15th BILETA Conference: "ELECTRONIC DATASETS AND ACCESS TO LEGAL INFORMATION".

Friday 14th April 2000.
University of Warwick, Coventry, England.

Electronic Commerce: A Comparative Analysis of the Malaysia Digital Signature Act 1997 and the Singapore Electronic Transaction Act 1998

Zinatul A. Zainol

Faculty of Law

Universiti Kebangsaan Malaysia

Bangi, Malaysia

Abstract

Both Malaysia and Singapore are geared at becoming trusted international electronic commerce hub (e-commerce) hub. To this end, Malaysia has enacted the Digital Signatures Act in 1997 and a year later, Singapore enacted the Electronic Transaction Act. The two Acts share two main objectives; to encourage electronic commerce and to boost both countries claim that they are providing a conducive legal framework to facilitate electronic commerce.

This paper seeks to adopt a comparative analysis of the two Acts. It will be focussed on two main theme; formation of electronic contract and secure e-commerce.

Keywords:

Electronic commerce, Malaysia, Singapore, digital signature, contract, certification authorities, security, electronic messages

1. Introduction

Both Malaysia and Singapore are geared at becoming trusted international electronic commerce (e-commerce)[1] hubs. Both countries are committed at providing a secure and effective legal, as well as technical framework to boost e-commerce. The past few years saw a consequential legislative endeavour, both in Malaysia and Singapore in the area of information technology law.

Four years ago, Malaysia establishes the Multimedia Super Corridor (MSC). The purpose of the MSC is to *enable Malaysia to leapfrog into the information age and to create an ideal environment that will attract world class companies to use it as a regional multicultural information age hub.* (Mohammad; 1998) In 1997, Malaysia enacted the Digital Signature Act (DSA), and is part of a larger legislative framework, known as 'Cyberlaws' - which clearly demonstrate the government's commitment in preparing the country for the information age. The purpose of the Malaysia DSA is to facilitate the growth of multimedia industry and e-commerce in Malaysia and is based

substantially on the Utah Digital Signature Act of 1996. (Chong; 1998) The other Cyberlaws are the Computer Crimes Act 1997, the Telemedicine Act 1997 and the 1997 Amendment to the Copyright Act. In 1999, the new Multimedia and Communication Act was passed.

The Singapore Electronic Transaction Act (ETA), passed in 1998, is based on the UNCITRAL Model Law on Electronic Commerce as well as the Illinois Electronic Commerce Security and the Utah Digital Signature Act.(Phang, Seng; 1999) The Singapore ETA seeks to provide a balance between a comprehensive legal regime and maintaining business efficacy.(Namazie; 1998)

This paper aspires to offer a few comparative comments and analysis with respect to the Malaysian Digital Signature Act 1997 and the corresponding Singaporean Electronic Transaction Act 1998. The two Acts share two main objectives: to encourage electronic commerce and to promote both countries claim that they are providing a conducive legal framework to facilitate e-commerce. Yet, they differ in terms of how and to what extent e-commerce should be regulated.

Before proceeding further, a few prefatory points must be outlined. Firstly, both Acts recognises public key-infrastructure. Secondly, the Malaysia DSA is a modest statute on digital signature and is focussed primarily on the legal recognition of electronic documents signed by digital signatures as well as the establishment and liability of certification authorities. The Singapore ETA, adopts a rather extensive approach. The Act, among other things, seeks to enact a Commercial Code to support e-commerce transactions and to help to establish uniformity of rules.[2]

2. Electronic Contracts

Our traditional contract law assumes that most contracts will take the form of a written offer and a written acceptance. (Munir; 1999) and the issue of formation of contract is often resolved by distinguishing between instantaneous or non-instantaneous mode of communications. Technological advances such as fax, telex and the internet pose a challenge to the traditional notion. More often than not, the conventional law and principles are stretched to fit new and prevailing situations.

The Singapore ETA, which is based largely on the provisions of the UNCITAL Model Law on Electronic Commerce, deals rather extensively about electronic contracts in Part IV (s. 11 - s. 15) of the ETA. In contrast, the Malaysia DSA, is totally silent on this issue. However, at the time Malaysia enacted the DSA, the other subsisting digital signature legislation, which is the Utah Digital Signature Act, is also silent on the same issue. As such, in Malaysia, guidance on issues relating to electronic contracts will have to be sought from the shoulders of the Contacts Act 1950. (Zainol; 1999)

2.1 Formation of electronic contract

s. 11(1) of Singapore ETA, provides that 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 an acceptance of an offer may be expressed by means of electronic records.[3]Section 11(2) of the ETA also clarifies 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.

