LEGAL ISSUES AND TECHNICAL ASPECTS ON MECHANISM OF DIGITAL SIGNATURE IN MALAYSIA

Tay Eng Siang & Goh Choon Yih

Lecturer, Faculty of Business and Law, Multimedia University
E-mail: estay@mmu.edu.my, cygoh@mmu.edu.my

ABSTRACT

The Digital Signature Act 1997 (Act 562) (hereinafter called "the Act") came into force since 1 October 1998 to regulate the use of digital signature and to provide for matters connected therewith in Malaysia. Among those issues concern on digital documents transmitted over any electronic networks are interception, tampering, deception, non-repudiation and authenticity. To what extent the digital signature has overcome or solved these concerns from legal and technical aspects? This paper intends to look into selected legal issues on digital signature and the technical aspects of digital signature mechanism in Malaysia. Suggestions and recommendations will also be made to improve the effectiveness of the present recognised digital signature system in protecting and solving the above issues.

KEYWORDS

Digital signature – legal & security issues – asymmetric cryptosystems –certification authority.

1. INTRODUCTION

The aim of this research is focused on the legally recognised digital signature in Malaysia. Among those crucial questions surrounding the digital signature are legal and security issues concerning digital documents transmitted over any electronic network such as interception, tampering, deception, non-repudiation and authenticity. To what extent the digital signature has overcome or solved these concerns? The objective of this paper is to look into the technical mechanism and selected legal issues on the recognised digital signature in Malaysia. Some suggestions and recommendations will also be made to improve on the effectiveness of the present recognised digital signature in protecting and solving the above issues.

This paper shall begin with the general definition of a digital signature (as compared with the traditional signature). Next we shall look into the legislation which governs and recognises the digital signature in Malaysia particularly from its technical mechanism and legal effects. Weaknesses on selected aspects of the recognised digital signature will be discussed and ended by proposals for amendment to the Act.

2. ELECTRONIC BUSINESS - SIGNATURE

For every transaction or business that is being conducted, the level of the security is always the main concern in determining the successfulness for these activities. According to Davis and Benamati (2003), security is the "quality or state of being secure", which includes "freedom from danger" and "freedom from fear and anxiety". With the evolving of Information Communications Technologies (ICT), a new way of business has evolved which we refer it as E-business. E-business includes the exchange of information not directly related to the actual buying and selling of goods through any electronic networks such as the Internet and intranet. For any dot-com company, information is the most important of all to the business. Securing information is the most expensive, difficult and complex aspect of e-business (Whelan & Maxelon, 2001). Among the information that need to be secured are business strategies, prices, customer's information, research information and others.

In the old days, security has always been about keeping people out (Whelan and Maxelon, 2001). When considering the security of a business today, it is very much about dissolving the boundaries between customer and the business, staff and the business, business and trading partner, and business processes with our business.

With the high acceptance and usage of computing technologies throughout the business, security has become an increasing concern. The challenges a company might face can be subdivided into a few areas. For the purpose of this paper, we will focus on the area of information privacy and information integrity that most businesses are concern about.

Privacy infringement happens where others read or copy a data or information which they are not entitled. While keeping information private, it is important to note that sometimes is enough for a competitor to only watch how a business manage and organise important data and information.

The most concern threat is during the sending or transferring confidential data or information through any electronic network. A message or information sent by the sender might be tapped or copied by an unintended person before it reaches the intended receiver. This unintended person will be able to read, alter, or even delete the message. Hence, privacy and secrecy have been compromised. According to Davis and Benamati (2001), no matter how well a network is protected, some intrusion attempts will succeed. So, one company must understand the levels of security required in order to minimize the risk of this intrusion. One solution to this situation will be using some secret codes or symbols to represent the data or information. This is usually referred to as the digital signature and the technical mechanism of which will be discussed in Part 3.2 below.

2.1 Traditional signature

Traditionally, a person may sign on the document and the signature may serve various purposes. A "sign" is defined under section 3 of the Interpretation Acts of 1948 and 1967 (Consolidated and Revised 1989) (Act 388) to include the making of a mark or the affixing of a thumb-print. Signing a document serves the following general purposes. Firstly, a signature serves as a proof of evidence that the document is duly signed by a particular person. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer. Secondly, the act of signing a document calls to the signer's attention the legal significance of the signer's act and thereby helps prevent poorly considered engagements. Thirdly, a signature expresses the signer's approval or authorisation of the writing's content or the signer's intent that it has legal effect and force.

