Electronic Commerce Law: Singapore

Lim Wee Teck
Electronic Commerce Law: Singapore
Lim Wee Teck

The Electronic Transactions Act (‘ETA’) is the primary legislation governing electronic commerce in Singapore. Under the ETA, contracts concluded on-line have the efficacy accorded to written contracts. However, on-line contracts have their own unique issues as to authenticity and accuracy. The article looks at how the ETA attempts to resolve these issues, and the further issues that arise from the ETA provisions.

Introduction

Singapore’s push to become a hub for information technology has seen steps being taken to create a favourable and attractive environment in Singapore for information technology companies. Part of these steps have included putting in place the legal infrastructure to facilitate and regulate e-commerce.

In 1998, the Singapore legislature passed the Electronic Transaction Act 1998 (‘ETA’) to deal with e-commerce. Prior to 1998, subsidiary legislation was put in place regulating Internet Content Providers and Internet Service Providers (namely, the Singapore Broadcasting Authority (Class Licence Notification) 1996 and the Singapore Broadcasting Authority (Exemption) Notification 1996) and the Singapore legislature enacted legislation to deal with computer hacking (the Computer Misuse Act).

More recently, various amendments to existing legislation and subsidiary legislation have also been put in place rationalising the existing law to cope with moves in various industries towards the electronic framework. The amendments have dealt with computer and electronic evidence, copyright, income tax concessions for cyber-trading, electronic dealings in securities and futures, electronic prospectuses, and most recently, deregulation of the telecommunications industry.

This article will focus on the ETA as it remains the primary piece of legislation governing e-commerce in Singapore.

Contract Law In an E-Commerce Environment Generally

Singapore contract law is based on English common law. Accordingly, the basic common law requirements as to the formation of a contract apply: intention to create legal relations, capacity to contract, offer and acceptance, consideration and certainty of terms.

These basic requirements remain necessary whether the contract is made orally, on a paper document or on-line. In order to facilitate electronic commerce, the ETA has removed any doubts that these same requirements can be fulfilled in electronic form.
The validity of electronic contracts is confirmed by Part II of the ETA, which affirms the validity of electronic records in both the formation of the contract as well as pre-contractual statements.

The basis of formation of every contract is offer and acceptance, and section 11(1) of the ETA provides that, unless agreed to by the parties, an offer and/or acceptance may be expressed in electronic records. Section 11(2) of the ETA states that where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose.

Sometimes in the negotiation of a contract, pre-contractual statements and representations may be made. Where any of these statements are made by way of an electronic record, section 12 of the ETA provides that such statements have the same effect as they would have if made non-electronically.

Certain contracts are required by Singapore law to be in writing. For example, under section 6 of the Civil Law Act, guarantees have to be evidenced in writing. Section 7 of the ETA makes it clear that 'an electronic record satisfies that rule of law if the information contained therein is accessible so as to be usable for subsequent reference'.

It should be noted that section 7 does not apply to all contracts, as section 4 of the ETA excludes certain documents and contracts from its, among others, effect. Specifically, the following types of documents and contracts are excluded:

- 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.

Contracts may also be signed and section 8 of the ETA recognises electronic signatures, and provides for their proof: '[a]n 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

---

1 An ‘electronic record’ is defined in the ETA, section 2 as ‘a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another’.

2 An ‘electronic signature’ is defined in section 2, 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 or approving the electronic record’.
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’.

Contracting On-line: Authenticity And Accuracy

To promote e-commerce, the recipient of, say, an on-line offer, needs to know that the message is authentic, in other words, that he will be able to enforce any contract which he enters into, without fear that the counterparty will deny that he was the one who sent the offer. The recipient also needs to know that the message is accurate, that say, the offer to purchase 20 cats is not in fact originally an offer to purchase 20 hats that had been tampered with.

In relation to these issues, the ETA distinguishes between three types of electronic records:

• electronic records generally
• secure electronic records and/or electronic records signed with a secure electronic signature; and
• secure electronic records signed with a secure digital signature.

A recipient’s right to treat the electronic record as authentic and accurate, and the matters that he is required to prove, varies depending on the type of electronic record received. This approach allows for flexibility bearing in mind the protean nature of technology and the varying standards used from country to country.

Electronic Records Generally

Where an electronic record is actually sent by its originator, or the originator’s authorised agent, or by an information system programmed by or on behalf of the originator to send messages automatically, authenticity is not in question (barring a bare faced denial by the originator).

Section 13 of the ETA confirms that in these circumstances, the electronic record is that of the originator’s.

The issue of authenticity arises where the recipient receives an electronic record which the signatory denies was in fact sent by him. Does the recipient have to prove that the signatory of the electronic record in fact sent the message? If that was the case, the electronic/digital format of the electronic record would render this a very heavy burden for the recipient to prove. Accordingly, the ETA does not require the recipient to do this.

Under what circumstances is the recipient of the message entitled to regard the electronic record as originating from the signatory? There are two general tests that apply and these are set out in section 13(3) of the ETA:

‘As between the originator and the addressee, an addressee is entitled to regard an electronic record as being that of the originator and to act on that assumption if —

---

5 An example is where an e-mail service sends automatic leave of absence messages.
(a) in order to ascertain whether the electronic record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify electronic records as its own.

It should be noted that in both these tests, where the authenticity of the electronic record is disputed, the addressee is not required to prove that the electronic record in fact came from its signatory.

