Singapore Journal of International & Comparative Law
(2003) 7 pp 183–200

Digital Signatures, Certification Authorities: Certainty in the Allocation of Liability

Yee Fen Lim[*]

I. Introduction

Electronic signatures are a vital ingredient in the success of electronic commerce. Without them, it is questionable whether commerce can be effectively carried out on the Internet. While they have many uses in non-commercial transactions, it is their utility in the commerce arena that has brought them the international attention they currently have. In many respects, they also have a close relationship with encryption technology. Electronic signatures are simply an electronic confirmation of authenticity. This definition is deliberately broad enough to encompass all forms of electronic identification, from the very informal (and insecure), such as initials at the end of an email, to the very formal (and highly secure), such as iris scans. Digital signatures are a particular subset of electronic signatures. This paper will focus on digital signatures and argue that certainty with respect to the liability of certification authorities is crucial and holds the key to the success of digital signature take up.

II. The Legal Challenges of Electronic Signatures

A. *Definition and Recognition*

The key to a coordinated legal response to the challenges of signatures lies in a workable, acceptable and practical definition that will be recognised in all courts of law. Currently, no definition of electronic signatures has been internationally agreed upon. Definitions range in rigour from the very loose to the very strict. This issue is patently of international significance because without common, or

[*] BSc, LLB, LLM (Hons), Senior Lecturer, Department of Law, Macquarie University, Sydney, Australia.

similar, definitional frameworks, there can be little progress in developing the legal institutions necessary for the conduct of international electronic commerce.

The first step is to examine what it is about standard, paper-based signatures that make them legal. The Statute of Frauds makes writing a requirement of signature recognition but defines this requirement very broadly. This is aptly summed up in the 1869 case of *Howley v. Whipple*:[1]

> It makes no difference whether that operator writes the offer or the acceptance . . . with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by use of the finger resting upon the pen; nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office.

This requirement encapsulates an awareness of the terms above the signature, agreement to be bound by those same terms, knowledge of consequence of breach, awareness that the signature is non-repudiable as a sign of intent, and providing an unalterable permanent record of event.

The question 'What is a digital signature?' is not answered by merely pointing to the electronic equivalent of writing, nor is there a uniform answer to this question. In many jurisdictions, in the paper world, almost anything can qualify as a signature. However, in the electronic realm, a definition is not so simple.

B. *Function of Signatures*

One correlative of recognition is the requirement that, once a signature is recognised in a court of law, the person to whom that signature is attributed cannot deny the authenticity of the document to which it is attached. This idea is central to the way many people do business and demonstrates the need for trust within all transactions. It is expected that a contractor will be legally bound by a signed agreement, even if she later changes her mind. If a signature cannot be proven to be technically authentic—that is, if it cannot be proven to be the sender's electronic signature—the legal questions become moot. However, in the case of repudiation of a *prima facie* valid signature, the legal question is at the forefront of concern.

[1] 48 NH. 487 (1869).

Electronic signatures must serve the same essential functions as handwritten signatures, namely (i) authentication; (ii) integrity; and (iii) non-repudiation.[2] Authentication means ensuring that a party to a transaction or communication is who she purports to be. It is concerned with the source or origin of the communication. Integrity means ensuring that a communication has not been altered in the course of transmission. It is concerned with the accuracy and completeness of the communication. The recipient of an electronic communication must be confident of a communication's integrity before she can rely on and act on the communication. Integrity is critical to e-commerce transactions, especially where contracts are formed electronically. And finally, non-repudiation means ensuring that a party cannot later go back on the transaction should a dispute arise.[3]

The elements of authentication, integrity and non-repudiation are all elements that indicate the presence of trust. In the real world, there are numerous indicators of trust that one can rely on. The witnessing of signatures, paper with watermarks, letterheads, and handwritten ink signatures are all tools which can be employed to ensure the signature and content are genuine, authentic and reliable. In the electronic realm, none of these indicators of trust can be utilised. One can type one's initials at the end of an email, but it would be quite unreliable as an indicator of source. As a result, one form of electronic signatures, digital signatures using cryptography, has been developed to meet the requirements of authenticity, integrity and non-repudiation.

