

**NATIONAL E-COMMERCE LEGISLATION IN ASIA PACIFIC:
THE CASE IN SINGAPORE**

GOH Seow Hiong
shgoh@stanfordalumni.org

Disclaimer

The information provided in this article is not intended to be nor is it a substitute for formal legal advice, but is only intended as a general guide and discussion of the issues involved and is non-exhaustive. A reader should consult a qualified legal practitioner for specific advice in relation to e-commerce transactions and contracts that he enters into. The law is as stated in June 2004.

About the Author

Mr GOH Seow Hiong is the Director for Software Policy for Asia with the Business Software Alliance (www.bsa.org), and represents the views of BSA member companies before governments and the marketplace in the Asia Pacific region. He was formerly practising as an Advocate and Solicitor at the Singapore law firm of Rajah & Tann, where he advised clients on IT, e-commerce and telecommunication matters. He has been in the government service for over a decade prior to joining the law firm. He was formerly a deputy director of IDA, responsible for policy formulation to facilitate the development and growth of the e-commerce and ICT industries in Singapore, and for ICT security matters for the government and the industry. He received his Bachelor's Degree with Honours and Distinction in General Scholarship (equivalent of a First Class Honours) in Computer Science from the University of California at Berkeley, and his Master's Degree in Computer Science from Stanford University. He also has a Bachelor's Degree with Honours in Law from the University of London, and a postgraduate Diploma in Singapore Law with Merit from the National University of Singapore.

Overview

A nation's e-commerce legal framework can play an important role in enabling and facilitating e-commerce transactions within the country and across its borders. Such legislation creates the much-needed certainty for traditionally paper-based and physical world business transactions to be carried out in the electronic realm.

To understand the legal framework for e-commerce in Singapore, one needs to examine the foundation behind the formation of electronic contracts and the issues relating to disputes over such transactions. Hence, we will discuss the present legal framework that provides the rules upon which electronic contracts are formed. We will then discuss evidentiary issues in relation to matters of proof when it comes to disputes of electronic transactions. Finally, we will consider what is ahead for e-commerce laws in Singapore.

Foundation of Electronic Contracts

Under general contract law, there are well-established principles and rules that deal with how a legal binding contract is created. There must be an intention to create legal relations between the parties concerned, and each party must have the capacity to enter into the contract. There should be an offer made by one party and an acceptance of the offer by the other party, and there should generally be consideration¹ between the parties of the contract. The principle of privity of contract says that only a party to a contract can enforce the contract, even if the contract was for the benefit of a third party. There are however exceptions to this principle². Finally, the contract must not be one that is contrary to public policy. The application of these rules and principles together determine whether a contract is valid and binding.

In addition to the above, there are some additional concepts that apply for electronic contracts. The main legislation in Singapore governing electronic contracts is the *Electronic Transactions Act* (ETA)³. While the law of contracts broadly continues to apply both in the physical and electronic world, the ETA fills the gaps where the rules governing contracts in

¹ Consideration is the legal term given to the need for reciprocity or a bargain in contracts. It is the element of exchange, essentially a benefit to one party or a detriment to the other party.

² *Contract (Rights of Third Parties) Act* (Sing.), Rev. Ed. 2002, Chapter 53B.

³ *Electronic Transactions Act* (Sing.), Rev. Ed. 1999, Chapter 88 <<http://www.cca.gov.sg>>, referenced 30 May 2004

the physical world needs to be supplemented to deal with and support the environment enabled by new technologies. It is intended for the ETA to be construed consistently with what are commercially reasonable circumstances⁴. The ETA also provides additional legal support for new technologies to assist the court in recognising electronic evidence.

The ETA was passed in 1998 as an enabling legislation to remove the uncertainty around the legality of contracts that are formed electronically, to recognise electronic signatures and to clarify the liability of network service providers who merely carry traffic. The ETA sets out the voluntary licensing of certification authorities (CAs)⁵ as trusted third parties in the online world to provide the basis for other trust relations to be established. The *Electronic Transactions (Certification Authority) Regulations*⁶ stipulate the requirements for a CA to obtain a licence in Singapore, and the accompanying *Security Guidelines for Certification Authorities*⁷ stipulate the technical security requirements that must be met. There are also provisions in the ETA that enable Government agencies, without the need to amend their own governing Acts, to easily implement electronic systems to transact with the public. The ETA provides for the acceptance of applications and issuance of digital licences, with the ability to send and receive electronic documents in a reliable manner.

