlined in the next paragraph may be equally relevant to the situation where a service provider requires a court order before complying with a request to takedown third party material.

3.6.19 In an unreported decision (December 19, 2001) , which arose from proceedings in *Totalise v Motley Fool* [2001] EMLR 29, the UK Court of Appeal held that the party (a service provider) asked to disclose the identity of a user of its services should *not* have to meet the costs of the court order for disclosure if that party had a genuine doubt that the applicant was entitled to disclosure, and that they might be legally obliged not to disclose and could be subject to legal proceedings if they disclosed voluntarily (as was possible there since the disclosure breached the terms of the privacy policy).[128]

3.6.20 A regime requiring takedown only upon a court order or an order by a regulatory authority seems to work well. In the case of material that has to be taken down for reasons of public policy, it is appropriate that a responsible regulatory authority should be empowered to issue such orders as an executive authority is well-placed to decide issues of public policy. In the case of an assertion of private rights, it seems justifiable that the private party should initiate court proceedings to obtain a court order for the takedown of third party material and that the service provider should not have to bear the costs of obtaining the court where there is uncertainty as to the validity the private claim.

3.6.21 **The existing regime under section 10 of the ETA in effect follows this model.** The amendments discussed in paragraphs 3.4.1 to 3.4.14 above provide service providers with blanket immunity with respect to

[128] *Online Intermediaries and Liability for Copyright Infringement*, page 52, see footnote 43.

civil and criminal liability in respect of third party material. This immunity is, amongst others[129], subject to the obligations of a network service provider as such under a licensing or other regulatory regime established under any written law[130] e.g. the Class Licensing scheme, and any obligation imposed under any written law or by a court to remove, block or deny access to any material[131].

3.7 Protection for Removing or Disabling Content

3.7.1 The Singapore Copyright Act[132] provides that a service provider shall not be liable to any person in respect of any action taken by it in good faith in relation to the removal or disabling of access to, or removal of, material in reliance on a notice or knowledge referred to under that Act. This is subject to the requirement to notify the person who made available the material and other requirements relating to restoration of the material upon receipt of a counter notice. This protection applies whether or not it is ultimately determined that there was an infringement of copyright. Similar protection is provided in respect of restoration of material in accordance with a counter notice. Other jurisdictions with a notice to takedown regime also provide protection for service providers complying with the takedown regime.[133]

3.7.2 It has been suggested that Finnish law does not contain such a provision because under Finnish contract and tort law, it would be difficult to imagine a case where the service provider would be liable for complying with the law.[134]

3.7.3 Such a provision does not seem to be necessary in the case of section 10 of the ETA since compliance with obligations under the Class Licensing Scheme or a court order would not give rise to liability on the part of service providers.

[129] The other exceptions are obligations founded on contract and obligations under the Copyright Act: section 10(2)(a) and (d) respectively.
[130] ETA, section 10(2)(b)
[131] ETA, section 10(2)(c)
[132] Section 193DA, modeled on the US DMCA
[133] Under the Australian Act, Internet content hosts and ISPs have immunity from civil proceedings in respect of compliance with access-prevention notices and take-down notices respectively issued by the regulator. Broadcasting Services Act, 5th Schedule, s.84(2) and (3).
[134] *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.

3.8 Burden of Proof in Criminal Proceedings

3.8.1 The UK Regulations[135] provide that, where a service provider, charged with an offence in criminal proceedings arising from transmission, provision of access or storage of material relies on the defences in the regulations[136], the service provider only needs to adduce evidence sufficient to raise an issue with respect to that defence. The prosecution will then have to prove beyond reasonable doubt that the defence applies.

3.8.2 The Singapore Copyright Act similarly contains a provision requiring the court to presume, in the absence of evidence to the contrary, that the network service provider has complied with various conditions under the Act if the service provider adduces evidence to that effect.

3.8.3 Such provisions make it easier for a service provider to rely on the relevant defences by lessening the burden of proof on the service provider. **Such provision is however probably unnecessary in respect of defences claimed under section 10 of ETA since that provision is uncomplicated. It does not contain any of the additional conditions imposed by laws modeled upon the US DMCA[137] or EC Directive[138].**

3.9 Other Obligations

3.9.1 Various European countries have laws to aid the identification of anonymous or pseudonymous users who provide unlawful content. For example, French law requires service providers to keep records of the actual identity of customers to allow their identification.[139] Spanish law allows a court to request a service provider to monitor a specified recipient of the service and keep information regarding that person's activities, for a maximum of 6 months.[140] Luxembourg's law foresees the possibility for courts to require the monitoring of specific

[135] Electronic Commerce (EC Directive) Regulations 2002.
[136] i.e. regulations 17,18, or 19. See discussion above in paragraphs 3.5.4, 3.5.8 and 3.5.11.
[137] Singapore Copyright Act, see paragraphs 3.5.3, 3.5.7 and 3.5.9.
[138] E.g. the UK Regulations see paragraphs 3.5.4, 3.5.8 and 3.5.11.
[139] The French Freedom of Communications Act of 1986 as amended on 22 Aug 2000. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[140] Spanish draft Bill 2001 Article 11. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.

sites or general surveillance for periods of time when necessary for public order, the prevention and investigation of crime, public health and public safety or the safety of consumers[141]

3.9.2 Spanish law also imposes a duty to inform authorities upon gaining knowledge of existence of illegal activity.[142] Sweden has a law imposing criminal liability on operators of electronic bulletin boards who intentionally or grossly negligently fail to takedown certain material.[143]

3.9.3 The Singapore Copyright (Amendment) Bill 2005[144] seeks to amend the Copyright Act to clarify that the "safe harbour" provisions are not conditional on a service provider "monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with any standard technical measure" or "gaining access to, removing or disabling access to any electronic copy of any material in any case where such conduct is prohibited by law".[145]

3.10 Summary

3.10.1 The issues in considering an appropriate takedown regime may be summarized as follows:

> "It might usefully be asked what is desired – *post* publication removal or blocking of Internet content only on the demand of a properly empowered institution or court, thus respecting all legal defenses and the public interest; or some degree of cheap speedy restraint on illicit Internet content by the operation of NTD.[146] If we want the latter, can we introduce an element of public scrutiny more effective than the put-back rules of the DMCA? The issue here is really what body (if any) should adjudicate on notice and takedown - judicial or administrative, self-regulatory or with a more public constitutionalised role, industry funded or state funded, open or acting behind closed doors." [147]

[141] *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[142] Spanish draft Bill 2001 Article 11. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[143] *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[144] Bill No. 12 of 2005, introduced in Parliament on 16 May 2005.
[145] Proposed amendment to section 193A(3) of the Copyright Act.
[146] i.e. Notice to Takedown.
[147] *Online Intermediaries and Liability for Copyright Infringement*, footnote 43, page 32, see footnote 43.

3.10.2 The regime under section 10 of the ETA governs the civil and criminal liability of service providers in respect of third party materials, apart from liability under the Copyright Act and contractual obligations. [148] It seeks to provide service providers with certainty as to their liability. The obligation to remove or disable third party material may arise under a licensing or other regulatory regime established under any written law[149] e.g. the Class Licensing scheme, and obligations imposed under any written law or by a court to remove, block or deny access to any material[150].

3.10.3 **This regime requires takedown only upon a court order or order by an appropriate regulatory authority.** It has worked well. In the case of material that has to be taken down for reasons of public policy, the power to order material to be removed or disabled is vested in a regulatory authority[151]. In the case of an assertion of private rights, the matter is adjudicated by a court and the service provider is only required to act pursuant to a court order.

3.10.4 **Since section 10 does not impose conditions on service providers in order to benefit from immunity in respect of different functions, there is no need to categorise functions as in the Copyright Act and the EC Directive.** A self regulatory takedown regime would necessitate such categorisation since a network service provider's responsibility to takedown material would depend on what function it is performing.

Q9.	Should the immunity regime for service providers under section 10 of the ETA be changed (other than the changes mentioned in Q.6, 7 and 8)?

[148] Section 10(2)(d) and (a) respectively.
[149] ETA, section 10(2)(b)
[150] ETA, section 10(2)(c)
[151] Media Development Authority of Singapore in respect of the Class Licensing Scheme and Internet Code of Conduct.

PART 4
ELECTRONIC GOVERNMENT

4.1 The Government's electronic government initiative, e-Government Action Plan II (eGAP II), sets its core intent as delighting customers and connecting citizens. The goal is to serve the public best with infocommunications technology, in particular, by integrating services to deliver seamless and speedy service through single points of access.

4.2 Having achieved the target of providing practically all Government services online in eGAP I, the focus in eGap II is on integrating the delivery of such services through initiatives such as the Online Business Licensing Service, Integrated Trade and Logistics IT platform, National Electronic Payment Hub and Moving House Online. The new service delivery paradigm is 3P (public-private-people) Integration.[152]

4.3 The new paradigm, not surprisingly, gives rise to new legal ramifications. The integrated delivery of services means that the customer (by what seems to him to be a single transaction) is in fact carrying out multiple transactions. Such multiple transactions may involve dealings with one or more Government (or private) agencies governed under the same or different pieces of legislation.

4.4 This Part discusses changes to the ETA to facilitate further developments in e-Government. Although the existing law already contains various provisions relating to e-Government, in some respects it may not go far enough to harness the full potential of new technology to provide fully integrated services through single points of access. The proposed amendments to the ETA to facilitate e-Government are set out in **Annex B**.

4.5 The following issues are discussed in this Part:

- the use of electronic means in transactions with the Government, in particular electronic forms for the integrated delivery of Government services (Parts 4.7 and 4.8);

[152] Keynote Address by Acting Minister for Finance, Mr Raymond Lim at the e-Government Forum 2004 (28 October 2004), accessed at www.egov.gov.sg/e-Government+Forum+2004.htm.

- the involvement of intermediaries in the integrated delivery of Government services (Part 4.9);

- the retention of documents in electronic form (Part 4.10);

- the acceptance of electronic originals (Part 4.11); and

- other issues relating to the production of information in electronic form (Part 4.12).

The issues referred to in Parts 4.10 to 4.12 are not limited to government transactions, but encompass private transactions, as well. They are discussed here for convenience as they are, to a large extent, particularly relevant to government transactions.

4.6 Existing Law

4.6.1 The Legal Infrastructure for E-Government was harmonised and expanded in 1998 by the ETA which arose out of the recommendations of the Electronic Commerce Hotbed Study Group on Legal, Regulatory and Enforcement Issues[153]. The provisions of the **ETA** are generally applicable to Government transactions. Below, we highlight two provisions of the ETA which have particular relevance to e-Government.

4.6.2 **Section 47 of the ETA[154]** is the central provision that enables Government agencies[155] to adopt electronic means of carrying out

[153] The full text of the Study Group's report can be found at www.lawnet.com.sg (under Legal Workbench, Publications).

[154] Section 47 is set out below for ease of reference:

Acceptance of electronic filing and issue of documents

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

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

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

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

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

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

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

(iii) make such payment in electronic form.

government functions without the need to enact additional laws. It allows Government agencies to accept the filing, creation or retention of documents in the form of electronic records.

4.6.3 **Section 9 of the ETA[156]**, which allows electronic records to satisfy legal requirements for the retention of records, applies to

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

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

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

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

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

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

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

[155] By Government agencies, we mean to refer to any department or ministry of the Government, organ of state or statutory board.

[156] Section 9 is set out below for ease of reference:

Retention of electronic records

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

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

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

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

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

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

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

(4) Nothing in this section shall —

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

(b) preclude any department or ministry of the Government, organ of State or a statutory corporation from specifying additional requirements for the retention of electronic records

requirements for retention which are under the supervision of Government agencies, but only with the consent of such Government agency.

4.6.4 In addition, the **Interpretation Act**[157] has various provisions that facilitate the use of electronic means. First, it provides that authority to make subsidiary legislation includes the authority to provide for the manner and method in which any document, record, application, permit, approval or licence may be submitted, issued or served by electronic means, or for the authentication thereof.[158]

4.6.5 Second, the Interpretation Act also provides that authority to provide for fees and charges includes the authority to provide for the determination of the manner and method of payment. This includes payment by electronic means.[159]

---

that are subject to the jurisdiction of such department or ministry of the Government, organ of State or statutory corporation.

[157] Sections 2 (definition of "prescribed"), 7 and 20 are set out for ease of reference:

Interpretation of certain words and expressions

2.—(1) In this Act, and in every written law enacted before or after 28th December 1965, the following words and expressions shall, without prejudice to anything done prior to that date, have the meanings respectively assigned to them unless there is something in the subject or context inconsistent with such construction or unless it is therein otherwise expressly provided:

...

"prescribed" means prescribed by the Act in which the word occurs or by any subsidiary legislation made thereunder and, in relation to forms, includes being set out in electronic form on an electronically accessible server (such as an internet website) that is specified in the Act or subsidiary legislation in which the word occurs;

Forms

7. Except as is otherwise expressly provided, whenever forms are prescribed, slight deviations therefrom, not affecting the substance or calculated to mislead, shall not invalidate them.

Additional provisions as to subsidiary legislation

20. The following provisions shall also apply to subsidiary legislation:

(a) authority to make subsidiary legislation shall include —

.....

(iv) authority to provide for the manner and method in which any document, record, application, permit, approval or licence may be submitted, issued or served by electronic means, or for the authentication thereof;

(b) authority to provide for fees and charges shall include authority to provide for the determination of the manner and method of payment and the reduction, waiver or refund thereof, either generally or in any particular event or case or class of cases or in the discretion of any person; and

…..

[158] Cap.1, section 20(a)(iv). This sub-paragraph was added by the Electronic Transactions Act (Cap.88).

[159] Cap.1, section 20(b). The words "the determination of the manner and method of payment and" were added by the Statutes (Miscellaneous Amendments) Act 1997(Act 7 of 1997).

4.6.6 Third, the Interpretation Act enables forms that need to be prescribed to be set out in electronic form on an electronically accessible server (such as an internet website), instead of being published in the *Gazette*.[160]

4.6.7 The Interpretation Act further provides for the electronic *Gazette.* This enables subsidiary legislation[161] to be published electronically instead of in paper form.[162]

4.6.8 In addition, these provisions are supported by the computer output provisions in sections 35 and 36 of the **Evidence Act**[163] introduced in 1996 and bolstered by the **Computer Misuse Act**[164].

4.7 Prescribed Forms

4.7.1 The law often requires prescribed forms to be used for various transactions with Government agencies. In the past, such forms were typically intended to be completed and submitted in paper form. The layout and wording of the form would be published in the Act or subsidiary legislation prescribing the form.

4.7.2 The advent of electronic transactions brought with it the possibility of providing and accepting electronic forms. This might involve providing an electronic version of a form (e.g. by e-mail or on a website) for printing and submission in paper form. Alternatively, the form might be displayed onscreen via an online terminal or a website to allow input and submission to be done electronically.[165] There would usually be no difficulty in making the onscreen display correspond in appearance to the form prescribed by legislation. In

[160] Cap.1, definition of "prescribed" in section 2(1). Amendment made by the Statutes (Miscellaneous Amendments) Act 2003 (Act 9 of 2003).
[161] Subsidiary legislation includes rules, regulations, orders, notifications, by-laws or other instruments made under any Act, with legislative effect.
[162] Cap.1, definition of *"Gazette"* in section 2(1), read with section 2(6). Amendment made by the Electronic Transactions Act (Cap.88).
[163] Cap. 97.
[164] Cap. 50A.
[165] For example, e-filing of tax returns on the IRAS website or e-polling for HDB upgrading on terminals provided by HDB.

any case, slight deviations from prescribed forms, not affecting the substance or calculated to mislead, do not invalidate the forms.[166]

4.7.3 The law already supports such transactions. Government agencies that accept the filing of documents under written law are empowered to accept the filing of such documents in the form of electronic records.[167] The Government agency may, so long as it has a general power to make subsidiary legislation, make subsidiary legislation to provide for electronic submission, issue, service and authentication of documents.[168] Further, forms that need to be prescribed can also be set out in electronic form on an electronically accessible server (such as an internet website), instead of being published in the *Gazette*, provided that the Act or subsidiary legislation requiring the form to be prescribed specifies the server or website.[169]

4.7.4 One way of providing integrated services is to enable the user to perform multiple transactions from a single point of access. The law may require different prescribed forms to be submitted for different transactions. For convenience, the user should be able to input his relevant information just once instead of having to fill in the same information repeatedly in multiple forms. An input screen catering to such multiple transactions is unlikely to resemble any of the prescribed forms required for the different transactions. Nevertheless, by using technology at the backend, the information inputted by the user can be sorted and used to "populate" all the prescribed forms for the relevant transactions. The legal requirements for prescribed forms to be used for those transactions would therefore be satisfied.

4.7.5 However, there may not be any practical reason for "populating" the prescribed forms for individual transactions at the outset. Information in electronic form can be easily routed to the relevant authorities, who can then store such information in a database and view the information whenever they require and in whatever screen layout they prefer. When a user fills in a single composite electronic

[166] Interpretation Act (Cap.1) section 7.
[167] Electronic Transactions Act (Cap.88) section 47.
[168] Cap.1, section 20(a)(iv). This sub-paragraph was added by the Electronic Transactions Act (Cap.88).
[169] Cap.1, definition of "prescribed" in section 2(1). Amendment made by the Statutes (Miscellaneous Amendments) Act 2003 (Act 9 of 2003).

form in order to perform multiple transactions, the relevant information can be routed to the relevant authorities by technology at the backend.