III. Digital Signatures[4]

A digital signature uses encryption, specifically public key encryption, and a one-way-hash function to guarantee authenticity. There are two basic types of cryptographic system. Symmetric key ciphers, where both sides use the same key, were the earliest forms of encryption technique. The Data Encryption Standard (DES) and the Improved Data Encryption Algorithm (IDEA) are two of the more widely used symmetric key ciphers. In fact, DES has been used in the banking and finance sectors for decades. More recently, the Advanced Encryption Standard (AES) has been developed to meet the needs of the new millennium and the United States government has adopted Rijndael

[2] See Thomas J. Smedinghoff & Ruth Hill Bro, "Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce" (1999) 17 *John Marshall J. of Comp. & Info. Tech. Law* 723.

[3] Id., at 745–6.

[4] See further Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (OUP 2002), Chap. 6 on Electronic Signatures.

as the AES algorithm.[5] The method is simple. Write a message, encode it with a key, and send it to someone who holds the same key. The recipient then simply decodes the message. The key can be as long or short as required. The longer the key, the more secure the message. The difficulty with symmetric key cryptography, however, relates to the security of the key. The system requires two identical keys and can therefore only be as secure as the method of transporting and keeping the keys. If a key is lost, stolen, or otherwise revealed, the system is compromised. One solution to the problem of key management and transportation lies in the second main type of system, public key cryptography.

Public key cryptography uses two different, but mathematically related, keys, known as a 'key pair'. One key is used to encode, the other to decode. One of these keys is called the public key, the other is the private key, both of which can encode and decode. The public key is a unique, individual key but it is designed to be freely distributed to anyone who requires it. The associated private key is kept secret by the individual. When a third party wants to send a message to our private key holder, they encode it using the freely available public key. Once it is encoded with a particular public key, only the associated private key can decode the message. Therefore, the message can be sent through standard channels by anyone who has the public key, but can only be read by the intended recipient, the holder of the private key. Alternatively, a person can encode a message using a private key. This can then only be decoded using the associated public key. But the public key is freely available. Consequently, this system does not prevent the content of the mail being viewed; instead, using the system in this fashion acts as a guarantee of authenticity—a signature, if you will.

One-way-hash functions are a feature of cryptography which have a particular use in digital signatures. A one-way-hash function is an algorithm which, unlike a key, has no relation to any other algorithm and which is freely available. When the hash function is applied to simple text (a process called the 'crunch'), a number, known as a hash, is produced. The number is of a determined bit length depending on the size of the function—for example a 128-bit hash—and the longer the hash, the more secure the algorithm. The algorithm cannot be reversed, unlike key cryptography. Therefore, if a person is presented only with a 128-bit hash it is effectively useless; there is no way of knowing what the simple text is.

[5] See the NIST home page at http://www.nist.gov/aes/, accessed 5 June 2002, for up-to-date information.

A one-way-hash function alone makes a perverse tool of encryption because it is impossible to reproduce the original simple text once a hash is created. Fortunately, this is not its purpose. A hash is usually included at the end of the simple text message that was the basis for its creation. Therefore, the recipient can verify a message by using the same simple text and the same one-way-hash function. If the new hash matches the hash in the message, it is guaranteed that the simple text sent with the hash has not been altered.

With this background, a user using two methods can create a unique, verifiable mark of authenticity. Using public key encryption, a signature is produced through a series of steps.[6]

(1) The sender writes a message.
(2) The sender then uses her own private key to encrypt the message.

If the intended recipient were to receive this message, he could be reassured of the integrity of content and authenticity of sender. However, anyone with access to the public key could read it. Therefore, there are further steps which could be used to ensure confidentiality.

(3) The sender could then add a second layer of encryption using the public key of the recipient.
(4) The message is sent.
(5) The recipient decodes the message using the private key of the recipient.
(6) The recipient then decodes the final layer using the public key of the sender.