We will elaborate on and examine below the ETA provisions on electronic records, signatures and contracts, as well as their secure counterparts.

⁴ Section 3, ETA.

⁵ Technological solutions are available, if used, to prove to third parties the identity of the sender of an electronic message and to protect the integrity of such messages. Tools such as digital signatures allow for a signature (consisting of a string of numbers) to be attached to a document to provide two essential properties if the signature is successfully verified – it confirms that a document has not been tampered with since the time the signature was fixed, and it identifies the person who fixed the signature. These features of authentication and non-repudiation are not readily available with handwritten signatures. One means of the creation and verification of digital signatures is made possible through what is known as “public key encryption” or “asymmetric key encryption” technology. This involves the use of two distinct keys. They are mathematically related and randomly generated from prime numbers. The first key is known as a “private key”. It is held by and kept as a secret by the individual making the signature. The second key is known as a “public key”. This is made known to the world-at-large. A public key infrastructure facilitates the use of digital signatures. Under this infrastructure, a Certification Authority (CA) certifies (in the form of a digital certificate) that a given public key is associated with a specific individual. A CA may perform a face-to-face verification of the individual before such a certification is given. The digital certificate can subsequently be used to confirm the public key of an individual, and verify the signature that is generated by the individual. It is essential for the verifier of a signature to know that he is using the correct public key of the individual for verification.

⁶ *Electronic Transactions (Certification Authority) Regulations* (Sing.), Rev. Ed. 2001, Regulation 1 <<http://www.cca.gov.sg>>, referenced 30 May 2004.

⁷ *Security Guidelines for CAs*, September 1999 <<http://www.cca.gov.sg>>, referenced 30 May 2004.

Electronic Records, Signatures and Contracts

The ETA puts electronic documents and records on the same standing as physical documents by declaring that the validity or enforceability of such electronic versions cannot be denied their legal effect on the basis of them being electronic⁸. The ETA makes it clear that where a rule of law has a requirement for information to be in writing, an electronic record containing that information will similarly satisfy that requirement of being in writing, so long as the information can be accessed for subsequent use⁹. In the same vein, where a rule of law requires a signature, an electronic signature will also satisfy the rule of law¹⁰. The ETA has provided that an electronic signature can be proven in any manner¹¹. Where there are legal rules governing the retention of documents and records, the ETA sets out the circumstances and requirements where such rules can be satisfied by storing the information in an electronic form¹². However, where the rule of law already expressly provides for the requirements for the electronic retention of records, or where a government agency or organ of state has stipulated additional requirements, such requirements must be followed¹³. It should also be noted that in contracts, where the notice provision sets out specific mechanisms (such as notification by post or facsimile) for notifying the other party in writing, if e-mail or other electronic means are not explicitly listed as an authorised means of notification together with the other traditional mechanisms, such other electronic means may not be accepted as a valid method of giving notice.

The ETA expressly states that contracts can be formed electronically, unless the parties have agreed otherwise¹⁴. An offer and an acceptance for a contract can be made in the form of electronic records or messages. The intention of the parties to enter into a contract as conveyed in an electronic form is of equal standing as that conveyed through other traditional means¹⁵. The ETA has provisions governing attribution, i.e. how the identity of an originator and an addressee of an electronic record will be determined¹⁶. The parties can also agree on an acknowledgement of receipt of electronic records to be sent by the recipient, and the

⁸ Section 6, ETA.

⁹ Section 7, ETA.

¹⁰ Section 8(1), ETA.

¹¹ Section 8(2), ETA.

¹² Section 9, ETA.

¹³ Section 9(4), ETA.

¹⁴ Section 11, ETA.

¹⁵ Section 12, ETA.

¹⁶ Section 13, ETA.

receipt of the electronic record can be conditional upon the receipt of the related acknowledgement¹⁷. The mere receipt of such an acknowledgement can only be used to presume that the related electronic record was received, but not that the content of the record that was sent corresponds to the content that was received¹⁸.