4.7.6 Such composite electronic forms are unlikely to resemble the paper forms prescribed for the transactions performed. They can however be prescribed as an alternative means to the prescribed paper forms[170]. Since the electronic composite form is intended for use in different transactions, some portions of the form may elicit information for one transaction that is irrelevant to other transactions. The instructions on the form can clarify which portions need to be filled for particular transactions.

4.7.7 The provision in the Interpretation Act[171] that enables forms to be prescribed by setting out in electronic form on an electronically accessible server (such as an internet website) holds a solution. In reliance on this provision, legislation governing the relevant transactions can specify the server or website where the electronic composite form can be accessed. The electronic composite form would therefore be the prescribed electronic form for that transaction. Since such an electronic form is itself a "prescribed" form, it does not need to resemble any other prescribed paper forms.[172]

4.7.8 The existing law appears to provide adequately for the circumstances discussed above.[173] Nevertheless, proposed amendments to section

[170] See footnote 18.

[171] See footnote 18.

[172] There is therefore no need to rely on section 7 of the Interpretation Act.

[173] The Electronic Transactions Model Law prepared by the Commonwealth Expert Group on E-Commerce contains a provision that makes an electronic form equivalent to a prescribed non-electronic form provided 3 requirements are satisfied: s.8. The requirements are that the form must be (a) organised in the same or substantially the same way as the prescribed form, (b) accessible to the public authority so as to be usable for future reference and (c) capable of being retained by the person to whom it is given. The provision is subject to an overarching consent requirement: s.17. The Model Law also contains a provision on "Government uses" which is broadly similar to section 47 of the ETA: s.14.

We are of the view that a provision like that in the Commonwealth model law would not be useful in Singapore. This is because section 47 already enables the Government to use electronic forms in place of prescribed forms. The 3 requirements may be overly restrictive, for example in requiring that the electronic form must be organised in the same or substantially the same way as the prescribed form. In any case, the relevant public authority can adopt any of these requirements under section 47

The provisions of the Commonwealth Model Law referred to are set out below:

47 to facilitate the use of electronic records for a wide range of government functions will also apply to facilitate use of electronic forms. **Proposed section 47(3) provides that a requirement of written law for a document to be filed is satisfied by the transmission, in the manner specified by the Government agency, of an electronic record specified by the Government agency for that purpose.**[174] (See illustration on workings of proposed section 47(3) in paragraph 4.9.5.)

"**Prescribed forms**

8. A rule of law that requires a person to provide information in a prescribed non-electronic form to another person is satisfied by the provision of the information in an electronic form that is

(a) organised in the same or substantially the same way as the prescribed non-electronic form;

(b) accessible to the other person so as to be usable for subsequent reference; and

(c) capable of being retained by the other person."

"17. (1) Nothing in this Act requires a person to use, provide or accept information in electronic form without consent, but a person's consent to do so may be inferred from the person's conduct."

(2) Despite subsection (1), the consent of a public body [use of term also used in s. 14 for government] to accept information in electronic form may not be inferred from its conduct but must be expressed by communication accessible to the public or to those most likely to communicate with it for particular purposes."

"14.(1) If a public body has power to create, collect, receive, transfer, distribute, publish, issue or otherwise deal with information and documents, it has the power to do so electronically.

(2) Subsection (1) is subject to any rule of law that expressly prohibits the use of electronic means or expressly requires them to be used in specified ways.

(3) For purposes of subsection (2), a reference to writing or signature does not in itself constitute an express prohibition of the use of electronic means.

(4) Where the public body consents to receive any information in electronic form, it may specify:

(a) the manner and format in which the information shall be communicated to it;

(b) the type or method of electronic signature required, if any;

(c) control processes and procedures to ensure integrity, security and confidentiality of the information;

(d) any other attributes for the information that are currently specified for corresponding information on paper.

(5) The requirements of subsection 7(1) [requirement for writing satisfied by information in electronic form if accessible so as to be usable for subsequent reference] and subsection (3) [information in electronic form is not given unless the information is capable of being retained by the person to whom it is given] and section 8 [prescribed forms] also apply to information described in subsection (4).

(6) A public body may make or receive payment in electronic form by any manner specified by the public body [and approved by the responsible authority]."

Section 14(5) of the Model Law is intended to provide for subsections 7(1) and (3) [writing requirements] and section 8 [prescribed forms] to supplement any additional requirements specified by Government.

[174] See Annex B.

4.8 Non-documentary Information

4.8.1 Sometimes the law merely requires that information must be furnished to a Government agency without requiring it to be in documentary form e.g. information could be furnished orally.[175]

4.8.2 Currently, section 47(1)(a) of the ETA applies only to the filing, creation and retention of *documents*. It may be convenient to extend section 47 to legal requirements for information to be furnished to a Government agency.

4.8.3 Where a provision does not specify the form in which information is to be furnished, there is probably nothing to prevent the information from being furnished in electronic form e.g. via email. Nevertheless, by extending section 47 to such information, it will make it clear that section 47(2) applies so that the Government agency can make specifications concerning the acceptance of such information in electronic form. The Government agency, of course, has to consider whether any authentication of the sender of such information is necessary.

4.8.4 We propose to extend section 47 to apply to legal requirements for information to be furnished to Government agencies, whether in documentary or other form. For this purpose, we propose to insert the words "obtain information in any form" in section 47(1)(a). In addition, proposed section 47(3) provides that a requirement of written law for information in any form to be provided is satisfied by the transmission, in the manner specified by the Government agency, of an electronic record specified by the Government agency for that purpose.[176]

4.9 Intermediaries

4.9.1 Integrated transactions may be conducted via electronic systems that are administered by a party other than the Government agency responsible for administering the relevant transaction ("an

[175] E.g. the Money–Changing and Remittance Business Act (Cap.187) s.7 requires a person to submit an application for a licence to MAS and to furnish MAS with such information as they may require; the Sand and Granite Regulations (Cap.284, Rg1) requires submission of a written application and furnishing of information to the Licensing Officer.

[176] See draft amendments to section 47 in Annex B.

intermediary") and the intermediary may process the information submitted before transmitting it to the relevant Government agency. Especially where private sector services are integrated with the delivery of government services, the intermediaries may even be private bodies or businesses.

4.9.2 The relevant law may state that a person must submit documents or provide information *to a particular Government agency or officer*.[177] As such, there may be a doubt whether such legal requirements are satisfied by filling in an electronic form on an electronic portal run by another Government or private body.

4.9.3 Some legislation, such as the Sewerage and Drainage Act (Cap.294), anticipates this issue by providing for submission of plans to "such filing authority as the Director may designate".[178] This enables the use of a filing authority for the purposes of CORENET. However, most other laws do not have such a provision.

4.9.4 Proposed section 47(3) will ensure that a wide range of requirements under written law relating to Government transactions will be satisfied by the transmission, in the manner specified by the Government agency, of electronic records specified by the Government agency for that purpose. **If a Government agency specifies the submission of a specified record via a particular electronic system, proposed section 47(3) would ensure that an electronic record submitted in accordance with those specifications satisfies the requirements of law.**[179] **This would be effective notwithstanding that such electronic system is administered by an intermediary and that the intermediary processes the information submitted before transmitting it to the relevant Government agency.**

4.9.5 For example, if Law A requires paper Form A to be submitted to Agency A, and Law B requires paper Form B to be submitted to Agency B, both Agencies A and B can specify composite Form C

[177] E.g. the Money–Changing and Remittance Business Act (Cap.187) s.7 requires a person to submit an application for a licence to MAS and to furnish MAS with such information as they may require; the Sand and Granite Regulations (Cap.284, Rg1) requires submission of a written application and furnishing of information to the Licensing Officer.
[178] Section 33.
[179] See draft amendments to section 47 in Annex B.

(which is accessible on an integrated system operated by an intermediary T) for their respective transactions under Law A and B. When an applicant completes Form C and submits it via the integrated system, pursuant to section 47(3), he will satisfy the requirements of both Law A and Law B.[180]

4.9.6 We had earlier considered whether an additional provision specifically validating the use of intermediaries would be necessary for the purposes described in this Part.[181] We do not think that such provision would be necessary in view of the operation of proposed section 47(3).

4.10 Retention of Documents

4.10.1 Under some laws, Government agencies are empowered to require persons to retain certain documents, to be produced for inspection or reference if later required.[182]

4.10.2 Many businesses and individuals adopt the practice of converting their paper records into electronic form to reap the advantages of lower storage costs (since paper records are bulky and costly to store and manage). With the adoption of electronic filing systems, records are more and more commonly created and stored in electronic form

[180] The Online Application System for Integrated Services (OASIS), available through www.Business.gov.sg, provides advice on the licences and registrations necessary to set up a business, and enables applicants to make applications to different agencies online.

[181] **Integrated transaction systems**

47A. Section 47(3) and (4) shall, for the avoidance of doubt, also apply where an electronic record, or transaction (as the case may be) referred to in either of those subsections forms part of an integrated transaction system, notwithstanding that —

(a) more than one transaction is carried out with one or more Government agencies through the generation or transmission of a single electronic record;

(b) the transactions are governed by the same or different written laws; and

(c) the transaction is processed or routed, electronically or otherwise, through an intermediary.

[182] For example, under s 199 of the Companies Act, companies are obliged to retain their accounting and other financial records for a period of 7 years. Similarly, the Income Tax Act (Cap.134) s.67. Also Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap.65A), s.37, (Retention of records by financial institutions); Securities and Futures Act (Cap.289), s.102 (Keeping of books), s.131 (Register of securities); Goods and Services Tax Act (Cap.117A), s.44 (Giving of receipts); Singapore Tourism (Cess Collection) Act (Cap.305C), s.9; Prevention of Pollution of the Sea Act (Cap.243), s.13 (Regulations requiring the keeping of cargo record books); Financial Advisers Act (Cap.110) s.45 (Accounts to be kept by licensed financial advisers).

from the point of creation, and paper copies are only printed out when required for specific purposes.

4.10.3 It is important that legal requirements should not hamper businesses and individuals from adopting efficient and cost-saving technology for records management, unless there are good reasons for rejecting such means. The need to prevent fraudulent alteration of records may be a reason in some circumstances. However, it should be recognised that paper records may not necessarily be inherently safer since technology often provides adequate or superior means of preventing such fraud in the case of electronic records.[183] Another consideration is that electronic records are subject to the risk of technological obsolescence and may become inaccessible as a result of incompatibility of the storage format with later technology. It may therefore be appropriate to demand retention in paper form for records that will be required a long time into the future, especially if timely conversion of such records to ensure accessibility with later technology cannot be assured. Government agencies would also have to consider "downstream" issues, such as, how electronically retained records can subsequently be transmitted to the Government agency for inspection, whether a printout of the retained electronic records would suffice or whether the agency is prepared to go on-site to view the records.

4.10.4 Section 9 of the ETA provides that where a rule of law requires certain records to be retained[184], the requirement is satisfied by retaining them in the form of electronic records, subject to certain conditions as to accessibility, accuracy, details of its origin, destination and time of sending and receipt.[185] This provision applies both to Government and non-government transactions. However, in the case of Government transactions, the consent of the Government agency which has supervision over the requirement for the retention of such records must have been obtained.[186] The Government agency

[183] For example, via secure audit trails and access control. Forensic analyses required to detect paper forgery may be much more complicated.
[184] See footnote 182.
[185] These requirements, based on the UNCITRAL Model Law, are intended to replicate the purposes for which documents are reproduced to be retained.
[186] IRAS has guidelines on the "Keeping of Records in Imaging System" and "Keeping Machine Sensible Records and Electronic Invoicing" (see http://www.iras.gov.sg). Application for approval must be made in writing to the Comptroller.

may also specify any additional requirements for the retention of electronic records that are subject to the jurisdiction of the Government agency.[187]

4.10.5 In recognition of the trend towards the retention of records in electronic form, and the uncertainty caused by the requirement for prior consent from Government agencies to retain records in electronic form,[188] **we propose to amend the law to make it the default position that Government agencies will accept the electronic retention of documents.** We therefore propose to delete the requirement for consent in section 9(1)(d). With this amendment, the default position for Government agencies will be consistent with that for the private sector.

4.10.6 Government agencies will continue to be able to specify additional requirements for the retention of electronic records under their purview.[189]

4.10.7 To cater to situations where there are valid concerns regarding the appropriateness of electronic retention of documents for particular purposes, **Government agencies will be able to "opt-out" of the default position. Such opt-outs will be effected by publishing an order in the *Gazette* specifying the requirement of law and the documents, records or information to which section 9 shall not apply.[190]**

4.10.8 Government agencies should, in addition, give adequate publicity to their decision to exclude section 9 in respect of a requirement for the retention of certain documents. They could, for example, publish the fact on a publicly accessible central website (e.g. the Singapore Government Online portal[191]) or their own agency website or take

[187] Section 9(4) ETA.
[188] There have been industry complaints that many Government agencies when asked for consent for electronic retention, will either not comment or say vaguely and verbally (but not in writing) that they have no objection. This means that businesses cannot safely convert to electronic document management systems as they do not know whether they will fall foul of Government requirements later on.
[189] See Annex B, new section 9(1)(d) which is based on existing section 9(4)(b).
[190] See Annex B. Section 9(4)(b).
[191] www.gov.sg.

even more proactive steps to ensure that persons affected are aware of their requirements if necessary.

4.10.9 These amendments will enable businesses and individuals to confidently proceed to retain their records in electronic form, unless there is an order stating that section 9 does not apply to specified requirements of law in respect of specified documents, records or information.

4.10.10 We propose to retain both sections 9 and 47 although there would be some duplication in relation to the electronic retention of documents for Government purposes. These provisions should be allowed to work together since they address different aspects of the issue.

4.10.11 Section 9 is a general provision applying to both Government and private sector requirements. It stipulates requirements as to accessibility, accuracy and identification in relation to the retention of the documents.[192] It will apply to Government transactions unless the relevant Government agency has opted out of the provision.

4.10.12 We propose to retain the references to the retention of documents in section 47 for consistency with other Government functions governed by that provision. Since this is the principal section governing e-Government initiatives, it should, in our view, be as comprehensive as possible. Proposed section 47(3) applies where the Government agency has specified the documents and the manner of transmission. Section 47(1) deals with the flipside of the issue, that is, it is primarily concerned with empowering Government agencies to use electronic records for their functions, if they decide to do so. **We only propose a slight amendment to existing section 47(3)** [193] **to ensure that the default position with opt-out under section 9 will prevail.**

4.11 Originals

4.11.1 The law often requires the production of original documents to support applications to Government agencies. Government agencies

[192] These requirements, based on the UNCITRAL Model Law, are intended to replicate the purposes for which documents are reproduced to be retained.

[193] Existing section 47(3) will br renumbered as section 47(4). We propose to add the words "Subject to section 9 and 9A" at the beginning of the provision. See Annex B.

usually require original documents to be produced in order to verify certain information contained in that document. In most cases, the documents required pertain to Government records or certificates or licences issued by the Government. For example, one way of proving one's status for registration of citizenship by birth is to produce a birth certificate with the name of the child.[194] In other cases however, documents originating from other sources may be required. For example, a document duly authenticated to be the original document containing or recording testimony in a foreign court may be required for the purposes of extradition proceedings.[195]

4.11.2 In some situations, it may be convenient to accept an electronic copy of an original paper document. For example, the paper documents may be located in another country and the holder may not wish to let the document out of his possession.[196] The acceptance of electronic originals would cut down the need for face-to-face transactions to verify documents, thus paving the way for more Government services to be provided electronically from end-to-end.

4.11.3 As appropriate technology becomes available to safeguard the integrity of electronic documents, more and more organisations (governmental and non-governmental) are adopting electronic means of storing information and creating records. In such a case, there may no longer be a paper original since the record is created and stored in electronic form. It may be convenient for a Government agency requiring the production of original records to accept the production of such records in electronic form.

4.11.4 We envisage that in the future it may be less crucial for Government agencies to require paper originals for verification as Government agencies now frequently obtain information directly from source. For example, IRAS obtains pay information directly from certain employers, information on charitable donations to certain organisations is provided directly by the organisations, and information on dividend payments are obtained directly from the Central Depository.

[194] National Registration Act (Cap.201) section 12.
[195] Extradition Act (Cap.103) section 42(2).
[196] Indeed Canada was exploring the adoption of electronic imaging and transmission for immigration applications because often the applicants and their original documents are located outside Canada.

4.11.5 In this discussion, for convenience, we use the term "electronic originals" to refer to both electronic copies of paper originals as well as originals created in electronic form. The ETA currently does not contain any provision on the acceptance of electronic originals.

4.11.6 However, in some cases, such provision may not be necessary since the terms of the relevant provision of law imposing the requirement for the production of an original can already be read to admit originals created in electronic form.

4.11.7 In other cases, a piecemeal approach has been taken. Pursuant to the existing legislative framework which enables provisions to be made for the acceptance and authentication of documents by subsidiary legislation,[197] necessary legislative provisions have been made in Singapore as particular agencies adopt new electronic processes to facilitate the production of documents by electronic means.