The sender's private key guarantees the content and authenticity of the message; the recipient's public key guarantees that only the recipient can read the message. However, this is a very cumbersome process. Public key cryptography requires a significant amount of processing and the double layer of encryption, and therefore can be quite impractical. Instead, the one-way-hash function can be used to obviate this difficulty.

(1) The sender writes a message.
(2) The sender uses a one-way-hash function to 'crunch' the simple text and produce the hash.
(3) The hash is then encrypted with the sender's private key.

At this point, the sender has done little more than the first two steps above. If the message were sent now, the contents would be secure

[6] See further http://www.viacorp.com/crypto.html, accessed 24 September 2001 and http://www.cs.umbc.edu/~wyvern/ta/msginteg.html, accessed 24 September 2001.

and it would certainly have come from the sender, but anyone with the public key can decrypt the hash, and anyone at all can read the simple text. The private key guarantees that the message has come from the intended person and the encrypted hash guarantees that the message arrived in exactly the same form as when it was sent. This is a digital signature. However, in the interests of confidentiality:

(4) The sender encrypts both the simple text and the private-key-encrypted hash, with the recipient's public key.
(5) The message is sent.
(6) The recipient decrypts the entire encrypted message, that is, both the simple text and the hash, using his private key.
(7) The recipient then decrypts the hash using the sender's public key.
(8) The private key holder runs the simple text through the same one-way-hash function.
(9) The recipient compares the hash produced at his end with the hash produced by the sender.
(10) If the hash produced is identical to the one included in the message, the message is authentic.

Therefore, to produce a signature, in theory, steps one and two would be sufficient in the first process, and steps one, two, and three would be sufficient in the second process. The recipient's public key ensures that none other than the intended recipient can read it. This confidentiality feature is not technically part of the signature, but is generally included in most explanations of signatures.

The public key system is heavy on processing as enormous amounts of computing power is required to encode and decode entire messages. This means that it is only really practical to send short messages, such as signatures, using this system. Which brings us full circle. Public key cryptography is often used to encode a message which includes a symmetrical key. This way the transport of the symmetrical key is secure, and the subsequent messages, which are too long for the public key cryptography, can be easily coded and decoded.

Authenticity, integrity, and confidentiality are the three key components of effective and useful digital signatures. The one-way-hash method most efficiently ensures confidentiality because the hash is a relatively small number, and therefore easier to encrypt. Both methods are effective. One is mathematically more practical than the other.

No one can describe exactly how she produces a written signature because it is an infinitely individual product of mind, brain, and body. It is of course possible to duplicate the signature itself, but not the actual method for producing it, and these duplicates are difficult to produce and difficult to guarantee. Digital signatures, on the other hand, cannot be copied once produced; however, they are produced through a mathematical process which is easily describable and useful to anyone who knows it. Signatures rely on the secrecy of the keys used in their production. In paper signatures, the keys, or processes, cannot be known by another, but digital signatures are a different story. The standard for the security of digital signatures must be the standard for the measures taken to keep the private keys secret.

At the technical level, the methods and processes of digital signatures ensure the elements of authenticity, integrity and non-repudiation. The elements must be further carried through to the legal and infrastructure levels. To this end, the reliability of any cryptographic system also depends largely on the reliability of the system for distributing keys.

IV. Public Key Infrastructure

Systems developed to distribute and manage the public keys are referred to as public key infrastructures (PKIs). The main role of PKI is to provide a mechanism for public keys to be made publicly accessible. However, PKIs must also fulfil a number of other correlated functions.

First, there must be confidence that the given public keys belong to whom they purport to belong. The system would be unworkable if a public key is thought to belong to X when in fact it belonged to Y masquerading as X. Y would then be able to receive private, confidential and even commercially sensitive information intended for X.

Second, there must be a means of revoking public keys if the owner's private key has been compromised. The suitable analogy here would be the credit card owner who loses her credit card. There must be an effective mechanism whereby the key can be cancelled quickly and effectively.

Third, disused public keys must be kept and archived in the event of a dispute in the future. The keys would be required to be produced to enable the settlement of disputes.

