Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 3 (2011) 248–253

Procedia Computer Science

www.elsevier.com/locate/procedia

WCIT 2010

The application of the digital signature law in securing internet banking: some preliminary evidence from Malaysia

Hartini Saripan[a] , Zaiton Hamin[b,c,] *

[a]*Ph.D researcher/Lecturer, Faculty of Law, Universiti Teknologi MARA,40450 Shah Alam, Selangor, Malaysia*
[b] *Assoc. Prof. Dr.*
[c] *Director, Cyberlaw and Policy Centre, Faculty of Law, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia*

Abstract

Malaysia is one of the first countries in the world to blaze the trail for having a prescriptive legislation of governing the digital signature technology. Whilst the Digital Signature Act 1997 has always been acknowledged as one of the pioneers of a technology-specific legislative approach, the Act nevertheless, has been greatly exposed to numerous critiques, suggesting its inability to secure online transactions, including Internet banking. Moreover, the lack of any of its provisions being tested in the Malaysian courts has in turn, suggested that the law has an inconsequential application in securing Internet banking transactions. Drawn from an ongoing doctoral research, this paper will highlight a methodological process and a preliminary finding of eight multiple-case studies amongst banks offering Internet banking services in Malaysia. The research, at the onset revealed that in 'the real life situation', the digital signature technology is hardly being adopted in securing Internet banking transactions, which has consequently shaped the extent of the application of the digital signature law in Malaysia.

Keywords: Digital signature; Internet banking security; Prescriptive model

1. Introduction

The Malaysian Digital Signature Act 1997 (hereinafter 'the 1997 Act') was enacted more than ten years ago, only to see that none of its provisions has ever been contested in courts until today. Specifically designed to legally govern an online authentication using the digital signature technology, the law is suggested to be less applicable, which brings about the need of having this research. Despite of numerous setbacks of the 1997 Act, the law needs to be examined and the extent of its application requires serious attention in enhancing the implementation of this technology and its law in Malaysia, above all, within the Internet banking environment. This paper therefore, sets down some preliminary evidence on the issue of the application of the digital signature law in Malaysia. Adopting a prescriptive approach of the digital signature legislation, the implementation of the law has been substantially shaped by the deployment of this specific authentication technology in the context of Internet banking. In deliberating this issue, the paper commences with a general overview of the digital signature technology, capturing some technological backgrounds, which are essentially significant in understanding its law. A legal discourse on the Digital Signature Act 1997 is subsequently enlightened, presenting some critiques of the 1997 Act, which impliedly advocate the inability of the current law to secure Internet banking transactions. A summary of the methodology used in conducting the case-study is explained in the next section, whereas the preliminary result on the issue of the application of the 1997 Act is concisely described before the paper is finally concluded.

* Hartini Saripan. Tel.: +603-55211054; fax: +603-55444121.
E-mail address: hartinisaripan@gmail.com

1877-0509 © 2010 Published by Elsevier Ltd.
doi:10.1016/j.procs.2010.12.042

2. An Overview of the Digital Signature Technology

The inescapable presence of various Internet banking risks have urgently requires some solutions to address the problems. The emergence of electronic signatures (e-signature) therefore, is undeniably seen as one of the answers to this dilemma and digital signatures are no exception. Whilst Lincoln [1] views that this authentication tool is considered as one of the most secure e-signature technologies in the market, Smedinghoff and Bro [2] for example, describe "digital signature" as one technology-specific type of an e-signature. This is one of the most secure methods, which is created through the use of the public and private encryption process (Lincoln [1]) or known as the public key infrastructure (hereinafter 'the PKI'). In this regard, Mason [3] illustrates that the signing party employs a key pair, wherein the sender affixes the signature using their private key and the recipient checks the signature with the public key. Winn [4] has therefore, explains that a digital signature is part of a message that indicates the correct source and signifies that such message has not been altered in transit. This encrypted data, according to Freeman [5], uniquely identifies the sender and establishes the integrity of the document as only a party with the proper software can decode the signature. Koger [6] therefore, argues that the recipient of the document with a digital signature can eventually authenticate the data source as well as verifying its origin and data integrity to ensure that the document has not been altered and intercepted.

Apart from that, the PKI requires the use of a trusted third party, namely a certification authority (hereinafter 'the CA') in order to verify that a particular person owns a specific key (Berman [7]). In this regard, Mason [8] describes that the CA is a trusted third party who checks and verifies the identity of the person requesting the key pair. Whilst the private key is secret and is only distributed to the owner, he also explains that the public key can be obtained by looking at the CA's public database (Mason [8]). In this respect, the PKI requires the CA to play an important role in establishing a confidential and reliable environment for digital signatures to exist. As a result, Berman [7] opines that strangers (people entering into a relationship without pre-existing contractual business relationships and without pre-existing mutual trust) can enter into transactions with other strangers in the PKI because each party can rely on the CA to verify identities and signatures.