4.11.8 Section 47 does not currently extend to the acceptance of original documents in electronic form.[198] In order to provide a more comprehensive framework, **we propose to amend section 47 to allow Government agencies to accept electronic originals.**

4.11.9 In Part 5.11, we discuss the adoption of a general provision on originals[199]. In addition, we discuss in Part 4.12 other issues related to achieving functional equivalence between the production of information in electronic form and conventional means, which apply to both government and private transactions.

4.12 General

Multiple specific provisions?

4.12.1 A survey of other jurisdictions indicates that they have adopted provisions relating to the production and retention of documents and

[197] ETA s.47 and Interpretation Act s.20.
[198] Although the reference to the "filing of documents" in section 47 could possibly include originals in some circumstances, it would probably not extend to the production of originals for on-the-spot verification. Speaking of "filing" of electronic originals raises complications since transmission of the "original" to the Government agency's computer system would actually involve the transmission of a copy.
[199] See proposed section 9A in Annex B.

information in various ways. Some jurisdictions have followed the UNCITRAL formulation fairly closely. For example, Canada and Ireland have both the provision on electronic originals and the provision on retention of documents.[200] However, in addition, Canada also has provisions on providing information in writing[201] and in specific form[202].

4.12.2 The Australian Commonwealth has not adopted any provision on originals as such. The "production of documents" was thought to be a more appropriate term because the concept of an original document is not used in their laws.[203] Instead, their law contains a number of provisions dealing with specific situations in which documents are required to be retained or produced, namely: requirements for the production of documents in paper or similar form[204], recording of information in writing[205], retention of written documents[206], and retention of electronic communications[207].

4.12.3 New Zealand has a similar approach to Australia. Their law deals specifically with legal requirements to record information in writing[208], to give information in writing[209], to retain documents or information that is in paper or non-electronic form[210], to retain information that is in electronic form[211], to produce information that is in paper or non-electronic form[212], to produce information that is in electronic form[213], to provide access to information that is in non-electronic form[214], to provide access to information that is in

[200] Canadian Uniform Electronic Commerce Act ss. 11 and 13, and Irish Electronic Commerce Act 2000 ss.17 and 18.
[201] Canadian Uniform Electronic Commerce Act s. 8
[202] Canadian Uniform Electronic Commerce Act s. 9
[203] Revised Explanatory Memorandum on the Electronic Transactions Bill 1999 accessed at http://scaleplus.law.gov.au/html/ems/0/1999/0/0642410364.htm.
[204] Australian Commonwealth Electronic Transactions Act 1999 s.11.
[205] Australian Commonwealth Electronic Transactions Act 1999 s.12(1).
[206] Australian Commonwealth Electronic Transactions Act 1999 s.12(2) and (3).
[207] Australian Commonwealth Electronic Transactions Act 1999 s.12(4) and (5).
[208] New Zealand Electronic Transactions Act 2002 s.19.
[209] New Zealand Electronic Transactions Act 2002 s.20.
[210] New Zealand Electronic Transactions Act 2002 s.25.
[211] New Zealand Electronic Transactions Act 2002 s.26.
[212] New Zealand Electronic Transactions Act 2002 s.28.
[213] New Zealand Electronic Transactions Act 2002 s.29.
[214] New Zealand Electronic Transactions Act 2002 s.30.

electronic form[215] and to compare a document with an original document.[216]

4.12.4 The Australian and New Zealand laws deal with each kind of transaction separately and with specificity. Their approach highlights the fact that articles 8 and 10 of the UNCITRAL Model Law[217] cover a wide range of transactions and there is some overlap between the kinds of transactions that these articles apply to.

4.12.5 Some Singapore laws expressly refer to the requirement to produce "original" documents.[218] Other laws may simply require that a certain document be produced. Although the word "original" may not have been used, it may be clear from the context that a particular document is required and not a mere copy of it. Therefore section 9 (on retention of documents) and a provision on originals based on the UNCITRAL Model (if adopted) could apply simultaneously to the same transaction and document.

4.12.6 Such overlap may give rise to confusion if the two provisions have inconsistent criteria for the acceptance of information in electronic form. Further, inconsistencies as to whether consent is required from the party to whom the document is to be produced or for whom the document is retained could be problematic.[219]

4.12.7 **We therefore propose that, whether there is a single provision on originals or a number of specific provisions on different situations in which electronic communications are used, the requirements as to consent or opting out and compliance with additional technical requirements should be consistent across**

[215] New Zealand Electronic Transactions Act 2002 s.31.
[216] New Zealand Electronic Transactions Act 2002 s.32.
[217] i.e. respectively relating to originals and retention of documents, on which our proposed section 9A and our existing section 9 are based.
[218] E.g. Insurance (Accounts and Statements) Regulations 2004 requires lodgment of an "original" actuary's report with the Monetary Authority of Singapore (regulation 11); Moneylenders Rules requires moneylenders to keep "in a file in which he shall place in consecutive order the original memoranda of all loans made by him in that year" (rule 12); Land Surveyors Rules require the submission of "original" field notes, calculations and plans by examination candidates (rule 12). Originals are also widely required in relation to evidence and procedure in court proceedings. We do not deal with issues of evidence and procedure in court proceedings as these are specifically dealt with under the Evidence Act and Rules of Court (in connection with the electronic filing system).
[219] See further paragraphs 4.12.10 to 4.12.16 on requirements for consent in relation to provisions on production and retention of documents and originals.

such provisions. This is why proposed section 9A of the ETA adopts provisions on opting out and compliance with technical requirements that mirror the proposed amendments to section 9 of the ETA.[220]

4.12.8 **In the Singapore context, it may not be necessary to have multiple provisions dealing specifically with each kind of transaction.** This is because section 47 of the ETA already provides comprehensively for Government agencies to accept electronic means of carrying out its functions. Proposed section 47(3) ensures that the use of electronic means specified by Government agencies to carry out such transactions satisfies the legal requirements for such transactions.[221] As earlier noted, most legal requirements on the production or retention of documents or information relate to Government transactions. With the exclusion of negotiable instruments, documents of title and land transactions, there are probably no such legal requirements that apply between private parties.

4.12.9 **To minimise repetition and overlap between the provisions of the ETA, we propose to adopt a single provision on electronic originals instead of many separate provisions to cater to the different situations in which electronic communications are used.** However, we propose to adopt the provision on electronic originals despite the overlap with sections 9 and 47 for the reasons discussed in this Part.

Consent and additional technical requirements

4.12.10 Most of the jurisdictions surveyed expressly provide that their electronic transactions laws do not compel anyone to use or accept electronic technology without their consent, though consent may be inferred from conduct.[222] Such consent may be given subject to conditions regarding the form of the information or the means by

[220] See Annex B. Proposed sections 9A(1)(c) and 9(4) mirror section 9(1)(d) and 9(4)(b) respectively.
[221] See discussion in Part 1.4.
[222] Canadian Uniform Electronic Commerce Act s.5, Irish Electronic Commerce Act 2000 s.24 and New Zealand Electronic Transactions Act 2002 s.16. The Australian Commonwealth Electronic Transactions Act 1999 does not have a general consent provision, but there are consent requirements in each section in Division 2 of Part 2 of the Act, except section 12 (relating to retention).

which the information is produced, sent, received, processed, stored or displayed.[223]

4.12.11 The position with regard to acceptance of information in electronic form by the Government differs from jurisdiction to jurisdiction. The Australian Commonwealth requires Commonwealth entities to accept electronic communications, except in the case of transactions that have been specifically excluded by the legislation.[224] New Zealand requires consent to accept the electronic form to be obtained in relation to legal requirements to give information in writing[225] and to produce[226] or provide access[227] to information that is in paper or other non-electronic form.

4.12.12 On the other hand, the provisions on retention of documents or information in the jurisdictions surveyed, except Ireland, do not contain any requirement for the consent of the person for whom they are retained.[228] Perhaps it is thought that it is sufficient for the requirement for consent to come into play only when the information retained has to be produced to another party.[229] The New Zealand provision on the legal requirement to compare a document with an original document[230] also does not contain any provision on consent.

4.12.13 In addition to the requirement for consent to accept electronic communications, any additional technical requirements of Government agencies accepting such communications must also be complied with.[231] Section 16 of the New Zealand Act applies this without distinction between Government and non-Government bodies.[232]

[223] New Zealand Electronic Transactions Act 2002 s.16.
[224] Australian Commonwealth Electronic Transactions Act 1999 s.11.
[225] New Zealand Electronic Transactions Act 2002 Section 20
[226] New Zealand Electronic Transactions Act 2002 Section 27
[227] New Zealand Electronic Transactions Act 2002 Section 30
[228] Canadian Uniform Electronic Commerce Act s.13, New Zealand Electronic Transactions Act 2002 s.16, Australian Commonwealth Electronic Transactions Act 1999 s.12 c.f Irish Electronic Commerce Act 2000 s.18.
[229] i.e. the consent requirements in one of the provisions on production of documents will then apply.
[230] Section 32.
[231] Canadian Uniform Electronic Commerce Act s.8, 9 and 11, Irish Electronic Commerce Act 2000 s.17 and 18, and Australian Commonwealth Electronic Transactions Act 1999 s.11. Section 16 of the New Zealand Electronic Transactions Act 2002 applies this to provision without distinction between Government and non-Government bodies.
[232] New Zealand Electronic Transactions Act 2002.

4.12.14 We have proposed to amend section 9 to provide that, as a default position, Government agencies will accept the retention of documents in electronic form unless the requirement for retention of that document has been expressly excluded by order published in the *Gazette*. [233] This is intended to give greater certainty to individuals and businesses seeking to convert their paper records into electronic form.

4.12.15 Bearing in mind the difficulties that may be encountered as a result of inconsistent consent requirements, **we propose to adopt a similar opt-out provision[234] in relation to the provision on electronic originals (or, if specific provisions on different situations in which electronic communications may be used are preferred, in relation to each of those provisions)**. This requirement for Government agencies to opt-out is similar in approach to that in Australia.[235]

4.12.16 Existing section 9 of the ETA (on retention of electronic records) contains a provision requiring compliance with any additional requirements specified by the Government agency with purview over the retention requirement.[236] We proposed to retain this provision with modifications.[237] **We propose to adopt a similar provision on compliance with technical requirements of the relevant Government agency in the provision on electronic originals (or if specific provisions on different situations in which electronic communications may be used are preferred, in relation to each of those provisions).[238]**

4.13 The adoption of provisions for functional equivalence in relation to the production of information in electronic form raises various issues:

Q10. Do you have any comments on the proposed amendments to section 9 of the ETA in Annex B?

[233] See proposed section 9(4)(b) in Annex B and Part 4.10.
[234] See footnote 233.
[235] See proposed section 9A(4) in Annex B.
[236] Existing section 9(4)(b) of the ETA.
[237] Part 4.10. See proposed section 9(1)(d) in Annex B.
[238] Part 4.11. See proposed section 9A(1)(c) in Annex B.

Q11. Do you have any comments on the proposed amendments to section 47 of the ETA in Annex B?

Q12. Should Singapore adopt a single provision on electronic originals or provide specifically for different situations in which electronic communications may be used as a functional equivalent of paper or other non-electronic forms?[239] (See paragraphs 4.12.1 to 4.12.9, especially paragraphs 4.12.8 and 4.12.9).

Q13. Should consent to accept electronic originals be required? In this respect, should there be any distinction between Government agencies and private persons or entities, and if yes, what differences should there be? For example, should Government agencies be presumed to accept electronic originals unless they have opted out of doing so, as proposed in section 9A(4) in Annex B? Would your views differ if, instead of a single provision on electronic originals, there are specific provisions on the use of electronic communications in different situations? (See paragraphs 4.12.10 to 4.12.12).

Q14. Proposed sections 9 and 9A of the ETA[240] require compliance with any additional technical requirements as to form and procedure that Government agencies may have in relation to the acceptance of electronic originals. Should there be express requirements to comply with such additional technical requirements in the case where the intended recipient of electronic originals is not a Government agency? Would your views differ if, instead of a single provision on electronic originals, there are specific provisions on the use of electronic communications in different situations? (See paragraphs 4.12.13 to 4.12.16)

[239] See Australian Commonwealth Electronic Transactions Act 1999 and New Zealand Electronic Transactions Act 2002. Also Canadian Uniform Electronic Commerce Act.
[240] See draft sections 9(1)(d) and 9A(1)(c) in Annex B.

PART 5
UNCITRAL ELECTRONIC CONTRACTS CONVENTION AND RELATED ISSUES

5.1 The draft UNCITRAL Convention on the Use of Electronic Communications in International Contracts (the Convention)[241], is expected to be considered and possibly finalised by UNCITRAL at its 38th session scheduled to be held in Vienna from 4 to 15 July 2005. The draft Convention is available on the UNCITRAL website at www.uncitral.org. The Convention is intended to govern international commercial contracts.[242]

5.2 If the Convention is widely adopted by other countries, it will set an international standard. In view of Singapore's trading interests, it would be in Singapore's interest to have laws which are consistent with such international standards.

5.3 If Singapore accedes to the Convention, it is likely that same regime applicable under the Convention will be adopted for all contractual transactions whether local or international. The Electronic Transactions Act will therefore have to be amended for consistency with the provisions of the Convention. This is because it would be confusing to have 2 separate legal regimes for local and international contracts, especially since it is often difficult to determine in the case of electronic transactions whether one is contracting with a local or foreign party.

---

[241] The draft Convention and related documents are available at the UNCITRAL website (www.uncitral.org), under Working Group IV. The current version of the draft Convention is A/CN.9/571.

[242] Article 1(1) provides that the Convention applies "to the use of electronic communications in connection with the formation or performance of a contract [or agreement] between parties whose places of business are in different States". The word "formation" is to be interpreted widely to include all contracting stages, including negotiations and invitations to make offers. A/CN.9/571, paragraph 15.

Article 2(1) excludes certain types of transactions, in particular:

> "(a) Contracts concluded for personal, family or household purposes;
>
> (b) (i) Transactions on a regulated exchange, (ii) foreign exchange transactions; (iii) inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments; (iv) 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."

Article 2(2) excludes application to "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".

5.4 In Stage I of the *Joint IDA-AGC Public Consultation on the Review of the Electronic Transactions Act: Electronic Contracting Issues* (LRRD No.1/2004),[243] conducted in February to April 2004, we had highlighted the main changes and issues which would arise in relation to electronic contracting if the provisions of the draft Convention (as it then stood)[244] were to be adopted. Since then, the UNCITRAL Working Group has met twice[245] to continue its work on the Convention and the draft of the Convention has undergone various modifications.

5.5 In this Part, we will highlight the changes that have been made to the draft Convention and discuss the implications of those changes for electronic contracts. This Part also discusses issues that may arise from the adoption of the Convention provisions in the ETA. It is necessary to consider to what extent it would be appropriate to apply the provisions of the Convention, which is restricted in its application to the context of international contracts, to domestic contracts and non-contractual transactions[246].

5.6 The following topics are discussed in this Part:

- Consent and Variation (Part 5.7)
- Legal Recognition of Electronic Communications (Part 5.8)
- Writing Requirement (Part 5.9)
- Electronic Signatures (Part 5.10)
- Provision of Originals (Part 5.11)
- Time and Place of Despatch and Receipt (Part 5.12)
- Invitation to Make Offers (Part 5.13)
- Automated Message Systems (Part 5.14)
- Error in Electronic Communications (Part 5.15)
- Applicability of the Convention (Part 5.16)

5.7 Consent and Variation

5.7.1 Article 3 of the draft UNCITRAL Convention provides that "parties may exclude the application of the Convention or derogate from or

[243] Available on the AGC website (www.agc.gov.sg), under Publications.
[244] A/CN.9/WG.IV/WP.103.
[245] 43rd session (New York, 15-19 March 2004), 44th session (Vienna, 11-22 October 2004).
[246] e.g. Government transactions.

vary the effect of any of its provisions". Article 8(2) provides that "nothing in the 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". There has been no change to these provisions of the Convention. These provisions preserve party autonomy in relation to contracts to which the Convention applies.

5.7.2 In LRRD No.1/2004[247], we explored whether to adopt a consent provision in the ETA based on article 8(2). We also noted that section 5 of the ETA provides for variation by agreement of any provision of Part II[248] or IV[249] of the ETA and considered whether to amend or replace the provision in view of overlap with other provisions making specific sections apply subject to agreement otherwise and the need for mandatory requirements which should not be open to variation by agreement of parties, and also whether a variation provision would be necessary if there is a consent provision.

5.7.3 All of the respondents[250] agreed that parties should generally have the freedom not to use electronic means to contract. The majority of respondents felt that an express provision would help to clarify this point. Two respondents however were of the view that the common law already provides adequately for this. Under the common law, a party need not accept a contractual offer if he does not consent to it. The common law, it was pointed out, has a detailed system of rules and standards[251] to ensure consent.

5.7.4 The respondents[252] also generally agreed that parties should not be permitted to adopt standards that are lower than the minimum requirements for the legal recognition of electronic communications

[247] Consultation Paper for Stage 1 of the *Joint IDA-AGC Public Consultation on Review of the Electronic Transactions Act: Electronic Contracting Issues*, Part 2.1.
[248] On Electronic Records and Signatures generally and, in particular, containing provisions on the legal recognition of electronic records, the requirement for writing, electronic signatures, and the retention of electronic records.
[249] On Electronic Contracts and, in particular, regarding the formation and validity of contracts, effectiveness between parties, attribution, acknowledgment of receipt and time and place of dispatch and receipt.
[250] To the Stage 1 Consultation Paper. See footnote 247.
[251] e.g. rules relating to consent, intention to create legal relations, mistake, etc.
[252] See footnote 250.

in the ETA[253] and other rules of law. One respondent however cautioned that the requirements of such minimum standards should be made clear.