It is possible that the last two of these functions can be performed by the key owner. However, it is doubted if key owners can be trusted to remain honest in the event of a dispute. If businesses and consumers cannot be assured of the authenticity and the impenetrability of the signature systems they use, there is little likelihood of e-business becoming the benchmark for global commerce.

The PKI systems in use around the world generally utilise the services of a trusted third party to be responsible for attaching an individual with a public key. The trusted third party is generally known as a certification authority. The certification authority would require evidence that a particular individual is appropriately using a digital signature and this is normally achieved through requiring the applicant to present themselves at an office of the certification authority with proof of their identity. The certification authority then issues a digital certificate containing a copy of the public key of the individual signed by the certification authority.

Digital certificates are in essence messages indicating that a public key belongs to a particular person or entity. Digital certificates are themselves digital signatures as the certification authority uses its private key to validate the message. A certification authority in turn can be validated by higher certification authorities, thus creating a certificate chain. Hence, the trustworthiness of a certification authority may depend on its reputation in traditional business transactions, or, it may be a subscriber of a higher certification authority, and use the certificate of the higher certification authority to reassure subscribers and relying parties that it is not a bogus certification authority. The certification authority at the pinnacle of the certification authority hierarchy is known as a root certification authority and it issues root certificates. The root certification authority self-authenticates for purposes of determining the validity of the certificates.

The trends in PKI systems indicate the widespread use of two key pairs: one pair for use in signatures, the other for use in general communication. There are indications of a widespread use of PKI databases to lodge signature-only public keys. Access to standard encryption keys remains restricted in order to manage the flow of encrypted communication effectively. Emphasis is placed on the primary role of PKI in disseminating public keys for use in communication.

Public key infrastructure is a matrix of non-governmental certification bodies which have developed a system of cross-verification. This system produces authenticity by assuming that each authority wishes to protect and enhance its reputation. This assumption is then tested as each authority checks the security of another authority's system. In this way, one authority can often carry the seal of numerous others, as a testimony to its own reliability. In return, that authority will test and seal numerous others.

The question for users is one of information. Without certification, it would be impossible to tell whether the public key to be used in a transaction is either legitimately attached to the person you are led to believe it is, or as secure as you are led to believe. If the non-governmental authorities are relatively unknown in the sender's jurisdiction the problem is only slightly alleviated, because while there may be a seal, the consumer may have little knowledge of the authority behind it. The challenge for international policy-makers is to establish a system which clearly articulates the status of non-government certification bodies across jurisdictions. The PKI system is a non-governmental response to this dilemma but relies heavily upon quasi-customary notions of reputation and mutual trust.

The development of PKI is still in its infancy. The infrastructure is in the early stages of development and most of the progress in many jurisdictions thus far is the result of industry cooperation rather than legislative codification.[7] However, it is imperative that the roles and responsibilities within the PKI system are clearly defined so as to ensure the elements of authenticity, integrity and non-repudiation are maintained and the successful take up of e-commerce can occur.

V. Accreditation, Licensing and Liability of Certification Authorities

In relation to public key infrastructure, the issue of failure of a certified signature is a vexed question. Without confidence of where liability lies in PKI systems, consumers and businesses will not be willing to take up the use of digital signatures. This is an issue central to the 3 functions of PKIs identified above, namely authentication, integrity and non-repudiation. This is also a difficult question for national legislators and has produced, unfortunately, a variety of responses.