The ETA also deals with other important elements in the formation of contracts. These include the time and place of despatch and receipt of the electronic records relating to the contract. These may be explicitly agreed between the parties, or in some circumstances, may be prescribed through regulations. In the absence of such circumstances, the despatch of a record occurs when it enters a system outside the control of the originator¹⁹. In practical terms, if a party is using a personal computer in the course of forming an electronic contract by e-mail, despatch occurs when the message sent by that party leaves his computer and enters another machine outside his control (e.g. the Internet service provider). For receipt, the timing depends on whether the recipient has designated a particular system to receive such records. If there is a designated system, the time of receipt is when the record enters that designated system. The time of receipt of a record sent to any other non-designated system is when the record is retrieved by the recipient from the non-designated system²⁰. If no system is designated, then the time of receipt is when the record enters a system of the addressee. It is therefore advantageous for an addressee to designate the information system to which such electronic records are to be sent. The addressee will need to diligently check the designated information system for new records (similar to the need to check for incoming facsimiles). However, records sent to any other non-designated system would be deemed received only when the addressee retrieves the records from such a system.

In the electronic environment, despatch and receipt can take place almost anywhere geographically with a suitable telecommunication link. Hence, to avoid ambiguity, the ETA has provided that the place of despatch and receipt is deemed to be the place of business of the originator and the addressee, irrespective of where the record was actually despatched or received²¹. Where there is no such place of business, it will be deemed as the usual place of residence²².

¹⁷ Section 14, ETA.

¹⁸ Section 14(5), ETA.

¹⁹ Section 15(1), ETA.

²⁰ Section 15(2), ETA.

²¹ Section 15(4), ETA.

²² Section 15(5), ETA.

The ETA has allowed parties in a transaction to vary any of the above general rules on electronic contracting by agreement²³. However, the ETA has provided exceptions for which the above general rules on electronic contracting will not apply²⁴. These are in:

- the creation or execution of a will;
- negotiable instruments;
- the creation, performance or enforcement of an indenture, 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.

These exceptions may be modified by a ministerial order.

Electronic Signatures and Digital Signatures, Secure Electronic Records and Signatures

The ETA defines an electronic signature as meaning any letters, characters, numbers or other symbols in a digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record²⁵. This wide definition includes digital watermarking, scanned image of handwritten signatures, digital signatures and biometric signatures as possible forms of electronic signature. Each type of electronic signature has a different level of security afforded to it.

The ETA further defines a digital signature as 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:

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

²³ Section 5, ETA.

²⁴ Section 4, ETA.

²⁵ Section 2, ETA.

- whether the initial electronic record has been altered since the transformation was made²⁶.

It is envisioned that the digital signature will be one of several technological implementation of the secure electronic signature. The ETA allows for other forms of electronic signatures to be recognised.

The ETA further provides for secure electronic records and secure electronic signatures, and the presumptions accorded to such secure forms. A secure electronic record²⁷ is one that has a prescribed security procedure or a commercially reasonable security procedure (agreed to by the parties involved) applied onto it, and it can be verified that the electronic record has not been altered since a specific point in time. The ETA provides for an electronic signature to be secure²⁸ 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 at the time the signature was made, the signature was:

- unique to the person using it;
- capable of identifying such person;
- created in a manner or using a means under the sole control of the person using it; and
- linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature will be invalidated.

An important feature of the ETA is the provision²⁹ for the following rebuttable presumptions relating to secure electronic records and secure electronic signatures that are appropriately verified:

- the secure electronic record has not been altered since the specific point in time to which the secure status relates;
- the secure electronic signature is the signature of the person to whom it correlates; and
- the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

²⁶ Section 2, ETA.

²⁷ Section 16, ETA.

²⁸ Section 17, ETA.

²⁹ Section 18, ETA.

The Act goes further to provide for the effect of digital signatures. It specifies how a digital signature will be treated as a secure electronic signature³⁰, and how an electronic record signed with such a digital signature will be treated as a secure electronic signature³¹.

Correspondingly, the evidentiary presumptions described above will apply in these instances where the associated CA is licensed³². In addition, the Act describes the general duties relating to digital signatures³³, duties of CAs³⁴, duties of subscribers³⁵, and the regulation of CAs³⁶.

The services of a CA are useful in relation to e-commerce transactions, as the transactions will be legally binding although there is no prior face-to-face contact between the parties. The use of such technology is especially useful for high value online transactions, or where the identity of the customer is of primary concern. The CA also bears some liability in the event that the CA does not correctly identify the customer.

Evidentiary Issues of Electronic Transactions

One basic feature of information systems is the alterability of the documents and records in such systems. Systems on which e-commerce solutions are built are no exception. This feature makes the nature of the information and documents stored electronically fundamentally different from their physical counterparts. Unlike physical documents, changes made to electronic documents, if not protected by additional measures, are virtually undetectable. Naturally, in the event of a dispute where such electronic documents need to be produced in court proceedings, challenges will be raised as to the reliability and admissibility of the documents.