3. The Digital Signature Law in Malaysia

The Digital Signature Act 1997[b] and its Regulations 1998 were created to facilitate e-commerce activities as well as enabling businesses and the community generally to use digital signatures instead of conventional hand-written signatures in legal and commercial transactions, which include Internet banking businesses. This legislative framework clearly demonstrates the government's commitment to gear Malaysia into becoming a trusted international e-commerce hub by legalising the use of digital signatures. The 1997 Act is modelled after the Utah Digital Signature Act 1995, which Winn and Wright [9] explain that the latter Act was already repealed in 2006.[c] A technology-specific approach is clearly enshrined in the 1997 Act, in which, Caesar [10] argues that the Act has mandated the PKI or private key-public key technology to electronically authenticate electronic transactions. This prescriptive feature of this legislation, according to Brazell [11], has been clearly described by the provisions of the Act, which Saripan [12] later argues that the Act provides for a specific technological tool that is recognized by the law. The 1997 Act is enacted with 92 provisions, which are divided into 7 parts. "Digital signature" is defined in section 2 of the 1997 Act 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, whether the transformation was created using the private key that corresponds to the signer's public key; and whether the message has been altered since the transformation was made. This provision clearly shows that the Act only recognizes a digital signature technology as a legally valid electronic signature. Furthermore, Mason [13] contends that this legislation has also opted for a compulsory licensing regime, as enshrined in Part II of the 1997 Act.

Despite the fact that Malaysia is among the first to have a technology-specific legislation, some writers including Zaba [14] view that this development is rather anxious as well as intended to show their eagerness to response to the

---

[b] The Digital Signature Act 1997 was later amended in 2001.

[c] The Utah Digital Signature Act was repealed in 2006 by virtue of S.B. 20. signed by the Utah's Governor.

growth of technology. A considerable amount of literature has been published, suggesting the inability of the law to secure online transactions, particularly in the Internet banking environment. These studies have shown numerous criticisms on the shortcomings of the 1997 Act. In this regard, there has been a consensus in the literature for the past ten years that this Act is significantly defective. Ong [15] for instance, considers the Act as incomplete and has failed to recognise the fast changing pace of modern technologies. The first series of discussions have taken place in the 1990s when Chong [16] describes the work of the 1997 Act as deficient in which, there are still many areas to be addressed in ensuring that electronic commerce is truly borderless. Whilst Munir [17] identifies the failure of the Act to address several technical issues as the main flaw, Ong [15] also suggests that the 1997 Act should have been drafted to provide a scope to accommodate the evolving demands and vicissitudes of new technology. These literature are evidence of the fact that despite the remarkable job of the 1997 Act to set out the legal framework of digital signature, this Act remains as an incomplete piece of legislation, which urgently requires a critical re-examination of the current law in ensuring the security of e-commerce, including Internet banking transactions.

Also, Munir [17] argues that the setbacks of the Act are essentially based on the fact that the current digital signature law has faced at least seven deficiencies and downsides. Adopting the Utah Digital Signature law, Munir [17] critically observes that the local law has failed to 'see the forest for the trees' as the former law should be closely examined before it is accepted by other countries, including Malaysia as the 'model' legislation. The main critiques, which are rooted in some highlights, including the disadvantages of having technology-specific legislation as opposed to technology-neutral and issues relating to the certification authorities such as their qualifications, rights and liabilities have indeed called for a thorough reappraisal of the law and confirmed the need for this legislative work to be reviewed (Ding [18]). The deficiencies of the Act are consistently agreed by the literature until today. Recent discussions have led to the same conclusion that the 1997 Act is imperfect. The argument from Jalil and Pointon [19] maintains that the Act has omitted a number of provisions on several crucial areas to commercial transactions, which makes it incomplete and ambiguous. On the same thought, Tay and Goh [20] argue that the weaknesses on selected aspects of the Act have been underlined, which undoubtedly lead to the amendment of the Act in order to improve the effectiveness of the recognised digital signature in protecting and solving the security issues on e-commerce.

4. Methodology: A case-study

This is a qualitative research, which draws upon both the primary and the secondary data. The qualitative research is preferred in investigating the impact of the adoption of the digital signature technology on the application of its law in Internet banking as such method, according to Miles and Huberman [21], requires a comprehensive, systematic and integrated overview of the issue concerned within the context under study. As such, the integration of various strategies could be seen in both the primary and the secondary data drew on this doctoral study. Whilst the primary data is totally based on the empirical study, the secondary data is mainly referred to documents obtained during the fieldwork, field notes, relevant statutes including the Digital Signature Act 1997 and its Regulations 1998, hansards of such statutes, articles, books, journals and cases. The investigation of the adoption of the digital signature technology and its impact on the law in the field took place when eight cases (units of analysis) were studied from May 2009 to August 2009, which was represented by the main categories of commercial banks and the most relevant regulators of both the law and the financiers.