There are three basic approaches to the issue of regulation of electronic signatures which national legislators have taken. These approaches determine to a large extent the approach taken to deal with specific technologies such as digital signatures, and in particular, the issue of certification authority liability. The first approach towards electronic signatures is a minimalist approach which has the primary aim of facilitating the use of electronic signatures generally. These generally do not advocate a specific protocol or technology. The

[7] Australia is a typical example—there are also still many legal issues that require resolution; see, for example, the consultation paper released in June 2001 by the Australian Privacy Commissioner, *Privacy Issues in the Use of Public Key Infrastructure for Individuals*, available at <http://www.privacy.gov.au/publications/dpki.html> accessed 26 September 2001.

legislative framework seeks to remove existing legal obstacles to the recognition and enforceability of electronic signatures and records.[8]

The second approach is a more prescriptive approach that usually includes a desire to establish a legal framework for the operation of PKIs. Legislation and regulations enacted under this approach often adopt asymmetric cryptography as the approved means of creating a digital signature and impose certain operational and financial requirements on certification authorities. Most also prescribe the duties of key holders and define the circumstances under which reliance on an electronic signature is justified.[9]

The adoption of these approaches falls closely in line with the systems of law in which each has evolved.[10] Traditional common law countries such as Canada, the United States, the United Kingdom, Australia, and New Zealand have tended towards a minimalist approach. In contrast, civil law countries have tended to opt for the prescriptive approach.[11]

The third approach is a hybrid approach often in the form of two tiers. The first tier takes a broad view of what constitutes a valid electronic signature for legal purposes of laws and the second tier prescribes standards for the operation of PKIs.[12] The virtue of this approach is that there is scope for the creation of a defined and more predictable legal environment with the incorporation of an authentication technology of choice.

This two-tier approach is the approach adopted by the European Union Electronic Signatures Directive.[13] The two tiers can be seen as follows in the Directive. First, it ensures that a signature will not be denied legal effect solely on the ground that it is in electronic

[8] Susanna Frederick Fischer, "California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation" (2001) 17 *Boston U. J. of Sc. & Tech. L.* 229.

[9] *Ibid.*

[10] Internet Law and Policy Forum, *An Analysis of International Electronic and Digital Signature Implementation Initiatives*, available at http://www.ilpf.org, accessed 20 March 2002.

[11] Bradford Biddle, "Legislating Market Winners: Digital Signature Laws in the Electronic Commerce Marketplace" (1997) 34 *San Diego L. Rev.* 1225, at 1233–37; Amelia H. Boss, "The Internet and the Law: Searching for Security in the Law of Electronic Commerce" (1999) 23 *Nova L. Rev.* 583, at 602–03, 606; Report of Expert Group to the Attorney General of Australia, *Electronic Commerce: Building the Legal Framework, Executive Summary* (1998), available at http://www.law.gov.au/aghome/advisory/eceg/ecegreport.html, accessed 20 October 2001; *Electronic Signatures in Global and National Commerce Act of 2000,* 15 U.S.C. S 7001 (Supp. 2001) (U.S.); *Uniform Electronic Transactions Act* 1999 (U.S.); *Electronic Transactions Act* 1999 (Aust.); *Electronic Communications Act* 2000 (UK.); *Electronic Transactions Bill* 2000 (N.Z.).

[12] Fischer, *supra* note 8.

[13] Directive 1999/93/EC, available at http://europa.eu.int/comm./dg15/en/media/sign/Dir99-93-ec%20EN.pdf, accessed 8 April 2001.

form.[14] This applies to any electronic signature. The Directive calls such a general authentication method an 'electronic signature'. Second, the Directive also states that one specific kind of electronic authentication receives the same legal value as a hand-written signature.[15] This authentication method is described in the Directive as an advanced electronic signature based on a qualified certificate created by a secure-signature-creation device.[16] There are around 30 requirements that need to be fulfilled in order to have this kind of signature.

Another subscriber to the two-tier approach is Singapore's *Electronic Transactions Act* 1998. The regime takes a similar approach, and distinguishes between technologies based on levels of security by establishing one legal treatment for "electronic signatures," and another for "secure electronic signatures." The "electronic signatures" are generally given minimum legal effect, while the "secure electronic signatures" are entitled to an additional presumption of integrity, a presumption that the signature is that of the person with whom it is associated, and a presumption that the user affixed the signature with the intent of signing or approving the document.[17]

The point here is not to espouse a particular approach to electronic signatures regulation. The prescriptive approach and the two-tier approach obviously allow legislatures and regulatory agencies to play a direct role in setting the standards for and influencing the direction of new technologies. But it is their facilitation of mechanisms to stipulate liability and produce certainty in the use of digital signatures that is favourable. With the level of authentication and integrity and hence security attached to digital signatures at the technical level, the same level of authentication and integrity must also be present at the PKI level. It is only with the sufficient levels of authentication and integrity present at the PKI level that the non-repudiation function of digital signatures can be properly achieved.