2.2 Digital signature

In the digital world, digital signature can serve as analogues to paper signatures but are different in interesting ways. Digital signature appearing in digital documents transmitted in digital world may appear in many forms based on various systems, such as symmetric cryptosystem, asymmetric cryptosystem, EES (Escrowed Encryption Standard), biometric method (fingerprint validation and retinal scans), SSL (secure socket layer) and SET (secure electronic transaction).

The main issues arise in the online or electronic transactions are of trust and security. Parties to electronic contract must be satisfied that the sender and receiver in the electronic transactions are who they purported to be. The sender and receiver must also be convinced that their electronic record can be authenticated and not forged while in transit. Unlike traditional signature which may require person to witness the signature in certain situations, a digital signature will be verified by a licensed certification authority through a trustworthy system. Basically digital signatures provide assured provenance (only the person in possession of the private key could have created the signature) and non-repudiation (the object must have been signed by the possessor of the key, because the signature could not have been created in any other way).

Thus the invention of the digital signature has provided the following benefits: (a) authentication of the sender's identity to the receiver by an entrusted third party; (b) verification of genuineness of the message (*i.e.* that it has not been altered); (c) security of information sent (*i.e.* no one can tamper with the message without jeopardising the verification process); and (d) the sender is unable to repudiate the effect of his signature (*i.e.* sender is not able to say that the signature is not his).

3. DIGITAL SIGNATURE ACT AND ITS APPLICATION

Three aspects of digital signature will be discussed here, *i.e.* the recognised digital signature under the Act, its technical mechanism and the legal effects of the digital signature.

3.1 Digital signature under the Digital Signature Act

The Act came into force since 1 October 1998 to regulate the use of digital signature and to provide for matters connected therewith in Malaysia. The Act is modelled on the Utah Digital Signature Act 1995. The Act is proactive to facilitate the e-business/e-commerce activities by using the digital signature instead of conventional handwritten signature in legal and commercial transaction. The purposes of the Act are twofold, *i.e.* to encourage electronic transactions, especially commercial, to deter forgeries (computer-generated fraud) and to provide a more secure means of online identification procedure (Abu Bakar, 1999).

The Act establishes a regulatory regime for reliance of digital signatures and creates methodologies for ensuring security of signatures by imposing security audits by third parties, i.e. *licensed certification authority*. The Act also sets out a mandatory licensing scheme for *certification authorities* (being the issuers of digital certificates), the *subscribers* (owners of digital certificates) and *recognised repositories*.

"Certification authority" means a person who issues a certificate (section 2 of the Act). The licensing scheme is proposed to establish a minimum regulatory system to provide a basic level of reliability in certification authority practice without undermining the reliability of any signature by invalidating it for lack of a regulatory licence. The Act only recognises one type of "digital signature". Those signatures issued from unlicensed certification authority will not gain full protection offered by the Act compare to a signature from a *licensed certification authority*. It is an offence under section 4 of the Act for a person who carries or operates as a certification authority without a valid licence and shall, on conviction be liable to a fine not exceeding RM500,000/- or to imprisonment for a term not exceeding 10 years or to both. A "licensed certification authority" means a certification authority to whom a licence has been issued by the Commission and whose licence is in effect (section 2 of the Act). Note that the Commission here means the Malaysian Communications and Multimedia Commission established under the Malaysian and Multimedia Commission Act 1998 (Act 589) (section 2 of the Act). Currently there are three licensed certification authorities in Malaysia, *i.e.* MSC Trusgate.Com Sdn. Bhd. and Digicert Sdn. Bhd. with effect from 26 July 2000 and 25 June 1999 respectively and Bank Negara Malaysia being a restricted licensed certification authority with effect from 24 July 1999.

Section 27(1) of the Act provides that a *licensed certification authority* shall only use a *trustworthy system* – (a) to *issue, suspend or revoke a certificate*; (b) to publish or give notice of the issuance, suspension or revocation of a certificate; and (c) to *create a private key*, whether for itself or for a *subscriber*. The Act defines "*trustworthy system*" as computer hardware and software which – (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability and correct operation; and (c) are reasonably suited to performing their intended functions.