5.7.5 The prevailing view within the UNCITRAL Working Group was that the right of a party to derogate from the application of the draft Convention should not be restricted. It was noted that the draft Convention was only intended to provide functional equivalence in order to meet general form requirements and that it did not affect mandatory rules that required, for instance, the use of specific methods of authentication in a particular context.[254]

5.7.6 As the ETA extends beyond contracts to include other transactions**,** it is necessary to consider whether consent and variation provisions should extend to other transactions.[255]

5.8 Legal Recognition of Electronic Communications

5.8.1 Article 8 provides for the legal recognition of electronic communications as follows:

> "1. 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.".

5.8.2 This provision, read with the definitions of "communication"[256] and "electronic communication"[257] cover both (a) contracts formed by the exchange of electronic communications and (b) the general use of electronic means to convey a statement, declaration, demand, notice or request in connection with a contract.

[253] e.g. conditions applicable to the retention of electronic records under section 9 of the ETA. (See discussion in Part 4.10.) Also proposed section 9A on provision of originals. (See discussion in Part 4.11.) c.f. the reliability requirement discussed in Part 5.10.
[254] A/CN.9/571, paragraph 76.
[255] See discussion on consent in relation to section 9 (retention of electronic records) and proposed section 9A (Provision of originals) in Part 4, paragraphs 4.12.10 to 4.12.16.
[256] "communication" means any statement, declaration, demand, notice or request, including an offer and acceptance of an offer, that the parties are required to make in connection with the formation or performance of a contract.
[257] "electronic communication" means any communication that the parties make by means of data messages.

5.8.3 This provision is consistent with both sections 6 and 12 of the ETA. In LRRD No.1/2004,[258] we consulted on whether references to "declaration, demand, notice or request" should be added to section 12 of the ETA for consistency. The majority of respondents felt that this would be useful for clarity. Some respondents however felt it was unnecessary as "declaration of intent or other statement" covers all of the listed documents. **On balance, we do not think that any amendment is required to sections 6 and 12 of the ETA.**

5.9 Writing Requirement

5.9.1 Article 9 provides for electronic communications to satisfy legal requirements for writing as follows:

> "1. Nothing in this Convention requires a communication or a contract to be made or evidenced in any particular form.
>
> 2. Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.".

5.9.2 The words "the law" in the provision has the same meaning as in corresponding provisions of the UNCITRAL Model Law on Electronic Commerce and refer to rules based on statute, regulation or judicial precedent.[259]

5.9.3 This provision is consistent with section 7 of the ETA.

5.10 Electronic Signatures

5.10.1 In LRRD No.1/2004[260] we noted that the provision on the recognition of electronic signatures in article 9 of the draft UNCITRAL Convention (as it then stood)[261] included 2 variants. Variant A was based on article 7 of the UNCITRAL Model Law on

[258] See footnote 247
[259] A/CN.9/571, paragraph 125.
[260] See footnote 247
[261] A/CN.9/WG.IV/WP.103.

Electronic Commerce, while variant B was based on article 6, paragraph 3 of the UNCITRAL Model Law on Electronic Signatures.[262]

5.10.2 The Working Group decided in favour of retaining variant A only.[263] Paragraphs 4 and 5 of article 9[264] have been deleted. Article 9(3) of the draft Convention now provides for electronic signatures as follows:

> "3. Where the law requires that a communication or a contract[265] 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[266] if:
>
> (a) A method is used to identify the party and to indicate that party's approval of the information contained in the electronic communication; and
>
> (b) That method is as reliable as appropriate to the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement.".

[262] A/CN.9/546, paragraph 48, see footnote 241.
[263] A/CN.9/546, paragraph 54-57, see footnote 241.
[264] Article 9(4) and (5) of the draft UNCITRAL Convention (from the 49th session of Working Group IV), based on article 6 of the Model Law on Electronic Signatures , read as follows:

"4. An electronic signature is considered to be reliable for the purposes of satisfying the requirements referred to in paragraph 3 of this article if:
(a) The signature creation data are, within the context in which they are used, linked to the signatory and no other person;
(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
(d) Where the purpose of the legal requirement for a signature is to provide assurances as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
5. Paragraph 4 of this article does not limit the ability of any person:
(a) To establish in any other way, for the purposes of satisfying the requirement referred to in paragraph 3 of this article, the reliability of an electronic signature;
(b) To adduce evidence of the non-reliability of an electronic signature.".

[265] The words "declaration, demand, notice or request that the parties are required to make or choose to make in connection with a contract" have been deleted. See paragraph 5.8.2.
[266] Reference to "data massage" has been replaced by "electronic communication".

Definition of electronic signature

5.10.3 Article 9(3)(a) of the draft Convention lays down general criteria for functional equivalence between handwritten signatures and electronic signatures.[267] Article 9(3)(a) defines an electronic signature as "a method ... used to identify the party *and* to indicate that party's approval of the information contained in the electronic communication" (italics added). This conjunctive requirement may be read to mean that only an electronic signature that fulfils both the function of identification of the party *as well as* the function of indicating that party's approval of the information contained in the electronic communication meets that legal requirement of a signature in relation to an electronic communication.[268]

5.10.4 There may be instances where the law requires a signature that does not fulfil the function of indicating the signing party's approval of the information contained in the electronic communication. For example, in the case of requirements of law for notarisation of a document by a notary or attestation by a commissioner for oath, it is not the intention of the law to require the notary or commissioner, by signing, to indicate his approval of the information contained in the electronic communication. The signature of the notary or commissioner merely identifies the notary or commissioner, and associates the notary or commissioner with the contents of the document, but does not indicate the approval by the notary or commissioner of the information contained in the document. Similarly, laws may require the execution of a document to be

[267] Paragraph 3(a) of article 9 is based on article 7, paragraph 1(a) of the UNICTRAL Model Law on Electronic Commerce 1996. Article 7 of the UNCITRAL Model Law on Electronic Commerce states:

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

[268] It should be noted that under paragraph 3 of article 9, which originated from article 7, paragraph 1 of the UNCITRAL Model Law on Electronic Commerce, the mere signing of an electronic communication by means of a functional equivalent of a handwritten signature is not intended, in and of itself, to confer legal validity on the data message. Whether an electronic communication that fulfilled the requirement of a signature has legal validity is to be settled under the law applicable outside the draft convention. See paragraph 61 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996).

witnessed by a witness, who is required to append his signature to that document. The signature of the witness merely identifies the witness and associates the witness with the contents of the document witnessed, but does not indicate the approval by the witness of the information contained in the document. In each of the examples above, the notary or commissioner and the witness, by signing, can at most be said to "approve" the words in the *jurat*[269] and not all the information contained in the document.

5.10.5 By contrast, "electronic signature" is defined in the ETA as "any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating[270] *or* approving the electronic record" (italics added). The use of the word "or" makes the stated functions of the signature disjunctive. Therefore, the definition recognises electronic signatures that fulfill only one of the functions, even if it does not fulfill both of the functions, e.g. an electronic signature that authenticates the electronic record but does not indicate approval of the electronic record.

5.10.6 As article 9(3)(a) may prevent electronic signatures that are not intended to fulfill the function of indicating the signor's approval of the information contained in the electronic communication to satisfy a requirement of law for a signature, Singapore has submitted a comment to the UNCITRAL Secretariat requesting UNCITRAL to consider amending article 9(3)(a) to recognise that electronic signatures are sometimes required by law only for the purpose of identifying the person signing ("the signor") and associating the information with the signor, but not necessarily to indicate the signor's "approval" of the information contained in the electronic communication. The full text of the comment submitted to UNCITRAL is set out at Annex C.

[269] i.e. a memorandum usually appearing in legal documents above the signature of the notary, commissioner or witness, stating that that notary, commissioner or witness witnessed the signor of the document append his signature to the document.

[270] Although there is no explicit reference to the "identification" function in the definition, it is implicit in the definition.

Q15. Do you agree that the definition of an electronic signature should not require such a signature to fulfill both an identification as well as an approval function?

Reliability requirement

5.10.7 Article 9(3)(b) of the draft Convention contains a requirement that the method of signing must be "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" in order for the electronic signature to be legally valid.

5.10.8 This means that the parties to the electronic communication or contract are not able to know with certainty *ex ante*[271] whether the electronic signature used will be upheld by a court or other trier of fact as "appropriately reliable" and therefore not be denied legal validity, until after a legal dispute arises subsequently. It also means that even if there was *no dispute* about the identity of the person signing or the fact of signing (i.e. no dispute as to authenticity of the electronic signature), a court or trier of fact may still rule that the electronic signature was not appropriately reliable, and therefore invalidate the entire contract.

5.10.9 Such a provision will potentially have serious practical implications for electronic commerce:

(a) It will create uncertainty in electronic transactions because whether a signature method is appropriately reliable and hence not be denied legal validity will be determined *ex post*[272] by the court or trier of fact, and not *ex ante* by the parties. Although parties can exercise party autonomy by agreeing on a signature method, it remains that the parties' agreement is only one of the factors taken into consideration by the court or trier of fact.[273] Even if the parties were satisfied at the outset as to the reliability

[271] i.e. at the outset e.g. when signing.
[272] i.e. after the event
[273] This was explicitly noted at paragraph 60 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996), which states, "However, a possible agreement between originators and addressees of data messages as to the use of a method of authentication is not conclusive evidence of whether that method is reliable or not."

of the signature method, a court or trier of fact may rule otherwise.

(b) It could be used to the detriment of the very class of persons that the legal requirements for signature are intended to protect. A party could try to invalidate his own electronic signature as being insufficiently reliable, in order to invalidate a contract, where it is convenient to him. This would be to the detriment of the other party relying on the signor's signature. This provision then risks becoming a trap for the unwary or a loophole for the unscrupulous.

(c) It may be an impediment to electronic commerce. It will add to business costs if users feel compelled to use more sophisticated and costly technology to ensure that the reliability requirement is satisfied. Conversely, such uncertainty and additional costs may even discourage the use of electronic transactions.

5.10.10 This "reliability requirement" has its origins in article 7, paragraph 1(b) of the UNCITRAL Model Law on Electronic Commerce 1996. In the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 2001, it was noted that article 7 of the UNCITRAL Model Law on Electronic Commerce creates uncertainty as the determination of appropriately sufficient reliability can only be made *ex post* by a court or other trier of fact. In order to create more certainty *ex ante*, article 6, paragraph 3 of the UNCITRAL Model Law on Electronic Signatures 2001 was introduced.[274]

5.10.11 It is noted that there is no such "reliability requirement" for the legal validity of handwritten signatures (or any of the other marks on paper that may constitute a signature at law). Common law does not impose any form requirement on signatures. A person can sign by marking a cross "X" on a document. A person can also sign by a machine that prints his name on a document. Both the cross "X" and machine-printed name are legally valid signatures, though questions of proof may arise. In each case, it is a matter of proof whether the purported signor did in fact sign in that manner and intended thereby

[274] Paragraph 118 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 2001.

to sign the document. In order to establish the signature's function of linking the signor with the signed document, the context of the signing will always have to be demonstrated, whether the signature is on paper or electronic.

5.10.12 It is not the form of the signature, but the proven link between the signature and the purported signor based on the context, that gives the signature its legal effect. In commercial transactions, the person relying on a signature always takes the risk that the signature is not genuine, so he evaluates the risk that the signature is not genuine and protects himself accordingly.[275] The risk analysis will of course include the cost of having the signature made more reliable and the cost of its being not genuine. So a history of dealings with the purported signor, or a low-value transaction, may persuade someone to rely on a signature that would not be satisfactory if it were from a stranger or for a high value transaction. These precautions and judgments are not a matter of law but a matter of prudence. That is, a party may not feel comfortable about relying on a signature in the form of a cross "X", but that is a judgment by that party as a matter of prudence, and not a matter of law, as the signature in the form of a cross "X" is fully valid as a signature at law. We are of the view that this analysis applies equally where electronic commercial transactions and electronic signatures are concerned.

5.10.13 Singapore has submitted a comment to the UNCITRAL Secretariat proposing to delete paragraph 3(b) of article 9 of the draft Convention (A/CN.9/577), to achieve functional equivalence between handwritten signatures and electronic signatures, and to avoid the unintended difficulties that would be created by the inclusion of the general legal "reliability requirement" in paragraph 3(b). The full text of the comment submitted to UNCITRAL is set out at Annex C.

5.10.14 The ETA does not contain such a reliability requirement for electronic signatures to satisfy requirements of law for signatures. Instead section 8 of the ETA underlines that a flexible approach will be taken in the manner of proving an electronic signature.[276] If the

[275] This may involve checking the signature against known genuine versions of it, or getting the signature witnessed, notarized or guaranteed by a bank, etc.
[276] See footnote 277.

reliability requirement in the draft Convention is adopted, section 8[277] of the ETA would need to be amended. The regime suggested by the reliability requirement in the draft Convention more closely resembles the regime relating to secure electronic signatures under section 17.[278]

5.10.15 In our view, there should not be any general reliability requirement imposed in a provision providing for the functional equivalence of electronic signatures and handwritten signatures.[279]

5.10.16 Signature requirements under the law exist mainly in relation to specialised transactions (such as negotiable instruments or land transactions which have been excluded from the ETA) and transactions with Government agencies (which, under existing law[280] generally have power to stipulate alternative requirements). Where, after due consideration of the policy and purposes of specific requirements for a signature in a particular law, a relevant authority is satisfied that additional reliability requirements for electronic signatures would be desirable, such requirements can be prescribed in the relevant law or (in cases outside the ambit of the ETA) a court can impose such requirements as a matter of interpretation of the legal requirement[281]. It would be clearer to specify the standard of

[277] **Electronic signatures**

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

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

[278] **Secure electronic signatures**

17. If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that 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.

[279] i.e. section 8 of the ETA.

[280] i.e. section 47 of the ETA.

[281] The High Court in *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd* [2005] SGHC 58 decided that, notwithstanding the exclusion (under section 4 of the ETA) of contracts for

reliability required of electronic signatures in relation to particular requirements of law rather than to rely on a general reliability requirement.

5.10.17 If Singapore accedes to the Convention, such additional requirements would have to be declared under article 18(2) of the Convention (see Part 5.16).

Q16. Do you agree that a general provision providing for the functional equivalence of electronic signatures to handwritten signatures (e.g. section 8) should not contain any reliability requirement?

Q17. Should any laws imposing a signature requirement be clarified by prescribing the requirements as to reliability that should apply to electronic signatures? If yes, please state the legal requirement (e.g. Civil Law Act, section 6) and describe the standard that should be required of electronic signatures in order to satisfy that legal requirement.

5.11 Provision of Originals

5.11.1 Article 9(4), (5) and (6) of the Convention provides as follows:

> "4. Where the law requires that a communication or a contract to be presented 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 information be presented, that information is capable of being displayed to the person to whom it is to be presented.
>
> 5. For the purposes of paragraph 4(a):

the disposition of immovable property from the application of section 8 of the ETA, a court could decide whether, as a matter of common law, an electronic signature satisfied a legal requirement for signature under section 6 of the Civil Law Act in respect of a contract for lease.

> (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 which 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.
>
> [6. 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.]".

5.11.2 This provision was added to the Convention to support the effective use of electronic means to conclude arbitration agreements since the enforcement of an arbitral award and the referral of parties to arbitration under articles II and IV of the 1958 New York Convention require a party relying on the arbitration agreement to produce its original or duly certified copy thereof. Nevertheless the Working Group noted that the usefulness of this provision extends beyond arbitration.[282]

5.11.3 The provision does not however address the issue of singularity, which is relevant to documents of title and negotiable instruments. The general agreement of the Working Group seems to be that the issue should not be addressed in the Convention, but in future UNCITRAL work on negotiable instruments. Article 2(2) excludes various kinds of documents of title and negotiable instruments from the application of the Convention.[283] Article 9(6), which excludes letters of credit, bank guarantees and similar instruments from the application of article 9(4) and (5), is still under review by UNCITRAL. As an alternative, it was proposed that the draft convention give States the possibility to exclude the application of article 9(4) and (5) by declarations made under draft article 18.[284]

[282] A/CN.9/571, paragraphs 129, 130 and 132.
[283] See paragraph 5.16.3. A/CN.9/571, paragraph 156.
[284] See paragraph 5.16.5. A/CN.9/571, paragraph 138.

5.11.4 Article 9(4) and (5) is essentially the same as the provisions in article 8 of the UNCITRAL Model Law on Electronic Commerce.[285] The ETA does not currently contain any provision on electronic originals.

5.11.5 The issue of electronic originals was previously discussed in the Stage I consultation paper on *Review of Electronic Transactions Act: Electronic Contracting Issues*.[286] There was little enthusiasm for such a provision amongst the respondents to the consultation as it was felt that, for commercial purposes, private parties could be left to make their own arrangements for the acceptance of originals. One respondent however advocated that legislation would be useful in promoting the development and acceptance of technology for the use of electronic originals.[287]

5.11.6 The related issue of provision for electronic documents of title and negotiable instruments was discussed in the Stage II consultation paper on *Review of the Electronic Transactions Act: Exclusions under section 4*.[288] Here again, there was little enthusiasm for such a provision amongst the respondents. In the case of negotiable instruments, it was felt that there is currently no demand for such provision because electronic cheques are not widely used. In the case of documents of title, the respondents generally advocated caution. In both cases, it was felt that legislation should only be made in tandem with the development of international norms.