It appears that the above provisions are purely clarificatory and does not impact on the substantive common law of contract of Singapore. (Phang, Seng; 1999) With this in mind, the approach taken by the Malaysia DSA can be rationalised on practical grounds. The issue of formation of electronic contract can be resolved by referring to the Malaysia Contract Act 1950 and the English Common Law. S

2.2 Attribution of electronic messages

In the traditional face-to-face communication, it is relatively easy to determine who is the sender of a message but, in a faceless world, attribution is one of the key issues that must be resolved. The Singapore ETA has a set of escalating rules that are summarised as follows: (Seng; 1999)

Rule 1: If A (the party who allegedly sent the electronic message - referred to in the Acts as the "originator") did send the message to B (the party who allegedly received the electronic message - referred to as the "addressee"), the message is A's.[4]

Rule 2: If B receives a message allegedly sent by A, it will be deemed to be A's message if it was sent by A's agent.[5]

Rule 3: If B receives a message allegedly sent by A, it will deemed to be A's message if it was sent by a computer system programmed by A, or programmed by A's agent.[6]

Rule 4: If B receives a message allegedly sent by A, B is entitled to regard it as A's if B applied a procedure, either previously agreed to by A or implemented by someone related to A, for verifying that the message is A's[7], but not from the point in time when A informed B that the message is not his, and gives B reasonable time to act[8], or when B knows or ought to know that the message was not A's[9]or if in all the circumstances of the case, it is unconscionable for B to regard the electronic record as that of A or to act on that assumption.[10]

The above rules are, in principle, in line with the general principles of the law of agency, though the ETA explicitly provides that nothing in this section shall affect the law of agency or the law on the formation of contract.[11] This suggests that the whole part on attribution is not substantive, but rather procedural in nature. (Phang, Seng; 1999)

2.3 Receipt of electronic messages

When parties negotiate via an electronic network, it is desirable that they impose a requirement that the receiver of the message confirms its receipt with the sender of the message. This is particularly important when the parties are transmitting crucial messages such as ordering information or invoices.

Section 14 ETA addresses this issue and deals with the situations where the originator has agreed or requested that the recipient acknowledge the receipt of the electronic record. Where the parties do not specify that the acknowledgement be given in a particular form or method, it may be given by any communication to the addressee, automated or otherwise,[12] or by any conduct of the addressee, which is sufficient to indicate to the originator that the electronic record has been received.[13] If the originator states that the electronic records is conditional upon receipt of the acknowledgement, the electronic record is of no effect and will be treated as if it had never been sent, until the acknowledgement is received.[14] On the other, if the originator did not expressly state that his message is conditional upon receipt of the acknowledgement, he may give notice to the addressee and reimpose the requirement of acknowledgement.[15]

The receipt of the acknowledgement gives rise to a presumption, unless evidence is tendered to the contrary that the recipient has received the related electronic record. However, that presumption does not imply that the content of the electronic record has not been tampered or altered with in transit. [16]

2.4 Time and place of despatch and receipt

In an electronic environment, it is a moot point whether the

common law rules of communication of offer and acceptance should equally apply to electronic communications. Distinction is often made between instantaneous and non-instantaneous mode of communication.

In an electronic environment, it is a moot point whether the common law rules of communication of offer and acceptance should equally apply to electronic communications. Distinction is often made between instantaneous and non-instantaneous mode of communi

It has been suggested that the common law receipt rule will apply in situations where electronic communications is made by some kind of instantaneous mode of communication, particularly where there is a direct link between the trading parties (Reed; 1996) Alternatively, the common law postal or despatch rule will apply where the electronic records are stored in the network for some period of time for re-transmission before it is delivered to the addressee. (Phang, Seng; 1999)

It has been suggested that the common law receipt rule will apply in situations where electronic communications is made by some kind of instantaneous mode of communication, particularly where there is a direct link between the trading parties (Reed; 1996)