The expression "*digital signature*" as defined in section 2(1) of the Act, means a transformation of a *message* using an *asymmetric cryptosystem* such that a *person* having the initial message and the signer's *public key* can accurately determine – (a) whether the transformation was created using the *private key* that *corresponds* to the signer's public key; and (b) whether the message has been altered since the transformation was made. "*Asymmetric cryptosystem*" means an algorithm or series of algorithms which provide a secure key pair. A "*key pair*" is defined as a private key and its corresponding public key in an asymmetric cryptosystem, where the public key can verify a digital signature that the private key creates. A "*message*" means a digital representation of information. A "*private key*" (means the key of a key pair used to create a digital signature) is said to *correspond* with the "*public key*" (means the key of a key pair used to verify a digital signature) when both keys belong to the same key pair. A detailed discussion on the technical mechanism of the digital signature can be found in Part 3.2 hereof.

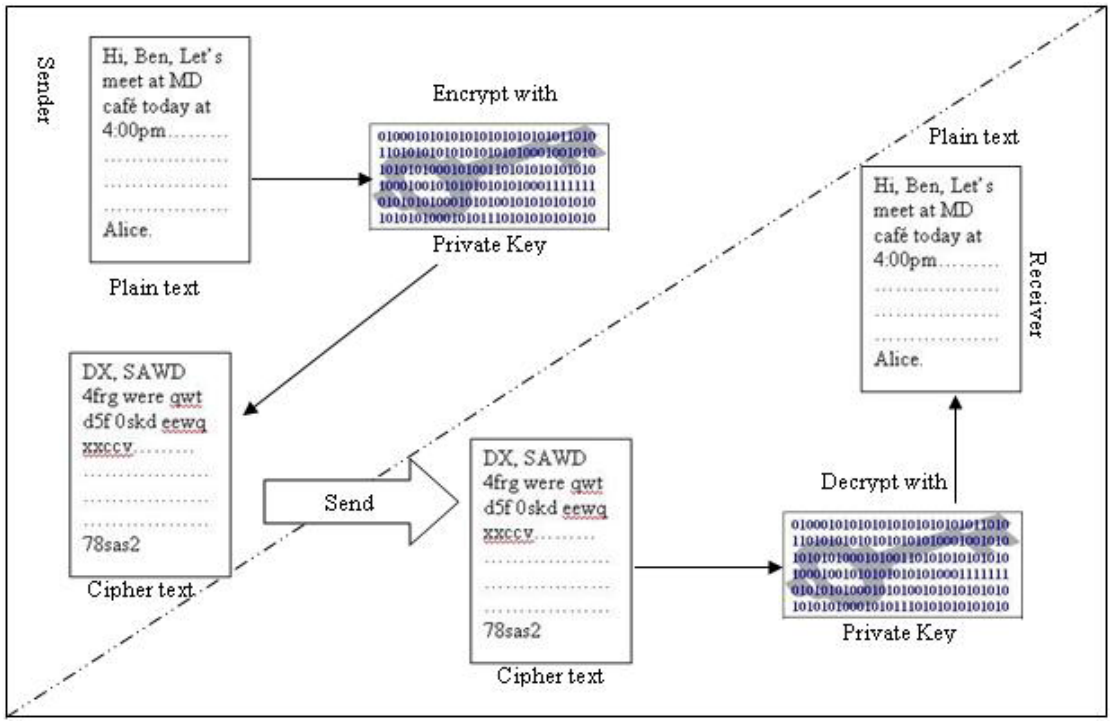
3.2 Technical mechanism of digital signature

Cryptography offers a possible solution to the risk of security issue. Cryptography is process of encrypting a message (referred to as "plain text") in order to maintain the privacy and integrity of the message's content before transferring the message through electronic networks. When the encrypted message (referred to as

"cipher text") received by the receiver, he needs to decrypt the encrypted message back to plain text message as it is being processed. In order to decrypt the message successfully, the receiver needs to use the same algorithm that has been used by the sender. If a different algorithm is used, the conversion will fail and hence it will indicate that the message is received by an unintended person.