5.11.7 Although we recognise that technology and practice in this area is still evolving, we note that provisions on electronic originals based on article 8 of the UNCITRAL Model Law on Electronic Commerce are widely accepted in other jurisdictions.[289] Such a provision could

[285] Except for drafting amendments substituting references to "communication or contract" in view of the limited ambit of the draft Convention.
[286] LRRD 1/2004, Part 7.2.
[287] Response by Mr Kenneth Lim of Crimson Logic, available on www.ida.gov.sg.
[288] LRRD 2/2004, Parts 4 (Negotiable Instruments) and 9 (Documents of Title, including discussion of the carriage of goods provision in articles 16 and 17 of the UN Model Law on E-Commerce).
[289] Canadian Uniform Electronic Commerce Act s.11, Irish Electronic Commerce Act 2000 s.17, Hong Kong Electronic Transactions Ordinance s.7. See also the US E-Sign Act s.101(d)(1) and (3). Section 32 of the New Zealand Electronic Commerce Act which relates to the "legal requirement to compare a document with an original document" however only adopts the requirement of reasonable assurance of integrity. Section 28 of the New Zealand Act relating to the requirement to provide information or to produce information in paper form adopts those criteria and could apply to the provision of originals. The Australian Commonwealth Electronic Transactions Act 1999 does not contain any provision on originals. Such issues are instead dealt with by section 11 and 12 of the

provide useful guidance on this nascent issue and facilitate the adoption of technology for electronic originals as it is developed. Further, if the draft Convention, which adopts a similar provision on electronic originals is widely adopted by other countries, it will set an international standard.

5.11.8 This provision does not prevent parties from agreeing to additional requirements in relation to the acceptance of originals. Further, with a consent provision, no one will be forced to accept electronic originals and private parties can continue to agree on arrangements to accept originals.[290]

5.11.9 In view of the general sentiment obtained from our public consultations, however, we agree that negotiable instruments and documents of title should continue to be excluded from the application of the ETA under section 4. Specific legislation may be made for such instruments when appropriate.

5.11.10 A further reason for the exclusion of negotiable instruments and documents of title is that the provision of originals does not address the issue of singularity. For similar reasons, it has been suggested that letters of credit and bank guarantees should also be considered for exclusion from the ambit of the provision on originals.[291]

5.11.11 With the exclusion of negotiable instruments and documents of title from the application of the ETA, we realize that a provision on electronic originals would have little application, except in relation to the requirement for originals by Government agencies. Nevertheless, we think that it would still be appropriate to adopt such a provision for consistency with legislation in other jurisdictions internationally and to complement our legislative framework in relation to the electronic retention of documents.[292]

Australian Act, relating to production and retention of documents, which also adopt criteria based on the UNCITRAL Model Law.

[290] See paragraph 5.7 on consent and variation.

[291] See paragraph 5.11.3.

[292] See Part 4.10 on the proposed amendments to section 9 of the ETA.

5.11.12 **We therefore propose to adopt a provision on electronic originals in the ETA.** (Please see proposed section 9A in Annex B.)[293]

Criteria for acceptance of electronic originals

5.11.13 Despite the different formulations adopted by the different jurisdictions surveyed[294], they have all adopted variations of the criteria of reliable assurance of integrity[295] (or accuracy) and accessibility[296] in provisions on electronic originals and similar provisions. "Accessibility", which covers both the usability of the record for subsequent reference and its capability of being retained by the person to whom the record is provided, is an extension of the requirement in the UNCITRAL Model Law which merely provides that the information must be capable of being displayed to the recipient.[297] It may however be questioned whether the capability of retention and re-use should be a requirement where the original is required only for the purposes of a once-off validation.

5.11.14 Where the provisions deal more specifically with particular situations, as in Australia and New Zealand, the criteria have been modified as appropriate for the specific situations. In New Zealand, where there are separate provisions in relation to paper documents being converted to electronic form and records that were created in electronic form, the requirements are basically the same for both forms of records except that in the case of conversion of an electronic record into a paper document, there is a requirement to notify the recipient if the integrity of the document cannot be assured and to produce the electronic record if requested to do so.[298] In the case of electronic communications that have to be transmitted, there

[293] See also Part 4.11 on originals in the context of e-Government.
[294] Canada, Australia, New Zealand and Ireland.
[295] "Integrity" means that the information has remained complete and unaltered, apart from any changes that arise in the normal course of communication, storage or display. The standard of reliability is to be assessed in relation to the document and in the light of all the circumstances.
[296] Canadian Uniform Electronic Commerce Act s.11, Irish Electronic Commerce Act 2000 s.17, Hong Kong Electronic Transactions Ordinance s.7. See also the US E-Sign Act s.101(d)(1) and (3). Section 32 of the New Zealand Electronic Commerce Act which relates to the "legal requirement to compare a document with an original document" however only adopts the requirement of reasonable assurance of integrity. However section 28 of the New Zealand Act relating to the requirement to provide information or to produce information in paper form adopts those criteria and could apply to the provision of originals.
[297] Hong Kong adopted the UNCITRAL formulation i.e. capability of display.
[298] New Zealand Electronic Transactions Act 2002 s. 29 and 31

is also a requirement for the record to identify the sender and recipient and time when it was sent and received.[299]

5.11.15 We note that some jurisdictions have added qualifications to the criteria. For example, in Australia, the requirement for accessibility has to be complied with "at the time the communication was sent" (in the provision on production of documents)[300] or "at the time of commencement of the retention of the information" (in the provision on retention of electronic communications) [301], and only to the extent that "it was reasonable to expect" that the information would be so accessible at that time.[302] Further, the provisions on retention of documents or information in Australia are limited to requirements for retention "for a particular period" and the requirement to retain additional information as to the origin, destination and time or sending and receipt continues only during that period.[303]

Q18. What difficulties or benefits do you foresee if the provisions of article 9(4) and (5) of the draft convention (relating to originals) are adopted in the ETA?

Q19. Do you have any comments on proposed section 9A in Annex B? Do you agree with the criteria for acceptance of electronic originals in proposed section 9A(1) and (2) in Annex B?

5.11.16 The adoption of a provision in the production of originals raises other issues. These are further discussed in Part 4.[304]

5.12 Time and Place of Despatch and Receipt

5.12.1 Article 10 of the Convention now reads:

> "1. The time of dispatch of an electronic communication[305] is the time when it leaves an information system under the

[299] New Zealand Electronic Transactions Act 2002 s. 27
[300] Australian Commonwealth Electronic Transactions Act 1999 s.11.
[301] Australian Commonwealth Electronic Transactions Act 1999 s.12(4).
[302] Also Irish Electronic Commerce Act 2000 s. 17(2)(c) and 18(2)(c).
[303] Australian Commonwealth Electronic Transactions Act 1999 s.12(4)(c)
[304] Paragraphs 4.12.1 to 4.12.9 discuss whether to have a single provision on originals or many specific provisions. Paragraphs 4.12.10 to 4.12.16 discuss consent and additional technical requirements.
[305] References to "data messages" have been replaced by references to "electronic communications".

control of the originator[306] 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, at 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 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.

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.".

5.12.2 Section 15 of the ETA provides that an electronic record is **despatched** when "it enters an information system outside the control of the originator or the person who sent the electronic record on behalf of the originator".[307]

5.12.3 The Convention changes this to the time it "leaves an information system under the control of the originator or of the party who sent it on behalf of the originator".

[306] The words in square brackets that were deleted referred to entry into an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.
[307] Section 15(1)

5.12.4 As regards **receipt** of an electronic record, a number of separate rules apply under section 15. If an information system has been designated for receipt of the record, the electronic record is received when it "enters the designated information system".

5.12.5 The Convention changes this to the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee". The concept of a "designated information system" has been replaced by the concept of an "electronic address".[308]

5.12.6 Under section 15, if the electronic records are sent to another information system that was not designated by the addressee, receipt occurs when it is retrieved by the addressee.[309] If no information system was designated by the addressee, *receipt* occurs when the electronic record enters the information system of the addressee.[310]

5.12.7 The Convention changes the time of receipt of an electronic communication "at another electronic address of the addressee" to the time "when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the

[308] The Working Group agreed on the understanding that this term is not limited to e-mail addresses, but is open to future technological development. It was also stated that, as used in the draft provision, the term referred to "a portion or location in an information system that a person uses for receiving electronic messages". The Working Group however preferred not to include a definition in the draft Convention, leaving the concept to be elucidated in any explanatory notes or official commentary to the draft convention. A/CN.9/571

[309] Section 15(2)(a)

[310] Section 15(2)(b).

Some jurisdictions have adopted a rule whereby, in the absence of a designated information system, a message is deemed to be received when the addressee *became aware* of the data message and the message was *capable of being retrieved*. Canada provides a presumption that an electronic record is received only when the addressee becomes aware of the record *and* it is accessible by the recipient: UECA section 23(2)(b). The Australian Act and New Zealand Act provide that the time of receipt is the time when the electronic communication comes to the attention of the addressee. The Report of the Australian Electronic Commerce Expert Group to the Attorney-General on Electronic Commerce: Building the Legal Framework, paras 2.15.15 and 2.15.17, noted the need to address the issue of whether an electronic record is communicated only if it is actually read by the recipient.

Such a rule is more equitable than holding an addressee bound by a message sent to an information system that the addressee could not reasonably expect would be used in the context of its dealings with the originator or for the purpose for which the message was sent. On the other hand, it may be potentially unfair for the addressee unilaterally to have power to determine whether and when receipt would occur. The test is also inherently more uncertain since it will often depend on factors within the knowledge of the recipient or the ISP alone. It may also be difficult to obtain evidence from an ISP based outside the jurisdiction of the court. The test of entry into a particular information system is, on the other hand, technically easier to prove.

electronic communication has been sent to that address". There is therefore no longer any distinction whether the addressee has or has not designated an electronic address for receipt; the same rules will apply as long as communication is sent to an electronic address that the addressee has not designated. Mere entry into the addressee's information system or capability of retrieval are no longer sufficient; The communication must be capable of being retrieved **and** the addressee must be aware that the electronic communication has been sent.

5.12.8 An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address. This presumption is rebutted if it is shown that the communication was not in fact retrievable. Specific examples discussed by the Working Group were situations where the communication arrived outside of office hours or where security or other devices would prevent the communication from being retrieved.[311]

5.12.9 As regards the **deemed place of dispatch and the deemed place of receipt** of an electronic communication, article 10(3) of the draft Convention provides similarly to section 15(4) of the ETA. Article 10(3) makes reference to article 6[312], which clarifies the meaning of place of business. Compared with section 15(5) of the ETA, article 6 of the draft Convention contains further clarifications on the provisions on location of the parties.

[311] A/CN.9/571, paragraphs 159 and 160.

[312] Article 6. Location of the parties.

1. For the purposes of this Convention, a party's place of business is presumed to be the location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location.

2. If a party has not indicated a place of business and has more than one place of business, then [, subject to paragraph 1 of this article,] the place of business for the purposes of this Convention 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.

3. If a natural person does not have a place of business, reference is to be made to the person's habitual residence.

4. A location is not a place of business merely because that is: (a) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or (b) where the information system may be accessed by other parties.

5. 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.

5.12.10 Article 6(1) presumes that a party's place of business is the "location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location".[313] The Convention does not impose any requirement that parties must disclose their identity or place of business, but article 7[314] expressly provides that the Convention does not affect the application of any rule of law requiring such disclosure.[315] Article 6(2), which relates to the situation where a party had more than one place of business, is similar to section 15(5)(a) of the ETA, except that it clarifies that regard is to be had "to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract".[316] Article 6(3) notably applies only in respect of a natural person who does not have a place of business. Section 15(5)(b), read with section 15(5)(c)[317], by contrast, extends to bodies corporate.[318]

5.12.11 Article 6 further clarifies that a "location is not a place of business merely because that is (a) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or (b) where the information

[313] The Working Group regarded this provision to be useful for companies with several places of business, with more than one having connections with a specific contract. This provision would allow the company to indicate one of its places of business, with the consequence that the indication cannot be challenged unless the company did not have a place of business at the location indicated. A/CN.9/571, paragraph 98.

[314] Article 7. Information requirements.

Nothing in this Convention affects the application of any rule of law that may require the parties to disclose their identities, places of business or other information, or relieves a party from the legal consequences of making inaccurate or false statements in that regard.

[315] Many European States impose such disclosure requirements on online service providers as a matter of consumer protection.

[316] The main purpose of this provision is to provide a default rule where a party having more than one place of business fails to indicate the place of business for that particular transaction. A/CN.9/571, paragraph 100. For cases where a party had only one place of business and did not disclose it, the definition in article 4(h) ("Place of business" means any place where a 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.) already provides an answer.

[317] Section 15(5)(c) provides that, in relation to a body corporate, "usual place of residence" means the place where it is incorporated or otherwise legally constituted.

[318] The draft Convention refers to "habitual residence" instead of "usual place of residence" because it is intended only to apply to natural persons. The Working Group felt it was unwise to alter the wording which is common in uniform law conventions. It acknowledged that there might be legal entities, so-called "virtual companies", whose establishment might not meet all the requirements of the definition of "place of business" in article 4(h). A/CN.9/571, paragraph 103.

system may be accessed by other parties".[319] It also provides that 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".[320]

5.12.12 Article 10(4) of the draft Convention is similar to section 15(3) of the ETA, except for consequential changes as a result of the adoption of the concept of "electronic address" and the term "electronic communication".

5.12.13 Various concerns were raised in respect of the earlier version of this provision of the Convention by respondents to LRRD No.1/2004[321]. A major concern was the uncertainty which arose from the provision that the presumption that the data message was capable of being retrieved would be rebutted if "it was unreasonable for the originator to have chosen that particular information system for sending the data message". This reference to unreasonableness has been removed from the current Convention draft. In the case of receipt at an electronic address that was not designated by the addressee, there is an additional requirement that the addressee must actually be aware that the communication has been sent. The adoption of the new concept of "electronic address" also helps to clarify the uncertainties that previously related to the term "information system" of that party or under their control. The concern about communications received after office hours or when the addressee does not in fact have access to the communication have also been addressed by the fact that the presumption concerning receipt is rebutted if it is shown that the communication was not in fact retrievable.[322]

[319] Article 6(4). The Working Group decided not to provide for "virtual companies" as the matter at this early stage was better left to the elaboration of emerging jurisprudence. A/CN.9/571, paragraph 107. See also footnote 318.

[320] Article 6(5). This only prevents domain name from being the sole factor in determining the location of a party. It does not prevent a court or arbitrator from taking into account the domain name as a possible element, among others, to determine a party's location, where appropriate. A/CN.9/571, paragraph 113.

[321] Part 5, see footnote 247

[322] See Part 5.12, especially paragraphs 5.12.5, 5.12.7 and 5.12.8. Other concerns raised about hijacked mail, denial of service attacks and wrong clock settings would all be matters to be proved to show that a communication was not capable of being retrieved or was not sent at the purported time, and are beyond the scope of the provision.

5.12.14 These default rules help to provide greater certainty as to the time and place of dispatch and receipt of electronic communications. Their adoption will however entail changes to the existing law under section 15 of the ETA.

Q20. What difficulties or benefits do you foresee if the provisions of article 10 of the draft Convention (relating to time and place of dispatch and receipt of electronic communications) are adopted in the ETA?

5.13 Invitation to Make Offers

5.13.1 Article 11[323] of Convention makes it the default rule that proposals made to the world at large are to be considered as an invitation to make offers. The provision preserves party autonomy by stating that the default rule is subject to clear indication of "the intention of the party making the proposal to be bound in case of acceptance". There has been no change to the provision since we consulted on it in Stage 1 of the ETA Review[324].

5.13.2 Respondents who agreed to this provision favoured it because it would give certainty to such transactions. Those who were not in favour of this provision preferred that the rules of common law should continue to apply.

5.13.3 This provision provides greater certainty as to whether proposals made to the world at large are binding. As the ETA does not contain any provision on this issue, the position in Singapore law has to be decided in each case based on common law principles.

Q21. What difficulties or benefits do you foresee if the provisions of article 11 of the draft Convention (relating to invitation to make offers) are adopted in the ETA?

5.14 Automated Message Systems

5.14.1 The provision on automated message systems, now in article 12 of the Convention, reads:

[323] This was previously article 12 of draft Convention, A/CN.9/WG.IV/WP.103.
[324] LRRD No.1/2004, paragraph 4.2.

> "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 each of the individual actions carried out by the systems or the resulting agreement."

5.14.2 The provision has only undergone minor drafting amendments. The term "automated message system" is used instead of "automated information system". The term is defined to mean "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 person each time an action is initiated or a response is generated by the system".[325] The term "person" is clarified by referring to "natural person".

5.14.3 This provision will facilitate the use of automatic message systems[326] as it makes it explicit that contracts formed by the interaction of an automated message system and an individual, or by the interaction of automated information 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.

Q22. What difficulties or benefits do you foresee if the provisions of article 12 of the draft Convention (relating to automated message systems) are adopted in the ETA?