S. 15 ETA addresses this issue and 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.[17] An electronic record is deemed to be despatched at the place where the originator has its place of business, and is deemed to be received where the addressee has his place of business.[18]

An electronic record is received when it enters an information system that the addressee has designated for receiving messages.[19]If the electronic record is sent to a non-designated information system, receipt occurs at the time when the electronic record is retrieved by the addressee.[20]But, where no information system has been designated, the electronic record is received when it enters an information system of the addressee.[21]

The Malaysian position on despatch and receipt of electronic communication is even less settled. The Malaysia DSA is totally silent on this point. The rule therefore, is to be found in the Contract Act 1950. S. 4 of the Act sets out the principles regarding the communication and revocation of offer (or proposal in the terminology of the Act) and acceptance. The Act provides that the communication

of acceptance is complete (a) as against the proposer, when it is put in the course of transmission to him, so as to be out of the power of the acceptor; and (b) as against the acceptor, when it comes to the knowledge of the proposer

A literal interpretation of s. 4 of the Act, would suggests that in Malaysia, there is no distinction between instantaneous and non-instantaneous mode of communication. (Zainol; 1999) This means the position in Malaysia is somewhat different from that of the common law. Postal acceptance is not complete upon posting and the acceptor is at liberty to revoke or cancel his acceptance before it reaches the acceptor.

3. Secure E-Commerce

Another significant issue that must be addressed is the issue of the security of electronic commerce. Parties to electronic contracts must be satisfied that the sender and receiver in the electronic transactions are whom they purport to be. They must also be convinced that their electronic record can be authenticated and not forged while in transit.

The Malaysia DSA, as the name suggests, is a digital signature legislation and therefore, is directed primarily on digital signatures and certification authorities. The Singapore ETA covers broader aspects of electronic commerce. Under the Malaysia DSA, the provision on Digital Signatures is compressed in part V of the Act but under the Singapore ETA, the corresponding provisions are more detailed and elaborated in three parts, i.e. Part II (Electronic Records and Signatures Generally), Part V (Secure Electronic Records and Signatures) and Part VI (Effect of Digital Signatures).

3.1 Signatures

Both the Malaysia DSA and the Singapore ETA share an important feature. They grant legal validity and sanctity to digital signatures. They declare that where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature (or electronic signature, as used in the Singapore ETA).[22] However, if reliance on the digital signature is not reasonable, the person relying on the digitally signed electronic record (or the recipient, in the terminology of the Malaysia DSA) assumes the risk that the digital signature is invalid or forged.[23]

The concept of a signature is already very wide because it is not confined to hand-written signatures. It appears to be a logical extension to stretch out the same concept into the electronic environment. (Seng; 1999) The Malaysia DSA goes further to declare that notwithstanding any written law to the contrary, (a) a document signed with a digital signatures in accordance with this Act shall be legally binding as a document signed with a hand-written signatures, an affixed thumb-print or any other mark; (b) a digital signatures created in accordance with this Act shall be deemed to be a legally binding signature[24]

The terms 'digital signature' and 'electronic signature', however, are terms of art. (Wu; 2000) Under the Malaysia DSA, a digital signature is defined as a transformation of a message using an asymmetric cryptosystem such that a person having the initial message 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 message had been altered since the transformation was made.[25] The definition of the digital signature under the Singapore is couched in similar vein but it is interesting to note that the Act interprets digital signature to mean electronic signature. A commentary of the Act observes that digital signature is a secure form of electronic signatures. (Seng; 1999)

Both Acts adopt a very specific definition of digital signatures - asymmetric cryptosystem. At the Bill Stage of the Malaysia DSA, this approach has been heavily criticised by the Opposition Party who feels that the DSA should be technologically neutral. *But, at the current state of play pubic key cryptography is one of the most viable solutions for digital signatures - it has been extensively tested and peer reviewed, it is mathematically sound, easily available, cost-effective and transportable.* (Chong, 1998)

Under the Singapore ETA, an electronic signature is declared to be secure if it can be verified by a prescribed or commercially reasonable security procedure, provided that at the time when the signature was made, the signature is (a) unique to the person using it; (b) capable of identifying that person; (c) created in a manner under the sole control of the person using it; and (d) linked to the electronic record in such a way that if the electronic record was changed, the signature would be invalidated.[26]A secure electronic signature, shall be presumed, unless evidence to the contrary is adduced that it is the signature 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.[27]