In the global world of the Internet, transacting parties may not be able to reliably verify each other's identity. A certification authority plays the important role of a trusted third party in vouching for the identities of holders of certificates that it issues. Parties participating in online transactions should be able to use the digital certificates to reliably verify the identities of the transacting parties. Due to their position of trust, certification authorities should be subjected to high standards and control.

[14] Directive 1999/93/EC, article 5(2).

[15] Directive 1999/93/EC, article 5(1).

[16] Directive 1999/93/EC, articles 2 and 5.

[17] Section 18, *Electronic Transactions Act* 1998.

A. *Licensing and Accreditation*

The regulation and control of certification authorities should not be dependant upon the licensed or unlicensed nature of a regime. The EU Directive allows for voluntary accreditation and the Singapore system allows for voluntary licensing. Singapore does not require certification authorities to be licensed, but it does impose a number of other requirements regardless of whether they are licensed or not. These requirements include that all certification authorities must issue a Certificate Practice Statement or abide by the statute-prescribed requirements for issuing digital certificates.[18] In addition, all certification authorities must comply with statutory standards for disclosing material information about a certificate and the procedures involved in revoking or suspending certificates.[19] Thus it can be seen that it is possible to regulate and control certification authorities independently of whether or not the regime requires certification authorities to be licensed.

Mandatory licensing of certification authorities is prohibited under the EU Directive. However, member states are permitted to include voluntary accreditation schemes for the purpose of creating an enhanced level of certificate services. Thus if a member state wishes to introduce a system of electronic signatures that is more secure than those specified in the Directive, they are permitted to do so under voluntary accreditation schemes. The Directive grants enhanced legal effect to electronic signatures that satisfy certain technical criteria. In practice, the evidentiary hurdles for signatures that meet the criteria for enhanced legal effect will be lower, which could create a powerful incentive to use them.

In Singapore, a licensed certification authority will enjoy the benefits of evidentiary presumption for digital signatures it certifies. This means that the party relying on the signature merely has to show that the signature has been correctly verified, and the onus is on the party disputing the signature to prove otherwise.[20]

B. *Liability*

Irrespective of the existence of any licensing schemes, the certification authority is in a position of trust. As such, certification authorities need to be subjected to an established set of standards and controls, so as to

[18] Section 29, *Electronic Transactions Act* 1998.

[19] See generally Part VIII, *Electronic Transactions Act* 1998.

[20] Sections 18 and 20, *Electronic Transactions Act* 1998 and *Electronic Transactions (Certification Authority) Regulations* 1999.

instil public confidence in the services offered by them. The liability of certification authorities should be clearly defined to ensure certainty and to promote take up of digital signatures. Two of the most hotly debated areas of liability of certification authorities are where there are inaccuracies or misrepresentations contained in the certificate and where the certification authority fails to revoke an invalid certificate. Under contract and tort law, the certification authority's potential liability can be quite steep depending on the value of transactions for which digital signatures can be used. Relying on contract and tort law is also problematic as it is dependant on the laws of particular jurisdictions and ensures little certainty.

In closed PKI systems, the parties may use contract law to apportion liability amongst themselves to an acceptable degree. In open PKI systems however, where a relying party has no contract with the certification authority and probably never will have such a contractual relationship, the matter falls to be determined under general law.[21] The law of negligence would provide a common source of applicable law but the concept of negligence is anything but uniform throughout the many jurisdictions. Further, in some jurisdictions such as Australia, statutes also confer rights on a consumer such as a relying party. For example, s52 of the Australian *Trade Practices Act* 1974 prohibits misleading and deceptive conduct on the part of corporations. Arguably, if a certification authority issues digital certificates with inaccuracies or if they fail to effectively revoke a certificate, they would be liable to the relying party under the Act. This, however, is exactly the type of uncertainty that is produced where certification authority liability is not clearly defined. One is left at the mercy of the laws of individual countries.