5.15 Error in Electronic Communications

5.15.1 Article 14 of the Convention provides 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

[325] Article 4(g) c.f definition of the term "information system" in article 4(f) as "a system for generating, sending, receiving, storing or otherwise processing data messages.

[326] E.g. reply slips on orders on Amazon.com, online travel insurance acknowledgements when users purchase insurance online.

> acting, has the right to withdraw 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;
>
> (b) 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; and
>
> (c) 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 errors made during the formation or performance of the type of contract in question other than an input error that occurs in the circumstances referred to in paragraph 1.

5.15.2 This issue was previously discussed in LRRD No.1/2004.[327] Most of the respondents to the consultation supported such a provision. One respondent voiced a concern that it is difficult to define "error". Others were concerned about regulatory burdens and the fettering of party autonomy. These concerns appear to be met by the current draft of the provision.

5.15.3 The provision has been amended to refer to "input" error. This clarifies that the provision applies only to errors relating to inputting wrong data, as opposed to other kinds of error such as misunderstanding of the terms of the contract or simply poor business judgment.

[327] Part 6.5, see footnote 247.

5.15.4 Further, the provision applies only if "the automated message system does not provide the person with an opportunity to correct the error". As most online systems would provide an opportunity to correct errors, [328] this provision would not affect such cases.

5.15.5 In other words, this provision is intended to cover a limited problem relating to the use of electronic communications. It would complement the common law of mistake[329] by balancing the need for certainty in commercial relationships and the need to protect consumers from unfair trade practices. It provides a fair basis for the exercise of the right of withdrawal[330] and would also tend to limit abuses by parties acting in bad faith. The provision "gives online merchants a way of giving themselves a good deal of security against allegations of mistake, and encourages good business practices in everybody's interests".[331]

Q23. What difficulties or benefits do you foresee if the provisions of article 14 of the Convention (relating to Error in Electronic Communication) are adopted in the ETA?

5.16 Applicability of the Convention

5.16.1 The Convention applies "to the use of electronic communications in connection with the formation or performance of a contract [or agreement] between parties whose places of business are in different States".[332] The word "formation" is to be interpreted widely to include all contracting stages, including negotiations and invitations to make offers.

[328] E.g the provision of an opportunity to confirm the order or to return and correct one's input.

[329] Under the common law doctrine of mistake which applies under Singapore law, a mistake is immaterial unless it is fundamental i.e. it results in a complete difference in substance between what the mistaken party bargained for and what the contract purports. It is likely that a court would allow the apparent contract to stand unless, on the facts, it must have been obvious to the other party that the person had made a mistake.

[330] The prevailing view of the Working Group was that the possibility to withdraw only the vitiated part of the communication was implicit in the right to withdraw the entire communication. It was decided however that the provision should not confer a right to vary the agreement. A/CN.9.571, paragraphs 194 and 196.

[331] Annotations to the Canadian Uniform Electronic Commerce Act. The provision was inspired by Canadian legislation e.g. section 22 of the Canadian Uniform Electronic Commerce Act.

[332] Article 1(1).

5.16.2 Article 2(1) excludes certain types of transactions, in particular:

> "(a) Contracts concluded for personal, family or household purposes;
>
> (b)(i) Transactions on a regulated exchange, (ii) foreign exchange transactions; (iii) inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments; (iv) 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.".

5.16.3 Article 2(2) excludes application to "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".

5.16.4 The following exclusions were deleted from article 2(2), as they were regarded as territory-specific issues that should be better dealt with at State level:[333]

> "(b) Contracts that create or transfer rights in immovable property, except for rental rights;
>
> (c) Contracts requiring by law the involvement of courts, public authorities or professions exercising public authority;[334]
>
> (d) Contracts for suretyship granted by, and on collateral securities furnished by, persons acting for purposes outside their trade, business or profession;
>
> (e) Contracts governed by family law or by the law of succession.".

5.16.5 An exclusion from article 9(4) and (5) where a rule of law or the agreement between the parties requires a party to present certain

[333] A/CN.9/571, paragraph 65.

[334] It was stated that this provision might have the undesirable effect of hindering the international development of electronic public procurement. Another difficulty was the reference to "tribunals" might be read to encompass arbitral bodies. A/CN.9/571, paragraph 65.

original documents for the purpose of claiming payment under a letter or credit, a bank guarantee or a similar instrument is still under consideration by UNCITRAL. As an alternative to such an exclusion, it was proposed that the Convention could give States the possibility to make such an exclusion by declaration under article 18.

5.16.6 Article 18(1) allows States to declare that the Convention will apply only to:

> "(a) When the States referred to in article 1, paragraph 1 are Contracting States to this Convention;
>
> (b) When the rules of private international law lead to the application of the law of a Contracting State; or
>
> (c) When the parties have agreed that it applies.".

5.16.7 Article 18(2) allows States to exclude matters from the scope of the Convention by declaration in accordance with article 20[335] in relation to declarations under articles 17(1) (Effect on territorial units), 18 (1) and (2) and 19(2), (3) and (4) (Communications exchanged under other international conventions).[336] It was noted, for example, that article 9 of the Convention would generally apply to any form requirements under the applicable law. Public policy rules contained in domestic law barring the use of electronic communications were to be dealt with either as exclusions under article 2 or by means of declarations of exclusions under draft article 18.

5.16.8 Section 4(1) of the ETA currently excludes Parts II and IV of the Act from applying to any rule of law requiring writing or signature in any of the following matters:

> "(a) the creation or execution of a will;
>
> (b) negotiable instruments;
>
> (c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts;

[335] Article 20 relates to the procedure and effects of declarations.

[336] Such declarations may be made at any time and not only at the time of the deposit of its instrument of ratification, acceptance, approval or accession. A/CN.9/571, paragraph 32.

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

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

(f) documents of title.".

5.16.9 Some of the exclusions under section 4 of the ETA correspond to exclusions under article 2 of the Convention, namely, the exclusions in article 2(2) correspond to the exclusion for negotiable instruments and documents of title in section 4(b) and (f) respectively. **The other exclusions in section 4 do not correspond to any exclusion under article 2 of the Convention. Those other exclusions, if they are to be retained in relation to the Convention, will have to be excluded by declaration under article 18(2).**

5.16.10 **It will also be necessary to make declarations with respect to provisions that impose any requirements for the acceptance of electronic communications which differ from the requirements under the Convention.** For example, if Government agencies impose additional technical or procedural specifications or any exclusions in relation to the acceptance of electronic communications (as provided for under section 9(4)(b) or 47(2) of the ETA, or proposed section 9(1)(d), 9(4)(b), 9A(1)(c) or 9A(4)) these additional specifications or exclusions will have to be declared insofar as they may affect contracts governed by the Convention.

5.16.11 It is also timely to review the legal requirements for writing, signature, retention of documents and originals under our law, to consider whether the rules for functional equivalence of electronic communications under the Convention are appropriate for the purposes of those legal requirements. For example, does an electronic signature adequately serve the purposes of section 6 of the Civil Law Act[337], or should there be specifications as to the standard

[337] Section 6 of the Civil Law Act provides:

Contracts which must be evidenced in writing

6. No action shall be brought against —

(*a*) any executor or administrator upon any special promise to answer damages out of his own estate;

(*b*) any defendant upon any special promise to answer for the debt, default or miscarriage of another person;

(*c*) any person upon any agreement made upon consideration of marriage;

of reliability that an electronic signature must meet to serve as a valid signature for the purposes of that section? If any additional requirements are to be applied for the recognition of electronic signatures for the purposes of such legal requirements, it will be necessary to declare those additional requirements under the Convention insofar as they may affect contracts governed by the Convention.

5.16.12 A further issue for consideration is whether Singapore should adopt any of the possible limitations to the applicability of the Convention mentioned in article 18(1). The imposition of such limitations would significantly restrict the applicability of the Convention. **Such limitations would seem to be unnecessary if we decide to align our law with that under the Convention. The ETA is for the most part already consistent with many of the provisions of the Convention. In most cases where there are differences, we propose to align the ETA to the Convention for consistency in the law applicable to domestic and international contracts, as well as other transactions.**

Q24.	What exclusions from the applicability of the Convention do you propose in the context of Singapore? Please specify legislative provisions affected where relevant. (See paragraphs 5.16.9 to 5.16.11)
Q25.	Do you agree that Singapore should not adopt any of the limitations in article 18(1)? (See paragraph 5.16.12)

5.17 Extension to Non-Contractual Transactions

Provisions in Part IV of ETA

5.17.1 Part IV of the ETA is entitled "ELECTRONIC CONTRACTS". The provisions in that Part are arguably limited in their application to contractual transactions. Some of the provisions, by reason of their

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

(*e*) any person upon any agreement that is not to be performed within the space of one year from the making thereof,

unless the promise or agreement upon which such action is brought, or some memorandum or note thereof, is in writing and signed by the party to be charged therewith or some other person lawfully authorised by him.

subject matter, can only apply to contracts e.g. section 11 which relates to formation and validity of contracts.

5.17.2 In the case of some other provisions, there is no intrinsic reason why they cannot apply to non-contractual transactions as well e.g. provisions relating to attribution (section 13), acknowledgement of receipt (section 14) and time and place of dispatch and receipt (section 15)[338]. Indeed, we note that in the Australian Electronic Transactions Act, provisions on time and place of dispatch and receipt of electronic communications and on attribution of electronic communications are not limited to contractual transactions.

5.17.3 **We propose that the provisions relating to attribution, acknowledgement of receipt and time and place of dispatch and receipt in Part IV of the ETA should be allowed to apply to non-contractual transactions as well.** There does not seem to be any need to extend section 12 (relating to effectiveness of an electronic record, declaration of intent or other statement between parties) to non-contractual transactions since section 6 (on legal recognition of electronic records) already applies.

Provisions of UNCITRAL Convention

5.17.4 The provisions relating to legal recognition of electronic records[339], requirement for writing[340] and electronic signatures[341] in the UNCITRAL Convention already have counterparts in the ETA[342] that apply generally and are not limited to contractual transactions. There is no reason why these provisions should now be so restricted even if the provisions in the ETA are to be aligned with the UNCITRAL Convention.

5.17.5 Similarly there is no reason to limit the provision on originals[343] to contractual provisions. Indeed, as pointed out, with the proposed exclusion of various types of contractual transactions from the ambit of this provision, its remaining area for application would largely

[338] See also Part 5.12 on article 10 of the UNCITRAL Convention.
[339] Article 8, see Part 5.8.
[340] Article 9, see Part 5.9.
[341] Article 9(3), see Part 5.10.
[342] i.e. sections 6, 7 and 8 respectively.
[343] Article 9(4), (5) and (6), see Part 5.11.

consist of non-contractual transactions such as government transactions. Notably, the related provision on retention of electronic records (section 9) in the ETA is not limited to contractual transactions.

5.17.6 It is also necessary to consider whether the consent and variation provisions[344] should apply to non-contractual transactions, and if so whether any modifications are necessary. Consent in relation to section 9 (retention of electronic records) and proposed section 9A (provision of originals) are discussed in paragraphs 4.12.10 to 4.12.16.

5.17.7 The provisions on invitation to make offers[345], automated message systems[346] and error in electronic communications[347] are, by their nature, relevant only to contractual transactions.

Q26. Should sections 13, 14 and 15 in Part IV of the ETA be allowed to apply to non-contractual transactions? (See paragraphs 5.17.1 to 5.17.3)
Q27. Do you have any comments on whether any of the provisions of the Convention should apply to non-contractual transactions? (See paragraphs 5.17.4 to 5.17.7)

[344] See Part 5.7.
[345] Article 11, See Part 5.13.
[346] Article 12, see Part 5.14.
[347] Article 14, see Part 5.15.

ANNEX A

ELECTRONIC TRANSACTIONS ACT
(CHAPTER 88, SECTIONS 42 AND 61)

ELECTRONIC TRANSACTIONS (CERTIFICATION AUTHORITY) REGULATIONS

[10th February 1999]

PART I

PRELIMINARY

Citation

1. These Regulations may be cited as the Electronic Transactions (Certification Authority) Regulations.

Definitions

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

"licence" means a licence granted under these Regulations;

"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 a licensed certification authority), creation of private keys or administration of a certification authority's computing facilities.

PART II

LICENSING OFCERTIFICATION AUTHORITIES

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.

Period of validity of licence
4. A licence shall be valid for a period of one year or such other longer period as the Controller may allow.

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.

Licence fees
6. —(1) An application fee of $5,000 shall be payable to the Controller on every application for the grant or renewal of a licence to be a licensed certification authority.
(2) If the application referred to in paragraph (1) is approved, there shall be payable to the Controller a fee of $1,000 for each year the licence is granted.
(3) There shall be payable to the Controller on every grant of the renewal of a licence a fee of $1,000 for each year the licence is renewed.
(4) The Controller shall not refund any fee paid if the application is not approved, is withdrawn or is discontinued or if the licence is suspended or revoked.

PART III

LICENSING CRITERIA

Financial criteria, etc.
7. —(1) An applicant for a licence shall comply with the following criteria:
(a) the applicant must be a company operating in Singapore;
(b) the applicant must be insured against liability for loss of not less than $1 million for each claim arising out of any error or omission on the part of the applicant, its officers or employees;
(c) the applicant must have —
(i) not less than $2 million in paid-up capital; and
(ii) in addition, a combined paid-up capital and proof of available financing of not less than $5 million; and
(d) the applicant must obtain a performance bond or banker's guarantee in favour of the Controller in a form approved by the Controller for an amount of not less than $1 million.
(2) The performance bond or banker's guarantee referred to in paragraph (1) (*d*) may be invoked —
(a) for payment of an offer of composition made by the Controller;
(b) for payment of liabilities and rectification costs attributed to the negligence of the certification authority, its officers or employees; or

(c) for payment of the costs incurred in the discontinuation or transfer of operations of the licensed certification authority, if the certification authority's licence or operations is discontinued.

Personnel

8. —(1) An applicant shall 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 or has made a composition or an 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 to have a trusted person who has been convicted of an offence referred to in that paragraph, if the Controller is satisfied that —
(a) the trusted person is now a fit and proper person to carry out his duties; and
(b) 10 years have elapsed from —
(i) the date of conviction; or
(ii) the date of release from imprisonment if he was sentenced to a term of imprisonment, whichever is the later.
(3) Every trusted person must —
(a) have a good knowledge of the Act and these Regulations;
(b) be trained in the certification authority's certification practice statement; and
(c) possess the relevant technical qualifications, expertise and experience to effectively carry out his duties.

Operational criteria

9. —(1) An applicant shall comply with the following operational criteria:
(a) the applicant must have a certification practice statement approved by the Controller;
(b) the applicant must undergo and pass an initial audit before a licence can be granted by the Controller; and
(c) the applicant must undergo and pass such audit as the Controller may, by notice in writing, require.
(2) The audits referred to in this regulation must be —
(a) conducted in accordance with the auditing requirements specified in regulation 10; and
(b) completed within such time as the Controller may, by notice in writing, specify.

Auditing requirements

10. —(1) An applicant must pass any audit required under regulation 9 (1) for compliance with —
(a) security guidelines as referred to in regulation 26;
(b) licensing conditions;
(c) its certification practice statement; and
(d) the Act and these Regulations.
(2) All audits 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.
(3) 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 been providing services or supplying equipment to the certification authority.
(4) Auditing fees shall be borne by the certification authority.
(5) A copy of every audit report shall be submitted to the Controller within 4 weeks of the completion of an audit.
(6) Failure to pass the audit may be a ground for revocation of a licence.

Controller to refuse to grant or renew licences in certain circumstances
11. —(1) The Controller may refuse to grant or renew a licence if —
(a) the applicant has not provided the Controller with such information relating to it or any person employed by or associated with it for the purposes of its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require;
(b) the applicant or its substantial shareholder is in the course of being wound up or liquidated;
(c) a receiver or a receiver and manager has been appointed to the applicant or its substantial shareholder;
(d) 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;
(e) 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;
(f) the Controller is not satisfied as to the qualifications or experience of the trusted person who is to perform duties in connection with the holding of the licence by the applicant;
(g) the applicant fails to satisfy the Controller that it is a fit and proper person to be licensed or that all its trusted persons and substantial shareholders are fit and proper persons;
(h) 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;
(i) the Controller is not satisfied as to the financial standing of the applicant or its substantial shareholder;
(j) 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 holding of the licence;
(k) 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
(l) 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).

PART IV

REVOCATION AND SUSPENSION OF LICENCE

Revocation or suspension of licence

12. —(1) A licence shall be deemed to be revoked if the certification authority is wound up.

(2) The Controller may revoke or suspend the licence of a certification authority —

(a) on any ground on which the Controller may refuse to grant a licence under regulation 11;

(b) if the certification authority fails to comply with a direction of the Controller made under section 51 of the Act;

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

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

(e) if the certification authority fails to carry on business for which it was licensed;

(f) 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

(g) if the certification authority contravenes or fails to comply with any condition or restriction applicable in respect of the licence.

(3) The Controller may revoke the licence of a certification authority at the request of that certification authority.

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

Powers of Controller in cases of misconduct, etc.

13. —(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 licensed 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) revoke the licence of the certification authority;

(b) suspend the licence 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 51 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.