Hence, out of eight units of analysis, six of them are the banks offering the Internet banking facility, ranging from the local banks, the Islamic banks and the International banks, whereas two of them are the relevant regulators. Apart from that, there are four departments in every bank involved in the interview i.e. the consumer Internet banking department, the corporate Internet banking department, the legal department and the IT security department. For the regulators, there are six departments involved in this research, which totalled up to twenty-eight respondents from both the banking industry and the regulators. For data collection process, semi-structured interviews were used as an instrument as Saunders et al. [22] believe that this tool is considerably useful in gathering valid and reliable information that are relevant in answering the research questions and achieving the research objectives. All interviews, except for two phone interviews and one email interview, were conducted face-to-face. These data were voice recorded, properly stored and transcribed before coding and indexing them into several nodes and codes. Audio recordings of all twenty-eight respondents, therefore, need to be fully transcribed, corrected and edited as part of data management process.

The primary data collected from eight case-studies were then, coded and categorized into several nodes. With the increase of a Computer Assisted Qualitative Data Analysis (CAQDAS), the NVIVO7 was used for a coding process, following the rise of contemporary qualitative data analysis. As highlighted by Coffey and Atkinson [23], the use of this software has resulted in a speedy and comprehensive search of data files with the ability to cope with multiple and overlapping codes as well as multiple searches using more than one code word simultaneously. The use of the operators AND, OR and NOT to combine code words was very useful in conducting complex retrieval of data, particularly when large numbers of codings were involved. In addition, with the help of the NVIVO7, the nodes were grouped in a hierarchical system or a tree structure, providing a means of organizing codes into 'parent' nodes or main nodes and 'children' nodes or subcategories of the main nodes. Once the data were coded or indexed, such data were displayed to facilitate a within-case and across- case analysis described by Yin [24]. Hence, conclusions were then drawn based on a within-case display as well as a multiple-case display, adopting either a simple counting tactic, noting patterns of the issues or making contrast and comparisons between the cases as enunciated by Miles and Huberman [21].

5. Preliminary result

The investigation of the issue on the application of the digital signature law revealed that the implementation of the law depends very much on the adoption of the technology. Whilst the law features a prescriptive legislative model in governing the use of the digital signature technology, the deployment of this asymmetric cryptosystem thus, shaped the application of the 1997 Act by the banks offering the Internet banking facilities in Malaysia. The evidence interestingly, showed that this authentication technology is being extensively applied in the corporate Internet banking rather than the consumer Internet banking. The research subsequently found that the use of other electronic signatures to authenticate online banking transactions at the consumer end has, to certain extent, resulted in the marginal application of the 1997 Act in the banking industry.

The use of the other authentication technologies in securing retail Internet banking transactions, which include a Transaction Authentication Code (TAC) and a Vasco Token, has been significantly based on the business, economic, infrastructure as well as legal rationalities. The notion of security versus cost versus convenience is illustrated as the most imperative concept to be taken into account before adopting any authentication technology. In this respect, the digital signature technology, on the other hand, is viewed by the respondents to be costly and inflexible, which eventually failed to reach the public at large. The corporate controlled environment, on the contrary, which merely involved several trusted people in a corporation such as checkers and approvers to authorize a transaction, justified the adoption of the digital signature technology in their Internet banking businesses. Being one of the high-end security mechanisms, this public key technology is ultimately chosen by some banks in gaining confidence by their corporate clients as well as conforming to the provisions provided by the 1997 Act.

In addition, the research also found that the inconsequential application of the digital signature law in Malaysia is due to various legal-related reasons. The role of the digital signature legislation to protect both banks and consumers is considerably doubted or rather not known to most of the respondents. This evidence therefore, essentially suggested that the minimal application of this law is partly contributed by the absence of legal knowledge on the 1997 Act. The respondents also questioned the ability of legal experts of either the internal legal personnel in the banks or the practitioners and judges in understanding this technology-specific law. The deskilling of these experts who were expectedly to be proficient in understanding the Act has in turn, decreased the confidence of the bankers to be governed by this piece of legislation. The fact that this law has never been tested before any of the Malaysian courts is, as a matter of fact, one of the key reasons for the banks to choose other authentication technologies, which are definitely cheaper and much more user-friendly to be applied by online consumers.