In Singapore, the *Evidence Act* (EA)³⁷ was amended in 1995 to deal with computer output evidence. The EA was first enacted in 1893 (as the then *Evidence Ordinance*) and governs the general admissibility of evidence in court. The EA was amended in 1995 to provide for the admissibility of computer output as evidence in court. The *Evidence (Computer Output)*

³⁰ Section 20, ETA.

³¹ Section 19, ETA.

³² Licensing of CAs under the ETA is voluntary.

³³ Sections 23-26, ETA.

³⁴ Section 27-35, ETA.

³⁵ Section 36-40, ETA.

³⁶ Section 41-46, ETA.

³⁷ *Evidence Act* (Sing.), Rev. Ed. 1997, Chapter 97.

*Regulations*³⁸ were promulgated in 1996 to establish the criteria for certifying imaging systems that can archive documents in an electronic form to be recognised under the EA. These amendments permitted the use of information stored in computers to be extracted as computer output and used in court. The amendments provide for the admissibility and weight of computer output to be used as evidence in criminal and civil proceedings, and allow for the accurate reproduction of documents by electronic or other technical processes to be admissible as secondary evidence.

The 1995 amendments to the EA provide for three ways for computer evidence to be admitted:

- by express agreement between the parties in the proceedings that the authenticity and accuracy of the contents are not disputed³⁹;

This method of admitting evidence requires both parties in the proceedings to agree that the computer output should be admitted as it is. This agreement can occur at any time, either before or during the proceedings.

- by showing that the computer output was produced by an approved process⁴⁰;

This method deals with computer output produced by an approved process. A process is approved when it has been audited and certified by an agency that is appointed by the Ministry of Law to be a Certifying Authority⁴¹. The Certifying Authority will audit the process in accordance with the published compliance criteria in order to certify it. Once the process is certified and approved, there will be a presumption under the law that the computer output produced by the approved process is accurate, unless it is proven otherwise.

The regulations on the compliance criteria for imaging systems were published as the First Schedule of the 1996 Regulations. The criteria in the regulations establish how businesses can seek certification and approval for their imaging systems so that they

³⁸ *Evidence (Computer Output) Regulations* (Sing.), Rev. Ed. 1997, Regulation 1.

³⁹ Section 35(1)(a), EA.

⁴⁰ Section 35(1)(b), EA.

⁴¹ To be distinguished from a Certification Authority under the ETA.

can be used to transform physical documents into electronic form, discard the physical copies and rely on the electronic copies⁴².

- by showing that the computer output was generated by a computer that was at all material times operating properly⁴³.

In this method, the party tendering the output will have to prove to the court the accuracy of the computer output. The system operator, manager or other experts may tender evidence to certify that the computer producing the output was operating properly and the computer output is correct and reliable. There should be no reasonable ground to believe that the electronic record is inaccurate, untruthful or unreliable. If there was any malfunction in the system, it should be shown that the malfunction was immaterial. Unlike the situation for the approved process, the accuracy of the output is not presumed, but needs to be proven.

There are additional provisions that supplement and support the three methods enumerated above. The EA provides⁴⁴ that if the court is not satisfied with the evidence given with the above three methods, it may call for further evidence to satisfy itself of the accuracy of the output from:

- a person responsible for the operation or management of the Certifying Authority;
- a person responsible for the operation of the computer;
- a person who had control or access over any relevant records and facts relating to the production of the computer output; or
- an expert appointed or accepted by the court.

In ascertaining the weight of the computer output that is to be admitted, the factors that the court will consider are⁴⁵:

⁴² The Auditor-General was also appointed as a Certifying Authority under the 1996 Regulations, primarily for the purposes of auditing government systems. In addition, the Ministry of Law, through the Appointment of Certification Authorities notification (*Appointment of Certification Authorities* (Sing.), Rev. Ed. 1997, S 273/2001), has also appointed several other commercial organisations as Certifying Authorities for the private sector. These appointments are for renewable fixed terms.

⁴³ Section 35(1)(c), EA.

⁴⁴ Section 36(1), EA.

⁴⁵ Section 36(4), EA.

- the circumstances from which any inference can be reasonably drawn as to the accuracy of the output;
- whether the information in the electronic record was recorded contemporaneously with the facts dealt with in that information;
- whether any persons involved had any incentive or motive to conceal or misrepresent the information in question.