These two cryptography technologies used today are the Symmetric Private Key Cryptography (also known as "symmetric cryptosystem" or "symmetric secret key cryptography") and the Asymmetric Public Key Cryptography (legally known as "asymmetric cryptosystem" under the Act or "public key encryption"). The Act recognises the Asymmetric Public Key Encryption only. The key used in these processes is just like password that carries out the process of encryption and decryption processes. Theses keys are generally numbers generated by computer using certain algorithm. The longer the key, the possibility for a person able to guess it will be lower. Symmetric Private Key Cryptography relies on a single key to encrypt and decrypt a message. Here, it means that the sender and receiver share a pair of same private key. The sender will encrypt a message using a private key and the receiver must use the same duplicate private key to decrypt it. The following illustration in Figure 1 shows the process of Symmetric Private Key Cryptography.

Figure 1. Symmetric private key cryptography



Private Key algorithm is almost difficult to guess. With the key length used, it might take a long time to guess the key. Another advantage of this algorithm is the encryption and decryption process are relatively fast.

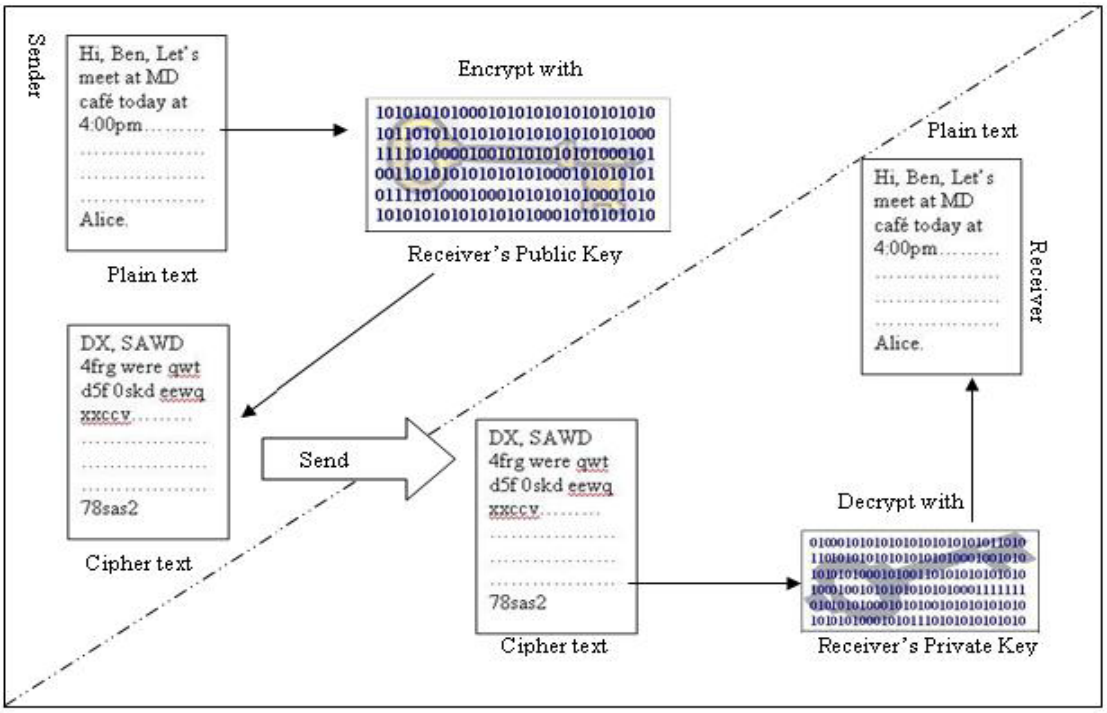
However, when the private key is discovered, lost or exposed to the public, all messages encrypted with this private key will be able to be decrypted by anyone who found the key. Here, the integrity of the message may be compromised as a person with the key can simply modify the message and re-encrypt it without the knowledge of the original sender. To avoid or at least to reduce this risk, the sender and receiver may change their shared private key often. Changing the private key frequently helps to decrease the possibilities to guess the key correctly in an acceptable time period. Even if the key is guessed successfully, at least not all messages, especially messages that are encrypted with previous key, will be exposed. Hence, it minimises the damage.

