Asian Social Science; Vol. 8, No. 12; 2012
ISSN 1911-2017 E-ISSN 1911-2025
Published by Canadian Center of Science and Education

Malaysian DSA 1997: A Review of Some Unresolved Issues

Rokiah Kadir[1]

[1] Faculty of Management and Economics, Universiti Malaysia Terengganu, Kuala Terengganu, Malaysia

Correspondence: Rokiah Kadir, Faculty of Management and Economics, Universiti Malaysia Terengganu, 21030 Kuala Terengganu, Terengganu, Malaysia. E-mail: rokiah@umt.edu.my

Received: July 5, 2012 Accepted: July 23, 2012 Online Published: September 20, 2012

doi:10.5539/ass.v8n12p221 URL: http://dx.doi.org/10.5539/ass.v8n12p221

Abstract

It is widely recognized that electronic commerce can make fundamental changes to the national economic landscape. As with other countries, the prospect of electronic commerce has driven the government to amend existing legislation and enact new laws to deal with emerging legal issues arising from electronic commerce activities. Policy framework and regulations are laid out for the purpose of creating facilitative environment for electronic commerce. For this purpose Malaysia has enacted the Digital Signatures Act in 1997 (DSA) and almost a decade later, the Electronic Commerce Act 2006. This paper aspires to offer some analysis of the Acts in terms of how far they support a conducive legal environment they sought to promote and are sustainable for e commerce development.

Keywords: digital signature act, electronic commerce act, signatures, rate of adoption

1. Introduction

It is widely recognized that electronic commerce can make fundamental changes to the national economic landscape. One of the critical factors to the success of electronic commerce relate to trust and confidence of the contracting parties to the transactions executed via the medium. Sellers would be willing to ship the products and buyers would be prepared to transfer funds if they are confident that their transactions are secure. Electronic signatures can be used for verification purposes, and the increased use of electronic signatures has called for the need to legislate for a specific legal framework to reduce legal uncertainty arising from the use of the signatures. In Malaysia the Digital Signature Act 1997 was a response to the need. The Digital Signature Act 1997, as its name implies is solely focused on the issue of digital signature. Section 62(1) of the 1997 Act provides that "where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that rule shall be satisfied by a digital signature". The Act goes on prescribing the necessary characteristic of digital signatures, stating which must be fulfilled if the signature were to replace the paper signature. What is obvious from the provision is that other forms of electronic signatures such as biometric or simple or low technology electronic signatures[1] could in no way satisfy the legal requirement of signatures for documents prepared electronically.

One may pose a question whether the law should adopt a different approach when it comes to virtual environment. On the one hand, it may be perceived that a tougher standard might be justified because of the vulnerability of the virtual environment to fraud, on the other hand, it may be argued that recognition of other forms of electronic signatures should be warranted from the perspective of convenience and practicality of business usage. It may be thought that if contracting parties think that simple electronic signatures are quite adequate given the value of their business, they should be allowed to choose appropriate electronic signatures and the law should accommodate the need. Denial of recognition means that contracting parties will have no choice but to use only the secure electronic signatures. This would impose unnecessary cost on the contracting parties, high security in terms of the identification and the integrity of the document may well not be necessary to low-value transactions.

2. Policy Consideration

There are two policy choices in this regard. The most liberal policy choice is to treat all electronic signatures including the low technologies as acceptable signatures. The use of any electronic signature should present no difficulty to the signature requirement. This policy stems from two reasons; first, the form of signature is not important, indeed any loose form of paper signature should be quite adequate as an acceptable signature. Further

the demonstration of intention constitutes the primary function of signature and the placing of any type of electronic signature could indicate the signatory's intention to be bound by the document. The UNCITRAL Model Law on Electronic Signatures 2001 and the EU Directive on Electronic Signatures which recognize all types of electronic signature through the two tier approach, i.e. both the low and high technology electronic signatures, reflect this policy choice. At the first level of the two tier approach, the legislation accepts any type of electronic signature, and at a second level, it attributes greater legal effect to certain widely used techniques, i.e. the digital signature. The first tier reflects that the law is contented with the basic function of intention attestation.

The second approach confines the acceptability of electronic signatures only to the high technology electronic signatures such as digital and biometric signatures. The justification of this policy lies in the reliability of the high technology electronic signatures in terms of the content authentication or integrity function. In the context of the paper environment, this policy requires legal recognition only to be given to handwritten signature. This policy can be seen with the German Civil Code where signature is understood to be a handwritten original signature[2].