The Malaysia DSA has a provision with similar effect. It declares that in adjudicating a dispute involving a digital signature, the court shall presume that where the digital signature is verified by the public key listed in a valid certificate, issued by a licensed certification authority, (a) that digital signature is the signature of the subscriber listed in the certificate; (b) that digital signature was affixed with the intention of signing the message; and (c) that the recipient of the digital signature has no knowledge or notice that the signer has breached a duty as a subscriber or that the signer does not rightfully hold the private key used.[28]

Even though digital signatures are declared to be a legally binding signature, there are several laws in Singapore that insist on writing or handwritten signatures. Section 4 of the ETA expressly provides that Part II (Electronic Records and Signatures Generally) and Part IV (Electronic Contracts) shall not apply to any rule of law requiring writing or signatures in any of the following:

(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 trust;

(d) any contract for the sale or 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.

The Minister however reserves the power to alter or modify the list.[29]It is felt that the Singapore ETA should not change some rules but with the increased awareness and confidence in electronic transaction, hopefully, the distinction will soon be no longer necessary. (Seng; 1999) In contrast, no similar provision can be found in the Malaysia DSA. It merely stipulates that the law does not preclude any symbol from being valid as a signature under any other applicable law.[30]

3.2 Requirement of Writing and Electronic Records

Where law requires a document information to be written, in writing or provides for certain consequences if it is not, the Singapore ETA declares that an electronic record satisfies that rule of law if the information contained therein can be retrieved for subsequent references.[31]The Act further affirms that an electronic record shall not be denied legal effect, validity or enforceability

solely on the ground that it is in the form of an electronic record.[32]The effect of this provision is that an electronic record is an equivalent to the traditional, non-electronic electronic record. In Malaysia however, no similar provision can be found in the Malaysia DSA.

3.3 Certification Authorities

In a public-key infrastructure scheme, Certification Authorities play a very prominent role. As trusted third parties, Certification Authorities certifies and identifies users electronically by issuing electronic identification certificates.

For a digital signature to enjoy legal status, it must be certified by a Certification Authority.

In Malaysia, licensing of Certification Authority is mandatory.[33] At the moment, DigiCert is the only licensed Certification Authority in Malaysia. This approach is adopted so that there is uniformity in the certification industry, and that regulation of digital signatures can be done more effectively. (Annamalai; 1997) although (Alkeniz; 1997) argued that licensing TTP, instead of increasing security, will in fact make electronic commerce less secure.

Therefore, in Malaysia, a digital signature is legally valid only if it is certified by a licensed Certification Authority. In fact, it is an offence to carry on or operate, or hold out as Certification Authority, unless that person holds a valid licensed under the Act. Upon conviction, it may be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding ten years or both.[34]

Although in Malaysia, licensing of Certification Authority is mandatory, this does not mean that a certificate issued by an unlicensed Certification Authority is invalid. In fact, the Act specifically provides that the licensing requirements under the Act shall not affect the effectiveness, enforceability and validity of any digital signatures.[35]The Act further provides that the liability limits for certification authorities and the effect of digital signatures, as provided for under the Act, shall not apply to unlicensed Certification Authorities.[36]Therefore, if an unlicensed Certification Authority is used, the validity of the digital signatures would be governed by a contract between the contracting parties, instead of the Malaysia DSA.

The Singapore ETA adopts a different approach. Licensing under the Singapore ETA is voluntary so that closed network may use their unlicensed Certification Authority. (Ter; 1999) But, It is not correct to assume that Unlicensed Certification Authority is not regulated. (Seng; 1999) They would still have to abide with other relevant provision of the Singapore ETA, such as the duties of certification authorities. In Singapore, digital certificates are recognised if there are issued by three bodies; licensed Certification Authorities, foreign Certification Authorities recognised by the Controller of Certification Authority[37], Government Department or Ministries approved by the Minister[38]and the parties may expressly agree between themselves to use digital signature which is property verified by reference to the sender's public key.[39]

5. Conclusion

Both the Malaysia DSA and the Singapore ETA represent each country's attempt to provide a conducive legal framework for electronic commerce. As we have seen, the Malaysia DSA concentrates on the legal recognition of digital signature but the Singapore ETA attempts to give electronic commerce transactions the legal recognition they deserves.