Effect of revocation or suspension of licence
14. —(1) A certification authority whose licence is revoked or suspended under regulation 12 or 13 shall, for the purposes of this regulation, be deemed not to be licensed from the date that the Controller revokes or suspends the licence, as the case may be.
(2) A revocation or suspension of a licence 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 revocation or suspension of the licence; or
(b) affect any right, obligation or liability arising under any such agreement, transaction or arrangement.

Appeal against refusal to license, etc.
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.
(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.
(3) In considering whether to defer the execution of the decision, the Controller shall have regard to whether the deferment is prejudicial to the interests of any subscriber of the certification authority or any other party who may be adversely affected.
(4) If an appeal is made to the Minister, a copy of the appeal shall be lodged with the Controller.

PART V

CONDUCT OF BUSINESS BY LICENSED CERTIFICATION AUTHORITIES

Trustworthy record keeping and archival
16. —(1) A licensed certification authority may keep its records in the form of paper-based documents, electronic records or any other form approved by the Controller.
(2) Such records shall be indexed, stored, preserved and reproduced so as to be accurate, complete, legible and accessible to the Controller, an auditor or an authorised officer.

Trustworthy transaction logs
17. —(1) Every licensed 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 a licensed certification authority);
(b) the process of generating subscribers' (where applicable) or the licensed certification authority's own key pairs;
(c) the administration of a licensed certification authority's computing facilities; and
(d) such critical related activity of a licensed certification authority as may be determined by the Controller.
(2) Every licensed 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 licensed certification authority shall retain all records required to be kept under paragraph (1) and all logs of the creation of the archive of certificates referred to in paragraph (2) for a period of not less than 7 years.

Types of certificates
18. —(1) Subject to the approval of the Controller, a licensed 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 section 20 (*b*) (i) of the Act; and
(b) certificates which shall not be considered as trustworthy certificates for the purposes of section 20 (*b*) (i) of the Act.
(2) The licensed certification authority must associate a distinct certification practice statement approved by the Controller for each type of certificate issued.
(3) The licensed 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 section 20 (*b*) (i) of the Act.

Issuance of certificates
19. —(1) In addition to the requirements specified in section 29 of the Act, every licensed certification authority shall comply with the requirements in this regulation in relation to the issuing 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 revocation or suspension 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 a licensed certification authority shall contain conditions with standards higher than those conditions specified in section 29 (2) of 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 a licence.
(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 licensed 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 licensed certification authority shall publish a signed copy of the certificate in a repository referred to in paragraph (2).
(8) Notwithstanding paragraph (7), the licensed certification authority may contractually agree with the subscriber not to publish the certificate.
(9) If the subscriber does not accept the certificate, the licensed certification authority shall not publish it.
(10) Once the certificate has been issued by the licensed certification authority and accepted by the subscriber, the licensed certification authority shall notify the subscriber within a reasonable time of any fact known to the licensed certification authority that significantly affects the validity or reliability of the certificate.
(11) The date and time of all transactions in relation to the issuance of a certificate must be logged and kept in a trustworthy manner.

Renewal of certificates
20. —(1) Regulation 19 shall apply to the renewal of certificates as it applies to the issuance of certificates.
(2) The subscriber identity verification method shall be that specified in the certification practice statement as approved by the Controller.
(3) The date and time of all transactions in relation to the renewal of a certificate must be logged and kept in a trustworthy manner.

Suspension of certificates
21. —(1) This regulation shall apply only to every licensed certification authority which allows subscribers to request for suspension of certificates.
(2) Every licensed 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 section 31 of the Act, the licensed certification authority shall ensure that the certificate is suspended and notice of the suspension published in the repository in accordance with section 34 of the Act.
(4) A licensed certification authority may suspend a certificate that it has issued if the licensed certification authority has reasonable grounds to believe that the certificate is unreliable, regardless of whether the subscriber consents to the suspension; but the licensed 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 section 32 or 33 of the Act.
(5) It is the responsibility of any person relying on a certificate to check whether a certificate has been suspended.
(6) A licensed certification authority shall suspend a certificate after receiving a valid request for suspension (in accordance with section 31 of the Act); but if the licensed 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 section 32 or 33 of the Act.
(7) A licensed 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) A licensed certification authority must terminate a suspension initiated by request if the licensed 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) A licensed certification authority must maintain facilities to receive and act upon requests for suspension at all times of the day and on all days of every year.

Revocation of certificates
22. —(1) In order to confirm the identity of the subscriber or authorised agent making a request for revocation under section 32 (*a*) of the Act, the licensed certification authority must use the subscriber identity verification method specified in the certification practice statement for this purpose.
(2) A licensed certification authority must, after receiving a request for revocation, verify the request, revoke the certificate and publish notification of it under section 35 of the Act.
(3) A licensed 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) A licensed certification authority shall give notice to the subscriber immediately upon the revocation of a certificate.
(5) The date and time of all transactions in relation to the revocation of certificates must be logged and kept in a trustworthy manner.

Expiry date of certificates
23. A certificate must state the date on which it expires.

Certification practice statement
24. —(1) Every licensed 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 licence requires the prior approval of the Controller.
(3) Every licensed 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, suspension, revocation and renewal 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 licensed certification authority must log all changes to the certification practice statement together with the effective date of each change.

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

Secure digital signatures

25. —(1) The technical implementation of the requirements in section 20 of 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.

Security guidelines

26. —(1) Every licensed certification authority shall ensure that in the performance of its services it materially satisfies the security guidelines determined by the Controller and published on the Controller’s Internet website.

(2) An auditor when determining whether a departure from the security guidelines is material shall exercise reasonable professional judgment as to whether a condition that does not strictly comply with the guidelines 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 a licensed certification authority of any system other than a trustworthy system.

(4) The security guidelines 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 security guidelines 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 licensed certification authority shall provide every subscriber with a trustworthy system to generate his key pair.

(7) Every licensed 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 licensed certification authority, the resulting signature is considered secure only if the licensed certification authority endorses the implementation of such mechanisms in conjunction with its certificate.
(10) Every licensed certification authority shall be responsible for the storage of keys (including the subscriber's key and the licensed 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 security guidelines for compliance by every licensed certification authority.

Incident handling
27. —(1) A licensed 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 CA system and network;
(c) unavailability of infrastructure; and
(d) fraudulent registration and generation of certificates, certificate suspension and revocation information.
(2) If any incident referred to in paragraph (1) occurs, it shall be reported to the Controller within 24 hours.

Confidentiality
28. —(1) Except for the purposes of Part XII of the Act, or for any prosecution under any written law or pursuant to an order of court, every licensed certification authority and its authorised agent must keep all subscriber-specific information confidential.
(2) Any disclosure of subscriber-specific information by the licensed 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 licensed certification authority for this purpose; or
(c) relates to the fact that the certificate has been revoked or suspended.

Change in management
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.

PART VI

REQUIREMENTS FOR REPOSITORY

Availability of general purpose repository

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

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

(3) Any down time, whether scheduled or unscheduled, shall not exceed 30 minutes duration at any one time.

Specific purpose repository

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

PART VII

APPLICATION TO GOVERNMENT AND STATUTORY CORPORATIONS

Application to Government and statutory corporations

32. —(1) For the purposes of section 20 (*b*) (iii) of the Act, a department or ministry of the Government, an organ of State or a statutory corporation that is approved by the Minister under that section to act as a certification authority shall comply with the provisions of Parts III (with the exception of regulations 7 and 11), IV (with the exception of regulations 12, 14 and 15), V (with the exception of regulation 29), VI, VII and VIII (with the exception of regulations 36 and 37) as if it were a licensed 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 department or ministry of the Government, an organ of State or a statutory corporation that is approved by the Minister under section 20 (*b*) (iii) of the Act.

PART VIII

ADMINISTRATION

Waiver

33. —(1) Any licensed 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 a licence.

(2) The application must be supported by reasons for the application and include the necessary supporting documents.

Disclosure

34. —(1) The licensed 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 submitted or since the application for the licence; 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 licensed certification authority has a continuing obligation to disclose to the Controller any changes in the information submitted.
(4) All current versions of the licensed certification authority's applicable certification practice statements together with their effective dates must be published in the licensed certification authority's Internet website.

Discontinuation of operations of licensed certification authority
35. —(1) If a licensed certification authority intends to discontinue its operations, the licensed certification authority may arrange for its subscribers to re-subscribe to another licensed certification authority.
(2) The licensed 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 licensed certification authority, the transfer must be done in a trustworthy manner.
(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.

Penalties
36. Any person who fails, without any reasonable excuse, to comply with regulation 16 (2), 17, 19 (2) or (11), 20 (3), 21 (10), 22 (5), 24 (7) or (8) or 28 shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000.

Composition of offences
37. Any offence under these Regulations may be compounded by the Controller under section 59 of the Act.

[G.N. No.S 60/99]

ANNEX B

PROPOSED LEGISLATIVE AMENDMENTS RELATING TO ELECTRONIC GOVERNMENT

The proposed amendments set out below are intended for the purposes of discussion. Changes to the existing provisions are indicated in *italics*.

A. Proposed new definition in section 2

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

Notes

Definition of terms

A.1 The term "**Government agency**" replaces the words "a department or ministry of the Government, organ of State or statutory corporation" in the ETA. The term statutory "body" has been substituted for wider application since some entities created by statute to carry out government or regulatory functions are not corporations e.g. the Medical Council.

B. Proposed amendments to section 9

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 it is 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 electronic records specified by the Government agency which has supervision over the requirement for retention of such records are complied with.
(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.

B.1 The words "or provides for certain consequences if it is not" are added in section 9(1) for consistency with the other provisions in Part II of the ETA e.g. sections 7 and 8. This is because a legal requirement may not make the retention of documents mandatory, but merely provide that if the documents are not retained, the person will suffer some consequences or handicap.

B.2 New section 9(1)(*d*) allows Government agencies to impose additional requirements on the retention of documents under their purview. It is based on existing section 9(4)(*b*) (replaced by the opt-out provision discussed in B.3).

B.3 New section 9(4)(*b*) allows Government agencies to opt out of section 9 by specifying accordingly in an order published in the *Gazette*.

C. Proposed new section 9A

Provision of originals
9A. *— (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 accessible by the person and capable of being retained by the person so as to be usable for subsequent reference; and
(c) any additional requirements relating to the provision or retention of such electronic records specified by the Government 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 documents, records or information be provided or retained in original form if the Minister has, by order in the Gazette, specified that this section shall not apply to that requirement in respect of those documents.

Notes

C.1 This provision is based on article 8 of the UNCITRAL Model Law. It however adopts the test of accessibility adopted in various other jurisdictions, instead of the "capable of display" test in article 8 of the UNCITRAL Model Law.

C.2 The words "or provides for certain consequences if it is not" are included for consistency with the other provisions in Part II of the ETA e.g. sections 7, 8 and 9 (as amended). This is because a legal requirement may not make the production or retention of originals mandatory, but merely provide that if the documents are not produced or retained, the person will suffer some consequences or handicap.

C.2 Section 9A(1)(*c*) allows Government agencies to impose additional requirements on the retention of documents under their purview. It mirrors proposed section 9(1)(*d*) above.

C.3 Section 9A(4) allows Government agencies to opt out of section 9A by specifying accordingly in an order published in the *Gazette*. It mirrors proposed section 9(4)(*b*) above.

D. Proposed amendments to section 47

Acceptance of electronic filing and issue of documents

47 —(1) Any *Government agency* that, pursuant to any written law —

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

(*b*) requires that documents be created or retained;

(*c*) *requires documents, records or information to be produced 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.*

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

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

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

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

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

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

(3) 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 Government agency;

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

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

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

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

such a requirement is satisfied by an electronic record specified by the Government 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 Government agency;

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

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

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

Notes

D.1 The words "any department or ministry of the Government, organ of State or statutory corporation" in section 47 are replaced by the term "Government agency" for simplicity. The term "Government agency" will be defined accordingly in section 2 of the ETA (See A in this Annex).

D.2 **Section 47(1)** - This subsection empowers Government agencies to adopt electronic means of carrying out their functions under written law. The amendments expand on the functions currently covered by the provision.

D.3 Currently, section 47(1)(*a*) applies only to the filing, creation and retention of *documents*. The inclusion of a reference to the obtaining of information in any form will extend the provision to situations where a document is not

required, for example, a requirement to orally inform the Government agency. This issue is discussed in Part 4.8.

D.4 New section 47(1)(*c*) extends the provision to the requirement for production of original documents. New subsections (1)(*c*) and (3)(*d*) make it clear that electronic copies of paper originals or electronic originals can satisfy any requirement under written law for production of paper originals. This issue is discussed in Part 4.11.

D.5 **Section 47(2)** - This largely reproduces the existing subsection (2) which empowers the Government agency to specify certain matters where it decides to perform the functions referred to in subsection (1) electronically.

D.6 **Section 47(3)** - This new subsection makes it clear that certain functions carried out by a Government agency electronically satisfy the relevant requirements under written law. The functions covered by subsection (3) generally reflect the functions referred to in subsection (1).

D.7 Section 47(3)(*c*) specifically refers to the requirement for prescribed forms. New section 47(3) validates the use of such forms whether or not they resemble the prescribed paper forms. This issue is discussed in Part 4.7.

ANNEX C

Comment on the draft UNCITRAL Convention on the Use of Electronic Communications in International Contracts (submitted to UNCITRAL Secretariat on 16 May 2005)

1 Singapore expresses its appreciation to Working Group IV on the completion of its work at the forty-fourth session, and considers that the revised version of the draft convention A/CN.9/577 represents a sound basis for consideration and adoption by the Commission.

2 At this juncture, we wish to highlight only certain limited issues which we feel were not fully considered by the Working Group IV in its deliberations. We propose that the Commission consider:

(a) amending paragraph 3(a) of article 9 of the draft Convention (A/CN.9/577) to recognise that electronic signatures are sometimes required by law only for the purpose of identifying the person signing ("the signor") and associating the information with the signor, but not necessarily to indicate the signor's "approval" of the information contained in the electronic communication; and

(b) deleting paragraph 3(b) of article 9 of the draft Convention (A/CN.9/577), to achieve functional equivalence between handwritten signatures and electronic signatures, and to avoid the unintended difficulties that would be created by the inclusion of the general legal "reliability requirement" in paragraph 3(b).

Issues relating to paragraph 3(a) of article 9

3 Paragraph 3(a) of article 9 lays down general criteria for functional equivalence between handwritten signatures and electronic signatures.[348] Paragraph 3(a) provides that only an electronic signature that fulfils both the function of identification of the party *as well as* the function of indicating that party's approval of the information contained in the electronic communication meets that legal requirement of a signature in relation to an electronic communication.[349]

---

[348] Paragraph 3(a) of Article 9 is based on Article 7, paragraph 1(a) of the UNICTRAL Model Law on Electronic Commerce 1996. Article 7 of the UNCITRAL Model Law on Electronic Commerce states:

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

[349] It should be noted that under paragraph 3 of article 9, which originated from article 7, paragraph 1 of the UNCITRAL Model Law on Electronic Commerce, the mere signing of an electronic communication by means of a functional equivalent of a handwritten signature is not intended, in and of itself, to confer legal validity on the data message. Whether an electronic communication that fulfilled the requirement of a signature has legal validity is to be settled under

4 However, there may be instances where the law requires a signature that does not fulfil the function of indicating the signing party's approval of the information contained in the electronic communication. For example, many countries have requirements of law for notarisation of a document by a notary or attestation by a commissioner for oath. In such cases, it is not the intention of the law to require the notary or commissioner, by signing, to indicate his approval of the information contained in the electronic communication. In such cases, the signature of the notary or commissioner merely identifies the notary or commissioner, and associates the notary or commissioner with the contents of the document, but does not indicate the approval by the notary or commissioner of the information contained in the document. Similarly, there may be laws that require the execution of a document to be witnessed by a witness, who may be required to append his signature to that document. The signature of the witness merely identifies the witness and associates the witness with the contents of the document witnessed, but does not indicate the approval by the witness of the information contained in the document.

5 The conjunctive requirement in paragraph 3(a) of article 9 would prevent electronic signatures from satisfying the requirement of law for a signature in such situations where the function of indicating approval of the contents of the electronic communication cannot be fulfilled by such signatures.

6 In order to also allow electronic signatures that are not intended to fulfil the function of indicating the signor's approval of the information contained in the electronic communication, to also satisfy a requirement of law for a signature, we therefore propose that paragraph 3(a) of article 9 should be amended to read as follows:

> "(a) A method is used to identify the party and to associate that party with the information contained in the electronic communication, and as may be appropriate in relation to that legal requirement, to indicate that the party's approval of the information contained in the electronic communication; and".

7 The phrase "*A method is used to identify the party and to associate that party with the information contained in the electronic communication*" represents the minimum functional requirements of any signature, handwritten or electronic. This phrase provides that electronic signatures that only fulfil these minimum functions will satisfy the requirement of law for signatures. The phrase "*and as may be appropriate in relation to that legal requirement*" recognises that the function that the electronic signature is intended to perform will depend on the policy or purpose behind that particular requirement of law in question, and provides that the electronic signature is required to fulfil the function of indicating the signing party's approval of the information contained in the electronic communication, where it is appropriate in relation to that legal requirement. For example, if the law requires a party to sign an offer document to indicate his acceptance of the terms contained in the document, that electronic signature would fulfil the requirements of the proposed paragraph 3(a) of article 9 if it identifies the signing party, associates that party with the information contained in the document **and** indicates that party's approval of the information contained in the document.