It may be observed that the first policy focuses on the intent of the parties, while the second policy, by contrast, emphasizes the security of the manner by which the signature is affixed. The second policy is based on a model that assumes signatures will primarily be used to prove personal identity. It is thought that the first policy choice is quite adequate for the general purpose of the signature requirement, and the second policy may only be needed in critical transactions. It may be thought that a law of general nature such as the Digital Signature Act 1997 or the Electronic Commerce Act 2006 should adopt the flexible policy by giving recognition to any signature. Emphasis on the security issue of signature, if any, should be achieved by means of a law of specific application, such as provided in the Land Registration Act 2002 of England, which requires the use of the advanced electronic signature e.g. the digital/biometric signatures for electronic conveyancing.

3. Why Simple Electronic Signatures Should Be Equally Accepted as Satisfying the Signature Requirement

There are two approaches to defining the form of the paper signature. A restrictive approach requires the signature to be done in the forms of one's full name, initial, surname or thumb print. According to this approach, only the scanned manuscript electronic signature, the typing of a name in electronic mail and biometric signatures would be compatible with the forms of the paper signature. The scanned manuscript signature and the typing of a name are equivalent to the name signature, and the biometric signature probably equates to the thumb print signature. A digital signature will be excluded as the signatory does not place a name or any distinctive physiological feature, but only apply a set of private keys. Equally, the clicking on an 'I accept' button in a web site and the giving of a unique sequence of characters would not satisfy the form of signature according to this restrictive approach. On the other hand, a pragmatic approach does not require the signature to exist in any particular form; a mark signature could well be sufficient according to this approach. The approach supports the acceptability of all types of electronic signature as good signature. It is thought that for many situations the pragmatic approach is quite adequate. The position is consistent with the fundamental function of signature-the demonstration of intention. Any form of signature should present no difficulty as the main purpose of placing a signature is to indicate an intention to be bound by the documents. The common law reflects the adoption of the pragmatic approach where the validity of signature does not hinge on any particular form[3].

In terms of functions, the main purpose of placing a paper signature is to indicate that the signatory agrees or is willing to be bound by the document (Reed, 2000)[4]. By placing a signature the signatory makes it clear that the signed document represents a completed declaration of will, and not just a draft which the signatory does not intend to be bound by. By signing a document, the signatory effectively demonstrates his intention to adopt its content. In this way the signature serves as a mechanism to prevent against repudiation, where the placing of the signature prevents the signatory later denying the signature and its necessary effect. This primary function of signature has been confirmed by the UNCITRAL Model Law on Electronic Commerce 1996 which stated that the signature attests "the intention of a party to be bound by the content of a signed contract, the intention of a person to endorse authorship of a text, or the intention of a person to associate itself with the content of a document written by someone else"[5].

The function is readily satisfied by all types of electronic signature; by typing a name, or clicking on a button, or writing a unique sequence of characters, or using secure electronic signatures, a signatory demonstrates his intention to adopt the content of the document. Indeed there should not be any doubt as to the capability of any electronic signature to satisfy this primary function of signature. The typing of a name etc are the means to

express the intent to be bound by the document when using the electronic communication. In the light of this, it is thought that the most appropriate policy is provided by the first policy choice supporting the use of all types of electronic signature in contracts with the signature requirement.

The second function relates to the identification of the signatory, which has been recognised by the Model Law as one of the function of the paper signature. Thus the signature is designed to "identify a person, to provide certainty as to the personal involvement of that person in the act of signing and to associate that person with the content of a document"[6].

The identification function is loosely met by the low-technology electronic signatures; the signatures may identify the signatory but their use is highly susceptible to forgeries. The high technology signatures, to a greater extent support the identification function through the registration process and the verification procedure. Despite the possible failings of the low technology electronic signatures in satisfying the identification function, those electronic signatures should be capable to satisfy the signature requirement. It must be remembered that the paper signature is equally not foolproof. A handwritten signature may not identify the signatory convincingly as the name alone may not provide sufficient proof of identity; it would be almost impossible for a relying party to prove the identity of the signatory only by looking at the signature, since a name or surname may be used by more than one person. A name signature could acquire a high level of certainty if it is verifiable through additional documents such as the driving licence, bank statements, utility bills, the passport or equivalent documents (Brazell, 2004). A name signature may have greater ability as identifier in countries which have systems for registration of identities. In Malaysia, for example, with the requirement for citizens above the age of twelve years to have identification cards, it is quite possible to verify an identity by cross checking with the National Registration Department, although it does not prevent manipulation. Secondly, the vulnerability of paper signature to forgery may also arise out of the possibility and ease of making change to the style of handwriting. A relying party who sees the signature for the first time would be unable to tell whether or not the signature belongs to the signatory, unless there is verification from a third party.