With the first method (express agreement), in practice, if a dispute has arisen and the point of contention concerns the accuracy of the records, agreement is unlikely to be reached. As such, it is useful to have a prior agreement before the dispute arises (e.g. at the time of the making the contract) that the computer output will be accepted.

The advantage of using the second method (approved process) is that once a system owner has its system certified and approved, the system records stored in that system and produced as computer output will be presumed accurate, and the onus will be on the disputing party to prove otherwise. This is a strong advantage for the system owner, and it can be a very onerous burden for another party without access or knowledge of the system in question to challenge the presumption.

The third method is a fall back provision, where in the absence of any agreement or the use of an approved process, it is left to the parties to prove the reliability of the output. Once proven, the electronic document may then be admitted as evidence.

For e-commerce systems, the EA and ETA offers two avenues through which the records of e-commerce transactions can be proven in court in the event of a dispute. The appropriate framework to be adopted for any particular system depends on the particular characteristics of the technical system in use, and the nature and the manner in which the transaction is conducted. The two approaches offers flexibility for the parties to choose an approach that best meets the business and legal requirements while balancing the security and usability requirements of the transaction.

Looking Ahead

The Singapore Government has called for a public consultation to review the country's cyber legislation. The scope of the review includes the ETA and the *Electronic Transactions (Certification Authority) Regulations*. The objective of the review is to update and fine tune the legislation and regulations to address the changing environment and international developments since the original enactment some five years earlier. The changes to the law are expected to be made by the first quarter of 2005.

The consultation is conducted in three stages through consultation papers⁴⁶ issued by the Infocomm Development Authority of Singapore and the Attorney-General's Chambers. The first stage is to deal with electronic contracting issues. The second stage is to deal with areas of exclusions under the legislation, and the third stage will deal with electronic signatures and certification authorities. Only the first two stages of the consultation have been released so far.

In the first part of the consultation dealing with issues of electronic contracting in the ETA, feedback on six broad areas was sought:

- The first area is in relation to party autonomy. The issues under consideration are whether the law should compel parties to accept offers and acceptances in the electronic form, and whether there should be certain mandatory requirements in electronic contracting that are not open to variation by the parties.
- The second area is in relation to the recognition of electronic signatures. The issue being considered is whether the UNCITRAL requirements in relation to function and reliability requirements are consistent with the provisions currently under the law.
- The third area is in relation to the formation of contracts. The issues under consideration include whether there should be a provision relating to when offer and acceptance in the electronic world should take effect, and whether a proposal to enter into an electronic contract made to the world-at-large should be considered an invitation to make an offer.
- The fourth area is in relation to the rules on time and place of despatch and receipt. The issue under review is whether the present rules should be amended to be

⁴⁶ Available at <http://www.ida.gov.sg> and <http://www.agc.gov.sg>.

consistent with UNCITRAL relating to the control over the electronic message and the capability to retrieve messages rather than the information system being used.

- The fifth area is in relation to automated systems. The issue under consideration is the status of electronic contracts resulting from the interaction with automated systems, as well as issues relating to errors made by a person in communication with an automated system.
- The sixth area deals with miscellaneous issues such as the validity of incorporation of terms and conditions by reference in electronic communication, the manner which originality of an electronic document is to be addressed, and whether legislation relating to the sale of goods in the physical world applies to electronic goods.

In the second part of the consultation on the exclusions under Section 4 of the ETA, the rationale behind the exclusions is considered and feedback is sought on whether the exclusions should be retained or modified. The recommendations in the consultation paper are that no changes be made with respect to wills, negotiable instruments and documents of title. In addition, the following are considered:

- For indentures, it is recommended that secure electronic signatures may be allowed to satisfy the requirements of sealing a deed.
- For trusts, the proposal is to limit the exclusion only to testamentary trusts and trusts relating to land.
- For power of attorney, the consultation paper reflects that there are benefits to remove the exclusion, although some jurisdictions limit the exclusion to certain types of powers of attorney.
- For transfer of immovable property, instead of a wide exclusion, consideration is being given to whether certain classes of people or types of land transactions should be allowed.
- For carriage of goods (including documents of title and negotiable instruments), feedback is sought on whether it should be permitted in a manner consistent with the UNCITRAL Model Law on Electronic Commerce.

The consultation also welcomes any other feedback on additions or amendments to the exclusions presently provided under Section 4 of the ETA. The consultation period for the first stage has already concluded and the second stage closes in August 2004.