---

the law applicable outside the draft convention. See paragraph 61 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996).

Issues relating to paragraph 3(b) of article 9

8 Paragraph 3(b) of article 9 contains a requirement that the method of signing must be "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" in order for the electronic signature to be legally valid.

9 This "reliability requirement" in paragraph 3(b) of article 9 has its origins in article 7, paragraph 1(b) of the UNCITRAL Model Law on Electronic Commerce 1996.

10 In the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 2001, it was already noted that article 7 of the UNCITRAL Model Law on Electronic Commerce creates uncertainty as the determination of appropriately sufficient reliability can only be made *ex post* by a court or other trier of fact. In order to create more certainty *ex ante*, Article 6, paragraph 3 of the UNCITRAL Model Law on Electronic Signatures 2001 was introduced. Paragraph 118 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 2001 states:

> … However, under article 7 of the UNCITRAL Model Law on Electronic Commerce, the determination of what constitutes a reliable method of signature in the light of the circumstances, can be made only by a court or other trier of fact intervening *ex post*, possibly long after the electronic signature has been used. In contrast, the new Model Law [on Electronic Signatures 2001] is expected to create a benefit in favour of certain techniques, which are recognised as particularly reliable, irrespective of the circumstances in which they are used. That is the purpose of paragraph 3, which is expected to create certainty (through either a presumption or a substantive rule), at or before the time any such technique of electronic signature is used (*ex ante*), that using a recognised technique will result in legal effects equivalent to those of a handwritten signature. Thus, paragraph 3 is an essential provision if the new Model Law is to meet its goal of *providing more certainty than readily offered by the UNCITRAL Model Law on Electronic Commerce* as to the legal effect to be expected from the use of particularly reliable types of electronic signatures. …" [Emphasis added]

11 At the forty-second session, the Working Group had considered two variants in paragraph 3 of article 9. Variant A was based on article 7 of the UNCITRAL Model Law on Electronic Commerce, while variant B was based on article 6, paragraph 3 of the UNCITRAL Model Law on Electronic Signatures.[350] The Working Group decided in favour of retaining variant A only.[351]

12 In choosing to retain only variant A, the Working Group may not have fully considered the implications of retaining in paragraph 3(b) of article 9, the general "reliability requirement" based on article 7 of the Model Law on Electronic Commerce.

[350] A/CN.9/546, paragraph 48.
[351] A/CN.9/546, paragraph 54-57.

13 Under paragraph 3(b) of article 9, the satisfaction by an electronic signature of a requirement of law for signature depends on whether the signature method was appropriately reliable for the purpose of the electronic communication in light of all the circumstances, as determined *ex post* by a court or other trier of fact. This means that the parties to the electronic communication or contract are not able to know with certainty *ex ante* whether the electronic signature used will be upheld by a court or other trier of fact as "appropriately reliable" and therefore not be denied legal validity, until after a legal dispute arises subsequently. It also means that even if there was *no dispute* about the identity of the person signing or the fact of signing (i.e. no dispute as to authenticity of the electronic signature), a court or trier of fact may still rule that the electronic signature was not appropriately reliable, and therefore invalidate the entire contract.

14 Such a provision will potentially have serious practical implications for electronic commerce:

(a) It will create uncertainty in electronic transactions because whether a signature method is appropriately reliable and hence not be denied legal validity will be determined *ex post* by the court or trier of fact, and not *ex ante* by the parties. Although parties can exercise party autonomy by agreeing on a signature method, it remains that the parties' agreement is only one of the factors in paragraph 3(b) of article 9 taken into consideration by the court or trier of fact.[352] Even if the parties were satisfied at the outset as to the reliability of the signature method, a court or trier of fact may rule otherwise.

(b) It could be used to the detriment of the very class of persons that the legal requirements for signature are intended to protect. A party could try to invalidate his own electronic signature as being insufficiently reliable, in order to invalidate a contract, where it is convenient to him. This would be to the detriment of the other party relying on the signor's signature. This provision then risks becoming a trap for the unwary or a loophole for the unscrupulous.

(c) It may be an impediment to electronic commerce. It will add to business costs if users feel compelled to use more sophisticated and costly technology to ensure that the reliability requirement is satisfied. Conversely, such uncertainty and additional costs may even discourage the use of electronic transactions.

15 It is noted that the reliability requirement originated from language in laws relating to the closed and heavily regulated area of funds transfer.[353] In that context, the question of

[352] This was explicitly noted at paragraph 60 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996), which states, "However, a possible agreement between originators and addressees of data messages as to the use of a method of authentication is not conclusive evidence of whether that method is reliable or not."

[353] See A/CN.9/387, paragraphs 81 to 87. At the 26th session of the Working Group on Electronic Data Interchange, which considered the Draft Provisions for Uniform Rules on the Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Trade Data Communication (which later revisions became the Model Law on Electronic Commerce), an earlier draft of article 7 contained the phrase "and the mode of identification of the sender is in the circumstances a **[commercially] reasonable** method of security against unauthorized messages", before it was suggested that the phrase be replaced by "a method of authentication is

whether the authentication or security procedure, e.g. a signature, is appropriate relates to the concept of attribution of that signature to the person. The UNCITRAL Model Law on Electronic Commerce originally needed a reliability test because it contained a general attribution rule in article 13.[354] In the Model Law on Electronic Commerce, article 7 and article 13 together affirmed the validity of an electronic signature and allowed the attribution of the data message to an originator as long as the addressee used a method agreed upon with the originator to verify the authenticity of the message, without the need to demonstrate the authenticity of the signature itself.[355] The attribution rule in the UNCITRAL Model Law on Electronic Commerce was ultimately limited to technology agreed between the signor and the relying party.

16 The draft convention does not deal with the attribution of electronic communications.[356] Therefore, the current paragraph 3(b) of article 9 of the draft convention imposes a general "reliability requirement" without any corollary attribution provision. In the absence of an acceptable attribution rule, attribution of a signature should be a matter of proof. There is no necessity for a "reliability requirement" to be introduced as a complement to a non-existent attribution rule.

17 It is noted that there is no such "reliability requirement" for the legal validity of handwritten signatures (or any of the other marks on paper that may constitute a signature at law). Common law does not impose any form requirement on signatures. A person can sign by marking a cross "X" on a document. A person can also sign by a machine that prints his name on a document. Both the cross "X" and machine-printed name are legally valid signatures, though questions of proof may arise. In each case, it is a matter of proof whether the purported signor did in fact sign in that manner and intended thereby to sign the document. In order to establish the signature's function of linking the signor with the signed document, the context of the signing will always have to be demonstrated, whether the signature is on paper or electronic.

18 It is not the form of the signature, but the proven link between the signature and the purported signor based on the context, that gives the signature its legal effect. In our view, electronic signatures are merely another form of signature, and should in principle be legally valid as signatures without any special requirements of reliability. Questions of proof of the making of the signature (which exist for both handwritten and electronic signatures) should not distort the law on the validity of signatures. If it is recognised that the legal effect of a signature is based on the proven link between the document, the signature and the purported signor, then it is irrelevant whether the signature method was of an appropriate level of reliability. In order to achieve functional equivalence between handwritten signatures and electronic signatures, there should not be any additional

---

sufficient if it is **as reliable as is appropriate** in all the circumstances to the purpose for which a communication was made". The phrase "commercially reasonable" originated from language used in article 5 of the UNCITRAL Model Law on International Credit Transfers, and Article 4A of the Uniform Commercial Code (UCC).

[354] If, as a matter of law, a signature is to be attributed to a particular person, then in fairness to that person it is necessary to ensure that the technical features of the signature are technically reliable.

[355] A/CN.9/571, paragraph 127.

[356] A/CN.9/546, paragraph 127.

reliability requirement for electronic signatures as contained in paragraph 3(b) of article 9.

19 In commercial transactions, the person relying on a signature always takes the risk that the signature is not genuine, so he evaluates the risk that the signature is not genuine and protects himself accordingly.[357] The risk analysis will of course include the cost of having the signature made more reliable and the cost of its being not genuine. So a history of dealings with the purported signor, or a low-value transaction, may persuade someone to rely on a signature that would not be satisfactory if it were from a stranger or for a high value transaction. These precautions and judgments are not a matter of law but a matter of prudence. That is, a party may not feel comfortable about relying on a signature in the form of a cross "X", but that is a judgment by that party as a matter of prudence, and not a matter of law, as the signature in the form of a cross "X" is fully valid as a signature at law. We are of the view that this analysis applies equally where electronic commercial transactions and electronic signatures are concerned.

20 We recognise that people have had many years of experience in evaluating how reliable a handwritten signature is, and therefore are able to easily judge what types of handwritten signatures are prudent to be relied upon. People are currently less familiar with the potentials and vulnerabilities of methods of signing electronically, and may be less proficient in making that prudential judgment. However, the law does not add any value to this lack of familiarity by introducing a general reliability requirement such as paragraph 3(b) of article 9. Such a reliability requirement merely transfers the prudential judgment from the relying party to the judge or adjudicator. The judge or adjudicator may be no more competent to make that prudential judgment, although he or she may have the benefit of expert evidence. Such expert evidence is also available to the relying party, but at a more useful point of time, before the transaction is consummated. As people become more familiar with electronic signatures, they will become more experienced at making that prudential judgment.

21 We note that in order to achieve the objective of harmonisation of laws relating to electronic commerce, the draft convention should contain either a uniform standard for the reliability requirement for electronic signatures (which can be in the form of a general "reliability requirement" as in paragraph 3(b) of article 9), or no reliability requirement (which will be achieved if paragraph 3(b) of article 9 were deleted). As pointed out above, the current paragraph 3(b) of article 9 creates significant uncertainty which does not promote the use of electronic commerce, and we are of the view that such a reliability requirement is unnecessary and inappropriate in the circumstances. We therefore propose that the better and more appropriate option is to have no reliability requirement for electronic signatures, and that paragraph 3(b) of article 9 be deleted.

22 If paragraph 3(b) of article 9 (and therefore the reliability requirement) is deleted, article 9 will provide that *all electronic signatures* that fulfil the functions described in paragraph 3(a) of article 9 will satisfy the requirement of law for signatures. This will

[357] This may involve checking the signature against known genuine versions of it, or getting the signature witnessed, notarized or guaranteed by a bank, etc.

provide parties with the certainty of knowing that the electronic signatures appended by them or being relied upon by them do satisfy the requirement of law for signatures, and therefore would not be denied legal validity on that basis.

ANNEX D

LEGISLATION REFERENCES

Singapore
Electronic Transactions Act (Cap.88) (1998)
Singapore Statutes online, available via *http://www.ecitizen.gov.s,* under Useful Links.

Australia
http://www.austlii.org/
Commonwealth Electronic Transactions Act 2000
New South Wales Electronic Transactions Act 2000
http://www.legislation.nsw.gov.au/
Electronic Transactions (Victoria) Act 2000
http://www.dms.dpc.vic.gov.au/

Canada
Uniform Electronic Commerce Act
http://www.ulcc.ca/
British Columbia Electronic Transactions Act (2001)
http://www.bcsolutions.gov.bc.ca/qp/
New Brunswick Electronic Transactions Act (2001)
http://www.gnb.cal
Ontario Electronic Commerce Act 2000
Manitoba Electronic Commerce and Information Act 2000

Hong Kong
Electronic Transactions Ordinance (Cap.553)
http://www.legislation.gov.hk/index.htm

Ireland
Electronic Commerce Act 2000
http://irlgov.ie/bills28/acts/2000/default.htm

New Zealand
Electronic Transactions Act 2002
http://www.legislation.govt.nz/

UK
Electronic Communications Act 2000
Electronic Commerce (EC Directive) Regulations 2002
http://www.opsi.gov.uk/

US
Electronic Signatures in Global and National Commerce Act (E-SIGN Act) (2000)
http://www.access.gpo.gov/

UNCITRAL
http://www.uncitral.org/
Model Law on Electronic Signatures (2001)
Model Law on Electronic Commerce, with Guide to Enactment (1996) and article 6*bis* (1998)
Draft Convention on Electronic Contracting draft before the 38th session of UNCITRAL (Vienna, 4-15 July 2005), see A/CN.9/577

EU
http://europa.eu.int/
Directive on Electronic Signatures (Directive 1999/93/EC)
Directive on Electronic Commerce (Directive 2000/31/EC)

The Commonwealth Secretariat
Model Law on Electronic Transactions
http://www.thecommonwealth.org

ANNEX E

LIST OF QUESTIONS

Q1. Do you have any comments on the proposal to move technology specific details in the ETA to the ETR?

Q2. Do you have any comments on the proposal to replace the current "licensing" approach to an "accreditation" approach in the ETA and ETR? (See Annex A)

Q3. Do you have any comments on the proposed amendments to the financial criteria and fees for CA accreditation?

Q4. Do you have any comments on the proposed increase in the accreditation duration from 1 year to 2 years?

Q5. Do you have any comments on the proposed amendments to limit the audit requirement to relevant security guidelines?

Q6. Is it necessary to clarify the meaning of "network service provider". Do you agree with the proposed definition of "network service provider"? (See definition proposed for discussion in paragraph 3.4.8)

Q7. Do you agree with the proposed deletion of the words "to which he merely provides access" in section 10(1) of the ETA? (See paragraph 3.4.14)

Q8. If section 10 of the ETA is amended as proposed in paragraphs 3.4.8 and 3.4.14, do you think any further safeguards are necessary? In particular, would the protection given under section 10 be too wide? (See paragraph 3.4.22). If yes, please elaborate with reference to specific kinds of liability from which network service providers should not be exempted.

Q9. Should the immunity regime for service providers under section 10 of the ETA be changed (other than the changes mentioned in Q.6, 7 and 8)?

Q10. Do you have any comments on the proposed amendments to section 9 of the ETA in Annex B?

Q11. Do you have any comments on the proposed amendments to section 47 of the ETA in Annex B?

Q12. Should Singapore adopt a single provision on electronic originals or provide specifically for different situations in which electronic communications may be used as a functional equivalent of paper or other non-electronic forms?[358] (See paragraphs 4.12.1 to 4.12.9, especially paragraphs 4.12.8 and 4.12.9).

Q13. Should consent to accept electronic originals be required? In this respect, should there be any distinction between Government agencies and private persons or entities, and if yes, what differences should there be? For example, should Government agencies be presumed to accept electronic originals unless they have opted out of doing so, as proposed in section 9A(4) in Annex B? Would your views differ if, instead of a single provision on electronic originals, there are specific provisions on the use of electronic communications in different situations? (See paragraphs 4.12.10 to 4.12.12).

Q14. Proposed sections 9 and 9A of the ETA[359] require compliance with any additional technical requirements as to form and procedure that Government agencies may have in relation to the acceptance of electronic originals. Should there be express requirements to comply with such additional technical requirements in the case where the intended recipient of electronic originals is not a Government agency? Would your views differ if, instead of a single provision on electronic originals, there are specific provisions on the use of electronic communications in different situations? (See paragraphs 4.12.13 to 4.12.16)

Q15. Do you agree that the definition of an electronic signature should not require such a signature to fulfill both an identification as well as an approval function?

Q16. Do you agree that a general provision providing for the functional equivalence of electronic signatures to handwritten signatures (e.g. section 8) should not contain any reliability requirement?

Q17. Should any laws imposing a signature requirement be clarified by prescribing the requirements as to reliability that should apply to electronic signatures? If yes, please state the legal requirement (e.g. Civil Law Act, section 6) and describe the standard that should be required of electronic signatures in order to satisfy that legal requirement.

[358] See Australian Commonwealth Electronic Transactions Act 1999 and New Zealand Electronic Transactions Act 2002. Also Canadian Uniform Electronic Commerce Act.
[359] See draft sections 9(1)(d) and 9A(1)(c) in Annex A.

Q18. What difficulties or benefits do you foresee if the provisions of article 9(4) and (5) of the draft convention (relating to originals) are adopted in the ETA?

Q19. Do you have any comments on proposed section 9A in Annex B? Do you agree with the criteria for acceptance of electronic originals in proposed section 9A(1) and (2) in Annex B?

Q20. What difficulties or benefits do you foresee if the provisions of Article 10 of the draft Convention (relating to time and place of dispatch and receipt of electronic communications) are adopted in the ETA?

Q21. What difficulties or benefits do you foresee if the provisions of Article 11 of the draft Convention (relating to invitation to make offers) are adopted in the ETA?

Q22. What difficulties or benefits do you foresee if the provisions of Article 12 of the draft Convention (relating to automated message systems) are adopted in the ETA?

Q23. What difficulties or benefits do you foresee if the provisions of Article 14 of the Convention (relating to Error in Electronic Communication) are adopted in the ETA?

Q24. What exclusions from the applicability of the Convention do you propose in the context of Singapore? Please specify legislative provisions affected where relevant. (See paragraphs 5.16.9 to 5.16.11)

Q25. Do you agree that Singapore should not adopt any of the limitations in article 18(1)? (See paragraph 5.16.12)

Q26. Should sections 13, 14 and 15 in Part IV of the ETA be allowed to apply to non-contractual transactions? (See Part 5.17.1 to 5.17.3)

Q27. Do you have any comments on whether any of the provisions of the Convention should apply to non-contractual transactions? (See Part 5.17.4 to 5.17.7)