This next function relates to the protection of the integrity of the data where the application of a signature supposedly prevents the tampering of the contents of the document. Similar to the identification function, the high technology electronic signatures to a large extent meet this function through the hash function in digital signature and the biometric features in biometric signatures. On the other hand, the low technology electronic signatures are less reliable and, hence, they are susceptible to fraud, virus attack etc. It is thought that the vulnerability of the low technology electronic signatures should not affect its acceptability as a good signature. The risk is also present with the paper signature; the content authentication function could only be achieved by signing each page of the document and initialling the parts which are cancelled or modified, as well as by distributing each copy of the signed document to each party, so that any change can be traced by comparing to the original copy. Putting the signed document in safe-keeping with banks would also guarantee the authenticity of the document (Brazell, 2004). Unless these measures are taken, the paper signature does not effectively accomplish this content authentication function.

4. The Digital Signature Act 1997

The Act was designed to address the emerging issues of electronic signatures. It was conceivable that the potential of fraud is considerable, due to the ease of intercepting and altering information sent via electronic medium. Digital signature was the secure electronic signatures prevalent at the time and the Act was meant to regulate the use of this technology. The Act is not satisfactory for two reasons; first the 1997 specifies only one technology and does not leave room for future technologies. Thus the sole recognition of the digital signatures in the 1997 Act rejects biometric signatures, regardless of its high technology features, as good signature. As a result it is possible that biometric signatures might not be adopted by electronic commerce in Malaysia for fear of their unclear status. By laying down features of secure electronic signatures, the acceptability of secure electronic signatures is no longer confined to certain specific technology of digital signature.

Second, the 1997 Act would also impact on the acceptability of simple electronic signatures as well. It may be thought that while the focus is on the issues of digital signature, given the predominant role played by public key cryptography in electronic authentication, the law should not discourage the use of other authentication techniques. The law should accommodate various levels of security which may suit different types and value of commercial transactions. By giving sole recognition to digital signature technology, the approach taken by the 1997 Act did not sufficiently reflect the business need for flexibility in the use of authentication techniques[7].

5. The Electronic Commerce Act 2006

The Act is commendable in terms of its inclusion of electronic signatures. The definition provision in section 5 which is quite sufficient to embrace all types of electronic signatures as a signature is a bold step taken by the authority despite that the UNCITRAL Model Law on Electronic Commerce 1996 on which the legislation was based contains no such provision. Section 5 defines electronic signature as "any letter, character, number, sound or any other symbol or any combination thereof created in an electronic form adopted by a person as a signature". It is easy to see that with the inclusion of this definition the Act seeks to improve the shortcoming in the Digital Signature Act 1997, the result being that all simple electronic signatures can clearly be captured within the definition. Section 5 conforms to the Interpretation Acts 1948 and 1967 which is content with the demonstration of intention as the main function a signature should achieve.

Section 9 addresses electronic signatures which are capable of fulfilling identification and content authentication functions. Section 9 also reflects a laudable move to extend recognition beyond the specific technology of electronic signatures such as digital signatures. Emphasis on functions of signature as criteria of acceptance allows the use of reliable electronic signatures such as biometric signatures. Section 9 states that "(1) where any law requires a signature of a person on a document, the requirement of the law is fulfilled, if the document is in the form of an electronic message, by an electronic signature which—*(a)* is attached to or is logically associated with the electronic message; *(b)* adequately identifies the person and adequately indicates the person's approval of the information to which the signature relates; and *(c)* is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required. Clause (2) provides that for the purposes of paragraph (1)*(c),* an electronic signature is as reliable as is appropriate if—*(a)* the means of creating the electronic signature is linked to and under the control of that person only; *(b)* any alteration made to the electronic signature after the time of signing is detectable; and *(c)* any alteration made to that document after the time of signing is detectable"[8].

The introduction of sections 5 and 9 and hence recognition of electronic signatures other than digital signatures is thought to be a creditable move from economics consideration as well. Market survey indicates that rate of adoption is generally low for digital signatures. In India for example, the rate of adoption of digital signatures is relatively at a low level[9]. In Europe, a study found that even after seven years of the implementation of electronic signature law the rate of adoption is quite disappointingly low (Roßnagel, 2006). The phenomenon could be attributed to the lack of awareness of the security concept of communication through the Internet. Adoption rate is greatly influenced by factors such as knowledge and awareness of consumers and their willingness to pay for digital services. It is a very important factor to the widespread use of digital signatures that users or customers must be convinced of the benefits of the use of this technology[10].

Thus it is high time that recognition is accorded to all types of electronic signatures. Nevertheless the introduction of sections 5 and 9 under the Electronic Commerce Act 2006 only partially resolves the problem of the prescriptive approach brought about by the Digital Signature Act 1997. The issue would have been better tackled by making amendment in the 1997 Act as well if biometric signatures were to be equally regulated. Without the amendment, secure electronic signatures other than the digital signatures might not receive equal treatment, for example it may be deprived of the liability provision in the 1997 Act. Thus if electronic data containing biometric features is used in an unauthorized manner with no fault of the subscriber, the relying party might not be able to invoke the liability provision since it is not provided in the 2006 Act.