This process of key exchange however will present a significant security risk. When changing to a new key or exchanging the key, the new key needs to be sent to either the sender or receiver through electronic networks. Hence, the new key might be tapped or copied by an unintended party without the

knowledge of the sender and receiver. In another words, to ensure a successful key exchange process, it must be as secured as an encryption process.

Public key encryption was introduced in 1970s as an alternative to private key encryption. This algorithm uses two different key pair to encrypt and decrypt a message. One key will be used to encrypt a message, and the other key is needed to decrypt the encrypted message. These keys must come in pair with one private key matching a public key. A person may keep his private key, and publishes his public key in the Internet or any electronic network. For example, Alice plans to send a message to Ben, she will use Ben's public key to encrypt the message. When Ben receives the encrypted message, only his private key is able to decrypt the message successfully. This process actually works both ways. If a message is encrypted by the sender's private key, it means the message must only be decrypted by his public key. Thus, the encryption process will be of no value as anyone can obtain the public key easily. The following illustration in *Figure 2* shows the process of Asymmetric Public Key Cryptography.

Figure 2. Asymmetric public key cryptography



Public Key encryption uses much longer keys than Private Key encryption. Longer key indicates that it is much difficult to guess and here it shows that Public Key encryption is more secured than Private Key encryption. However the process of Public Key encryption and decryption are very much slower than Private Key encryption. It causes this algorithm not suitable in encrypting long messages and real-time application of the message. Anyway, Public Key encryption has the advantage over Private Key encryption as the private key is not shared among the senders and receivers.

As mentioned earlier, one of the disadvantages of Private Key encryption is that it needs to exchange key frequently as to remain the privacy and integrity of the information. The process of key exchange poses another security concern as new key needs to be sent over the electronic network.
Public Key encryption will be able to solve this disadvantage as it does not need to exchange key like Private Key encryption does. On the other hand, it seems that Private Key encryption has its advantage as well over Public Key encryption in term of speed.

Obviously, the combination of these two technologies should be able to improve the process of encryption and decryption. For example, to speed up the process, Alice can use her private key to encrypt the message. To avoid the message being decrypted by anyone by using her public key, Alice will use Ben's (the receiver) public key to encrypt her private key. It is liked inserting a key into a sealed envelope (refer as digital envelope). Alice will then send the encrypted message and the encrypted private key to Ben. Here, the

private key used to encrypt the message only being used for one time only. We may refer this private key as Session Key. Hence, there will be no key exchange problem. *Figure 3* below illustrates this process.

Upon receiving the message with the encrypted private key, Ben will use his private key to decrypt Alice's private key. Here, it is like unsealing the envelope to retrieve the key. Then, Ben will use Alice's private key to decrypt the message. *Figure 4* illustrates the process when receiving the digital envelope and message.