Significantly, the EU and Singapore have taken a similar approach to the issue of certification authority liability. Both have taken an approach that combines some variant of strict liability for certain acts or misrepresentations with a system that permits the certification authority to limit its liability under certain circumstances. In Singapore for example, sections 23 and 30 of the *Electronic Transactions Act* 1998 set out the reliance that can reasonably be placed on digital certificates. Section 44(1) of the Act requires licensed certification authorities to specify recommended reliance limits in the certificates they issue. Section 45 of the same Act states that the recommended reliance limit is effectively a cap on the certification

[21] The Certification Authority's agreement with the subscriber may specify the allocation of liability as it relates to a relying party but reaching agreement on the allocation and the enforcement of the allocation of liability may be difficult.

authority's potential liability for losses caused by reliance on a misrepresentation in the certificate or as a result of any failure to comply with the statute-prescribed requirements for issuing a certificate. Non-licensed certification authorities may also place reliance limits on the certificates they issue but the statute only accords this legal advantage to licensed certification authorities.

In terms of forged digital signatures, licensed certification authorities also stand in a more advantageous position. Section 45 of Singapore's *Electronic Transactions Act* 1998 absolves a licensed certification authority from liability so long as the requirements of the Act have been complied with. This to some extent reflects the allocation of liability of parties who rely on a paper-based signature that has been forged. Section 44(2) of the same Act allows licensed certification authorities to specify different reliance limits for different types or classes of certificates issued. This takes into account the situation where the value of the transaction is $10 as opposed to a transaction worth $1 milllion.

Similarly, the EU Directive generally imposes strict liability on a certification authority for losses caused by reliance on an inaccurate qualified certificate or failure to abide by the requirements for issuing a qualified certificate. Certification authorities can however specify the permissible uses of a qualified certificate and the maximum value of any transaction for which it may be used.[22] In effect, these schemes permit the certification authority to define the value of a particular certificate in the manner described above.

These strict liability schemes should be followed internationally. In particular, there should be a floor of agreed acts and misrepresentations where strict liability applies. These can then be limited through giving the requisite notice on the digital certificates themselves. There is merit in the wording of the EU Directive's approach but for the inclusion of the concept of negligence. Article 6(1) and 6(2) reads:

> 1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:
>
> (a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;

[22] Directive 1999/93/EC, article 6.

> (b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
>
> (c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;
>
> unless the certification-service-provider proves that he has not acted negligently.
>
> 2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

The concept of negligence and in particular, its absence, is one that absolves a certification authority from liability. Hence it is a central concept in determining the liability of a certification authority. However, as noted above, negligence is a concept that has different meaning in different jurisdictions and it has also been interpreted differently in many jurisdictions. Its inclusion in any digital signatures regulation should be avoided for the very reason that it will wreak inconsistencies and confusion across jurisdictions. Further, the confusion as to the meaning and interpretation of will not be evident. Subscribers, relying parties and the general public will be under the misconception that their conception and understanding of negligence is a universal one.

An example of where the EU Electronic Signature Directive has been implemented is in the United Kingdom, by the *Electronic Communications Act* 2000 and the *Electronic Signatures Regulations* 2002 which came into force on 8th March 2002. The provisions of the EU Directive that relate to the supervision of certification service providers and their liability in certain circumstances are found in the *Electronic Signature Regulations 2002.* The relevant portions of Regulation 4 states:

> **4.** -(1) Where –
> (a) a certification-service-provider either –
> (i) issues a certificate as a qualified certificate to the public, or
> (ii) guarantees a qualified certificate to the public,