6. Conclusion

The preliminary evidence of the case-study has generally shown that the application of the digital signature law in Internet banking (or the lack of it) is beyond doubt, shaped by the adoption of this authentication technology by the bank. In this respect, the prescriptive approach adopted by the legislation only allows the law to come into play when the technology is strictly implemented in accordance of the law. As a result, the insignificant use of the

technology by the banks offering Internet banking facilities led to the trivial application of its law. The result clearly evident that the infeasibility of this technology due to its technological and legal weaknesses could be some reasons that were taken into consideration by the consumer Internet banking in preferring other technologies, which are more cost-effective. This business mentality has in due course, undermined the ability of the digital signature law to secure online transactions, primarily, in the context of Internet banking.

Acknowledgements

We would like to thank the management of our institution, Universiti Teknologi MARA for their relentless support in enabling us to present this paper. Also, we are heartily thankful to our financier, the Ministry of Higher Education Malaysia for providing us with the financial assistance, without whom, this presentation would not have been possible.

References

[1] A. Lincoln, "Electronic Signature Laws and the Need for Uniformity in the Global Market", *8 J. Small & Emerging Bus. L. 67,* 2004.
[2] T. J. Smedinghoff and R. H. Bro, "Moving With Change: Electronic Signature Legislation As A Vehicle For Advancing E-Commerce",
17 J. Marshall J. Computer & Info. L. 723, 1999.
[3] S. Mason, *Electronic Evidence: Disclosure, Discovery & Admissibility*, First Edition, LexisNexis Butterworths; London, 2007.
[4] J. K. Winn, "The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce", *37 Idaho L. Rev. 353,*
2001.
[5] E. Freeman, "Digital Signatures and Electronic Contracts", *EDPACS: The EDP Audit, Control & Security Newsletter, Vol. 32, Issues 3,*
pp. 18-24, 2004.
[6] J. L. Koger, "You Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace as Primary Legislator of
Electronic Signatures",*11 Transnat'l L. & Contemp. Probs. 491,* 2001.
[7] A. Berman, "Note: International Divergence: The "Keys" to Signing on the Digital Line - The Cross Border Recognition of Electronic
Contracts and Digital Signatures", *28 Syracuse J. Int'l L. & Com. 125*, 2001.
[8] S. Mason, "Digital Signatures: Is that really you?" *IEE Engineering Management,* 2005, p. 12.
[9] J.K. Winn and B. Wright, *Law of Electronic Commerce,* 4th Edition, Aspen Publisher: New York, 2008-2 Supplement.
[10] L. Caesar, "Malaysia's Legal Framework for Promoting Technology", 2001, available at www.asiasociety.org.
[11] L. Brazell, *Electronic Signatures and Identities: Law and Regulation*, 2nd Edition, Sweet & Maxwell; London, 2008.
[12] H. Saripan, "Electronic Signature Legislative Models: The Reappraisal of the "Unfortunate" Divergence" [2009] *3 MLJ xx*.
[13] S. Mason, *Electronic Signature in Law*, 2nd edition, Tottel Publishing; West Sussex, 2007.
[14] S. Zaba, "Digital Signature Legislation: The First 10 Years", *Information Security Technical Report II*, 2006, pp. 18-25.
[15] R. Ong, "Consumer Based Electronic Commerce: A Comparative Analysis of the Position in Malaysia and Hong Kong", *International*
Journal of Law and IT, 2004.
[16] J. Chong, "A Primer On Digital Signatures And Malaysia's Digital Signatures Act 1997", *14 Computer Law & Security Report,* pp 322-
333, 1998.
[17] A. B. Munir, *Cyber Law: Policies and Challenges,* Butterworths Asia:Singapore, 1999.

[18] J. Ding, *E-Commerce Law & Practice*, Sweet & Maxwell Asia: Selangor, 1999.
[19] M. A. Jalil and L. D. Pointon, "Developments in Electronic Contract Laws: A Malaysian Perspective", *Computer Law & Security Report,* vol. 20, 2004.
[20] T. E. Siang and G. C. Yih, "Legal Issues and Technical Aspects on mechanism of Digital Signature in Malaysia" Paper presented at the International Conference of E-Commerce 2006, Gurney Resort Hotel and Residence Penang, Universiti Utara Malaysia and MDMC (Multimedia development corporation) ,19-20September 2006.
[21] M. B. Miles and A. M. Huberman, *Qualitative Data Analysis: An Expanded Sourcebook*, Sage Publications: Thousands Oaks, 1994.
[22] M. Saunders et al., *Research Methods For Business Students,* Pearson Education Limited: Essex, 2000.
[23] A. Coffey and P. Atkinson, *Making Sense of Qualitative Data: Complimentary Research Strategies*, Sage Publications: Thousand Oaks, 1996.
[24] R. Yin, *Case Study Research: Design and Methods*, Sage Publications: Thousand Oaks, 1994.