Figure 3. Creating and sending digital envelope by sender

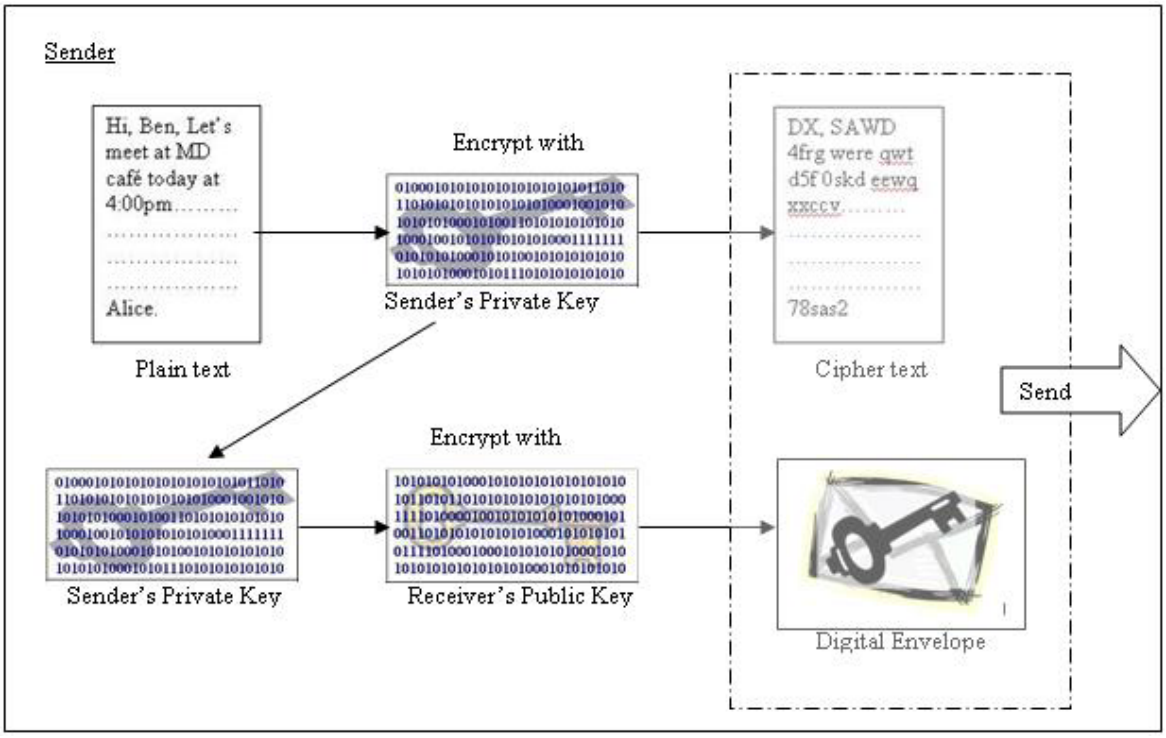
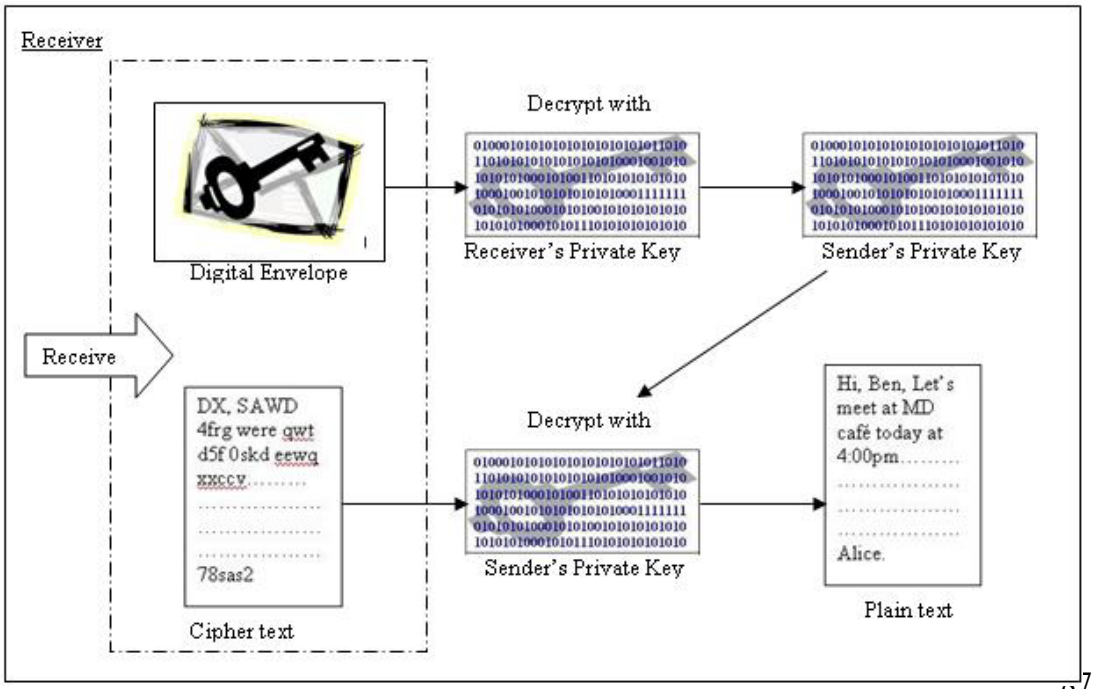


Figure 4. Receiving digital envelope



There is still a remaining issue to be considered on this encryption and decryption process. Says that Ben receives the message stated it is from Alice and the message is said to be encrypted by Ben's public key. The concern now is how can Ben be sure that the message he received is actually sent by Alice? Anyone could have stated the message using Alice's name, and easily obtain Ben's public key and encrypt the message.