It is interesting whether the Malaysia DSA will follow the Singapore ETA's approach in regulating electronic commerce transactions. Both Acts are still in their infancy stage, and it is only with the passage of time that will decide whether the two Acts are adequate to boost both country's claim that they are providing conducive legal framework for electronic commerce.

Bibliography

Annamalai, Nagavalli (1997) Cyberlaws of Malaysia - The Multimedia Super Corridor, 12 Journal of International Banking, p 473

Alkeniz et al (1997) Cryptography and liberty: Can trusted third parties be trusted? http://elj.warwick.ac.uk/jilt/cryptog/97

Chong, John (1998) A Primier on Digital Signatures and Malaysia's Digital Signatures Act 1997, Computer Law & Security Report Vol 14 no 5, p. 322

Mohamad, Mahathir (1998) Excerpts From the Speeches of Mahathir Mohamad on the Multimedia Super Corridor, Pelanduk Punlications, Malaysia

Munir, Abu Bakar (1999) Cyber law Policies and Challenges, Butterworths Asia, Kuala Lumpur

Namazie, Farah (1999) 1998: A Year of IT Legislation, IPAsia March 1999, p. 35

Phang, Andrew; Seng, Daniel (1999) The Singapore Electronic Transactions Act 1998 and the Proposed Article 2B of the Uniform Commercial Code, International Journal of Law and Information Technology, Vol 7 No 2, p 103

Ter, Kah Leng (1999) New Laws on E-Commerce: Singapore, Computer Law and Security Report Vol 15 No 1, p 8

Wu, Richard (2000) Electronic Transactions Ordinance - Bulding a Legal Framework for E-Commerce in Hong Kong, the Journal of Information Law and Technology (JILT) http://www.law.warwick.ac.uk/jilt/00-1/wu.html

Reed (ed) (1997) Computer Law, Blackstone Press, London

Seng, Daniel (1999) Legal Guide to the Electronic Transactions Act

Zainol, Z.A (1999) Electronic Data Interchange (EDI) and Formation of Contract: A Malaysian Perspective, International Journal of Law and Information Technology, Vol 7 No 3, p. 256

---

[1] Findings from Boston Consulting Group's NetBizAsia Strategy Report entitled *E-tail of the Tiger: Retail e-commerce in Asia Pacific* found that the total online revenue in Asia Pacific was US$2.8 billion in the last quarter of 1999, compared with US$3.47 billion in Europe and US$36.6 billion in the US. In 2000, the online retail revenue in Asia Pacific is expected to go beyond US$7 billion. In Malaysia however, the online retail revenue in 1999 was US$10 million.

[2] s. 3 of ETA states 6 objectives of the Act:

(a) to facilitate electronic communication 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 alterations 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 development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

[3] electronic record means 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.

[4] S. 13(1) ETA

[5] s. 13(2)(a) ETA

[6] s. 13(2)(b) ETA

[7] s. 13 (3)(a) ETA

[8] s. 13(4)(a) ETA

[9] s. 13(4)(b) ETA

[10] s. 13(4) (c) ETA

[11] s. 13(8) ETA

[12] s. 14(2)(a) ETA

[13] s. 14(2)(b) ETA

[14] s. 14(3) ETA

[15] s. 14(5) ETA

[16] s. 14(5) ETA

[17] s. 15(1) ETA

[18] s. 15(4) ETA

[19] s. 15 (2)(a) ETA

[20] s. 15(2)(a)(i) ETA

[21] s. 15(2)(b) ETA

[22] s. 62(1)DSA and s. 8(1) ETA

[23] s. 63 DSA and s. 22 ETA

[24] s. 62(2) DSA

[25] s.2 DSA

[26] s. 17 ETA

[27] s. 18 ETA

[28] s. 67 (c) DSA

[29] s. 4(2) ETA

[30] s. 63 (3) DSA

[31] s. 7 ETA

[32] s. 6 ETA

[33] s. 4(1) DSA

[34] s. 4(2) DSA

[35] s. 13(3)DSA

[36] s. 13(1) and 13(2) DSA

[37] s. 43 ETA

[38] s. 20(b)(iii) ETA

[39] s. 20(b)(iv) ETA