Under the section 13(3)(a) test, the recipient merely has to prove the existence of a prior agreement and that he adhered to the procedures specified in the prior agreement. However, comparatively few recipients will have the benefit of a prior written agreement.

Under the section 13(3)(b) test, the recipient has to prove that the purported originator of the electronic record enabled a third party access to the method used to identify electronic records as his. Here, since such information is unlikely to be in the possession of the recipient, it is suggested that, practically, it will be very difficult for the recipient to be able to show this where an originator denies that electronic record in fact came from him.

A further difficulty with section 13(3) is that it states that while it grants the recipient the right to regard the electronic record as being that of the originator's and to act on this assumption, it is unclear what this actually entails in legal terms. Does it, for example, accord a right on the recipient to render the originator liable on the online contract?

As regards accuracy, section 13(5) of the ETA provides that 'where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the electronic record received as being what the originator intended to send, and to act on that assumption.' The issues facing a recipient of such an electronic record are the same as with the assumption of authenticity.

**Secure Electronic Record And/Or Electronic Record Signed With Secure Electronic Signature**

Section 18(2) of the ETA provides that where an electronic record is signed using a secure electronic signature, a presumption is raised (rebuttable by contrary evidence) that the secure electronic signature is that of person to whom it correlates, and that the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.
What constitutes a secure electronic signature is set out in section 18(4) of the ETA which states that a secure electronic signature is one that is treated as a secured electronic signature by virtue of sections 17 or 20 of the ETA (which deals with secure digital signatures and is accordingly dealt with under the next sub-heading).

Section 17 of the ETA provides:

‘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.’

Again, the recipient does not have to prove that the purported originator actually signed the electronic record. He does have to show, however, that the secure electronic signature was one that met the criteria set out above, and also that a ‘prescribed security procedure’ or a ‘commercially reasonable security procedure agreed to by the parties involved’ was applied.

A ‘prescribed security procedure’ is one that is prescribed by the Minister pursuant to section 61 which states that the Minister may ‘make regulations to prescribe anything which is required to be prescribed under this Act’. As at this date, no security procedure has been ‘prescribed’ by the Minister.

A ‘commercially reasonable’ security procedure is to be determined according to criteria set out in section 16(2) of the ETA. Section 16(2) states that:

‘…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.’

Accordingly, the recipient would have to show both a prior agreement and that the security procedure agreed on was ‘commercially reasonable’ within the meaning of section 16(2).

Once he is able to do this, the burden of proof would then fall on the purported originator to show that he was not the person who sent the electronic record.

The accuracy of the electronic record is dealt with under section 16(1) which provides:

‘If a prescribed 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 from such specific point in time to the time of verification.’

The same factors must be shown as with the issue of authenticity and such a secure electronic record will be presumed to have not been altered since the specific point in time to which the secure status relates (section 18(1) of the ETA).

**Secure Electronic Records Signed With A Secure Digital Signature**

Secure electronic records signed with a secure digital signature are a sub-set of secure electronic records generally. Under section 20 of the ETA:

‘When any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature 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 a licensed certification authority operating in compliance with the regulations made under section 42;
(ii) the certificate was issued by a certification authority outside Singapore recognised for this purpose by the Controller pursuant to regulations made under section 43;

(iii) the certificate was issued by a department or ministry of the Government, an organ of State or a statutory corporation 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.’

Sections 42 and 43 referred to in section 20 essentially provide a framework by which secure digital signatures verified by a reliable third party entity may be used.

The presumptions raised under section 18 of the ETA as to authenticity and accuracy apply equally to secure electronic records signed using a secure digital signature. The advantage of using a secure digital signature under section 20 is that, unlike section 17 which requires proof of a host of facts before the status of ‘secure electronic signature’ may be accorded, the recipient of an electronic record merely has to show that he relied on the fact that the electronic record was signed using a digital signature which satisfied any one of the requirements set out in section 20. Generally speaking, this would merely entail reliance on approved or licensed authorities.

When A Contract Made On-line Is Formed

Under Singapore contract law, a contract is concluded when an offer is accepted. To be effective, the acceptance must be communicated to the offeror and the rules that have been applied under English contract law as to when the acceptance is to be treated as communicated apply in Singapore as well.

Accordingly, for written communication, an acceptance by post is effective when the letter is posted to the offeror, and an acceptance by fax is effective when the fax is received at the offeror’s machine. The ETA is silent as to when a contract is formed although it does stipulate when an electronic record is ‘sent’ and ‘received’.

An electronic record is ‘sent’ 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. If the addressee has designated an information system for the purpose of receiving electronic records, receipt occurs (i) at the time when the electronic record enters the designated information system; or (ii) if the electronic record is sent to an information system of the addressee that is not the designated information system, at the time when the electronic record is retrieved by the addressee. If the addressee has not designated an information system, receipt occurs when the electronic record enters an information system of the addressee.
Conclusion

While the ETA has been one of the first pieces of legislation passed to govern and regulate the growth of e-commerce initiatives, legislative development did not stop there and short after, amendments to legislation and subsidiary legislation were put into effect to deal with other areas of e-commerce development which were briefly outlined in the introduction. Suffice it to say, however, that the coming year will undoubtedly see further changes as governments, both in Singapore and world wide, strive to harness the behemoth of the Internet.

◆ This article was first printed in Asia Business Law Review, July 2000.