> (b) a person reasonably relies on that certificate for any of the following matters –
>
> (i) the accuracy of any of the information contained in the qualified certificate at the time of issue,
>
> (ii) the inclusion in the qualified certificate of all the details referred to in Schedule 1,
>
> (iii) the holding by the signatory identified in the qualified certificate at the time of its issue of the signature-creation data corresponding to the signature-verification data given or identified in the certificate, or
>
> (iv) the ability of the signature-creation data and the signature-verification data to be used in a complementary manner in cases where the certification-service-provider generates them both,
>
> (c) that person suffers loss as a result of such reliance, and
>
> (d) the certification-service-provider would be liable in damages in respect of any extent of the loss –
>
> (i) had a duty of care existed between him and the person referred to in sub-paragraph (b) above, and
>
> (ii) had the certification-service-provider been negligent,
>
> then that certification-service-provider shall be so liable to the same extent notwithstanding that there is no proof that the certification-service-provider was negligent unless the certification-service-provider proves that he was not negligent.
>
> (2) For the purposes of the certification-service-provider's liability under paragraph (1) above there shall be a duty of care between that certification-service-provider and the person referred to in paragraph (1)(b) above.

Regulation 4 then continues in the same vein but in relation to the failure of a certification authority to register revocation of a certificate. Regulation 4 in effect sets up a duty of care between the certification authority that issues a qualified certificate and a relying party who has suffered loss. Regulation 4 however imposes liability on certification authorities in certain circumstances even though there is no proof of negligence, unless the certification authority in question can prove it was not negligent. Like the EU Directive, the UK legislation speaks in terms of negligence, a jurisdiction-specific concept which perpetuates uncertainty and confusion across jurisdictions.

The Singapore legislation is framed in terms of duties. Part VIII of the *Electronic Transactions Act* 1998 sets out the duties that certification authorities must observe. These are fairly clear and they do not refer to jurisdiction specific legal concepts such as negligence. They are also quite detailed and allow standards to be set and maintained regarding a range of matters including contents of digital certificates and the conduct of business. However, the Singapore legislation does not clearly state the legal sanctions if the duties are breached. In the event of a breach, a number of sanctions are possible. First, it may give rise to a common law action for breach of statutory duty.[23] Secondly, under s51 of the Act, the Controller may issue a notice in writing directing the certification authority to comply with the provisions, failing which the certification authority would be guilty of an offence under s51. An offence under s51 carries either a fine of up to $50,000 or imprisonment of up to 12 months, or both. Thirdly, under s42, the Minister may make regulations with respect to a range of matters concerning certification authorities, and these may provide that the contravention of a specified provision is an offence, and to also further specify the penalty. In the event of non-specification of the penalty, s56 specifies the default penalty that will apply to an offence under the Act or regulation.

For a relying party, the duties set out in Part VIII and the breach of them may not be of direct relevance as they do not generally provide civil sanctions. The main provision of significance to a relying party would s45 discussed above. A relying party would be wise to only rely on certificates issued by licensed certification authorities. It is implicit in s45(b) that such a certification authority would be held liable for a misrepresentation in the certificate of a fact that the certification authority was required to confirm, but the amount of the liability would be capped at the recommended reliance limit. When this is taken together with the criminal sanctions present for breach of the duties under Part VIII, an effective system for deterring breach of the duties under Part VIII is produced. With a system that encourages and supports the discharge of duties and hence encourages and supports certainty, the Singapore regime is undoubtedly the most effective regime for attaining the elements of authenticity, integrity and non-repudiation at the legal infrastructure level.

VI. Conclusion

Digital signatures are a specific breed of electronic signatures. They have been technically designed to provide a high level of authentication and integrity. The system for the distribution of the public keys must also necessarily be one which meets the requirements of authenticity and integrity so as to provide confidence in the usage of

[23] Daniel Seng, *Legal Guide to The Electronic Transactions Act*, at 25.

digital signatures. Herein lies the role of certification authority regulation. The law must provide users with certainty and re-assurance that the characteristics of authenticity, integrity and non-repudiation exist. This can be achieved by clearly defining the apportionment of liability should a digital certificate fail. And this includes defining the liability without reference to concepts such as negligence which are jurisdiction-specific legal concepts.