6. Concluding Remarks

Malaysia was among the earliest countries which respond to the need to regulate digital signature. Albeit the effort is commendable it is far from satisfactory. Focusing on high technology electronic signature alone and denying recognition to other forms of electronic signature is not thought to be an appropriate policy. In contracts of high monetary value, parties contracting via the internet may prefer to use more secure electronic signature due to the inherent risk in internet communication, where a relying party who is wary of the security issue may want to be assured that the signatory is who he says he is. With the high financial interest at stake, identification through electronic mail or a web page order form may not provide sufficient evidence that it was a certain party who had entered into the transaction. However, it must be remembered that the needs of contracting parties may vary and in some circumstances they may well be content to use simple electronic signatures. These differing needs can be better accommodated if the DSA has adopted a facilitative approach towards various types of electronic signatures.

References

Akdeniz, Y., Walker, C., & Wall, D. (2000). *The Internet, Law and Society*. Longman, Harlow.

Blythe, S. (2005). Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security. *Richmond Journal of Law & Technology.*

Brazell, L. (2004). *Electronic Signatures Law and Regulation*. Sweet & Maxwell, London.

Lloyd, I. J. (1997). Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures. In Edwards, Lilian, & Waelde, Charlotte (Eds.), *Law & the Internet: Regulating Cyberspace*. Hart, Oxford.

Mason, S. (2003). *Electronic Signatures in Law*. LexisNexis, London.

New Zealand Law Commission, Electronic Commerce, Part I. (1998). *A Guide for the Legal and Business Community, para 314.* Retrieved from http://www.lawcom.govt.nz

Reed, C. (2000). What is a Signature. *The Journal of Information, Law and Technology*.

Roßnagel, H. (2006). On diffusion and confusion–Why electronic signatures have failed- Trust and Privacy in Digital Business. Proceedings of the 3rd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus 06), Springer LNCS 4083, pp. 71-80. Krakow, Poland.

Schellekens, M. H. M. (2004). *Electronic Signatures Authentication Technology from a Legal Perspective.* Asser Press, The Hague.

Spencer, J. R. (1973). Signature, Consent, and the Rule in L'estrange v. Graucob. *Cambridge Law Journal, 105*.

Spyrelli, C. (2002). *Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach towards Electronic Authentication.* Retrieved from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/

Treitel, G. H. (2003). *The Law of Contract* (11th ed.). Sweet and Maxwell, London.

Appendix

[1] The low technology electronic signatures include the typing of a name, the clicking on an 'I accept' button, the giving of a unique sequence of characters, and a scanned manuscript signature.

[2] Section 126(1) provides that "if writing is prescribed by law the document must be signed by the maker in his own hand by signature of his name, or by his mark notarially authenticated".

[3] See the judgement of Evershed MR in *Goodman v. J Eban* [1954] 1 All ER 763 who stated: "a signature is not confined to actual writing with a pen or pencil, but appears to have related to marking with the sign of the cross. The later meanings include: 'to place some distinguishing mark upon (a thing or person)… [and] to attest or confirm by adding one's signature; to affix one's name to (a document, etc)".

[4] See also the New Zealand Law Commission, Electronic Commerce, Part I, "A Guide for the Legal and Business Community" (1998), para 314. Retrieved from http://www.lawcom.govt.nz

[5] Guide to Enactment 1996, paragraph 53.

[6] See Guide to UNCITRAL Model Law on Electronic Signatures, 2011.

[7] See also the definition of the advanced electronic signature under the Electronic Signatures Regulation of UK. Section 2 defines advanced electronic signature as "an electronic signature-

(a) Which is uniquely linked to the signatory,

(b) Which is capable of identifying the signatory,

(c) Which is created using means that the signatory can maintain under his sole control, and

(d) Which is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable".

[8] It's early days for digital signatures in India. Retrieved from http://www.expresscomputeronline.com

[9] In Malaysia, the use of digital signatures in the early stages is quite low. In 2002 around 42,000 certificates

were issued and this number has increased to 2.03 million in 2008. Total income earned from the sale of digital certificates in 1999 was about RM0.01 million and a decade later the amount has increased to RM23.7 million. Government has played a significant role in the increased rate of use of digital signatures through the implementation of Mykad identity card, driver's license, tax payment, electronic procurement etc. No doubt the adoption rate would have remained low without the government's contribution and policy in this regard. Adoption rate of digital signatures in Japan, Korea, Taiwan and Singapore is higher. See Industry Performance Report by Malaysian Communications and Multimedia Commission http://www.skmm.gov.my