Even if the message was originally sent by Alice, how could Ben be sure that the content has not been tampered or changed before it reaches him? Here, obviously the integrity of the message will be questioned.

One way to ensure the integrity of a message in this situation is to use a digital signature. To create a digital signature, Alice needs to extract a portion of the content of the message by using a hashing algorithm executed by her computer. The resultant of this process is a message digest. This message digest will be encrypted by Alice's private key, hence creating her digital signature. The digital signature will be attached along with the message and then encrypted using Ben's public key.

When Ben receives the message, he will use his private key to decrypt the message along with the digital signature. To check the validity of the message, Ben will decrypt the digital signature using Alice's public key to get the message digest. Then, Ben needs to use the same hashing algorithm that Alice used to create a new message digest. A message digest is very unique to the message, changes made on the message will change the message digest as well when using the same hashing algorithm. If Alice's message digest matches Ben's message digest, then the fact Alice is the sender is valid. It is because only Alice's public key can decrypt the message digest. The integrity of the message is also maintained. However, if Alice's message digest does not match Ben's message digest, it means the message may have been modified before it reaches the receiver. The following Figure 5 and Figure 6 illustrate the process of creating and verifying a digital signature respectively.

Figure 5. Creating a digital signature

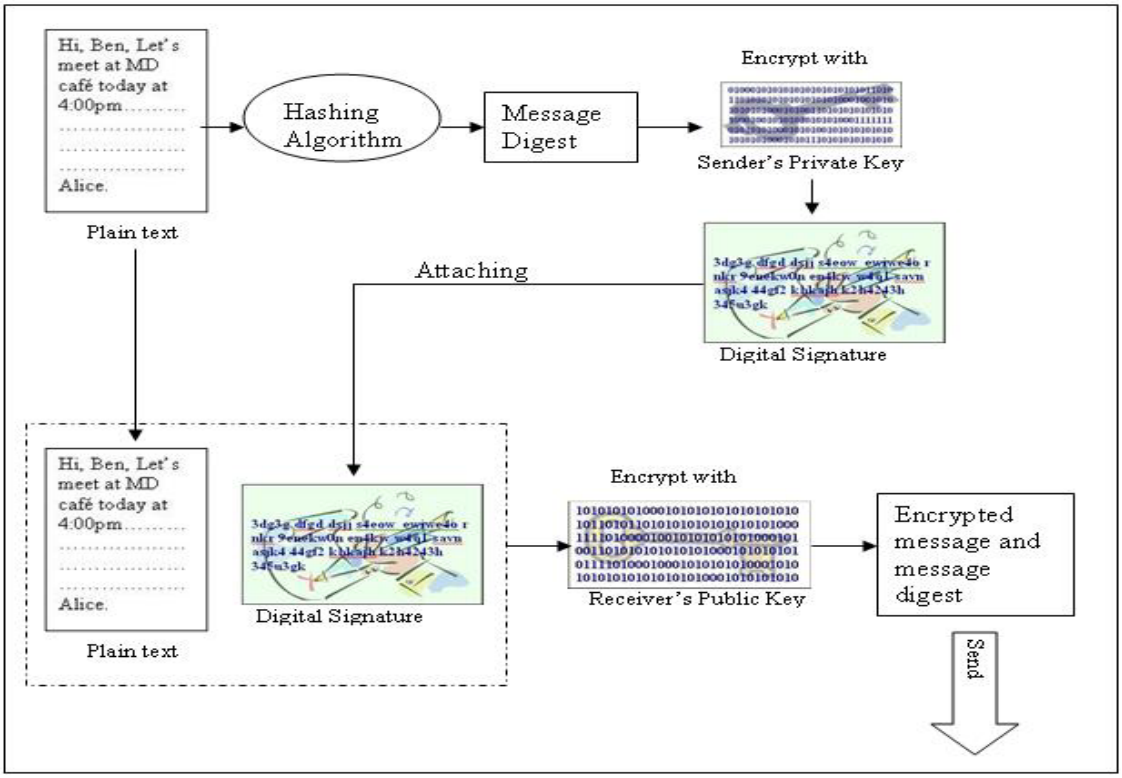
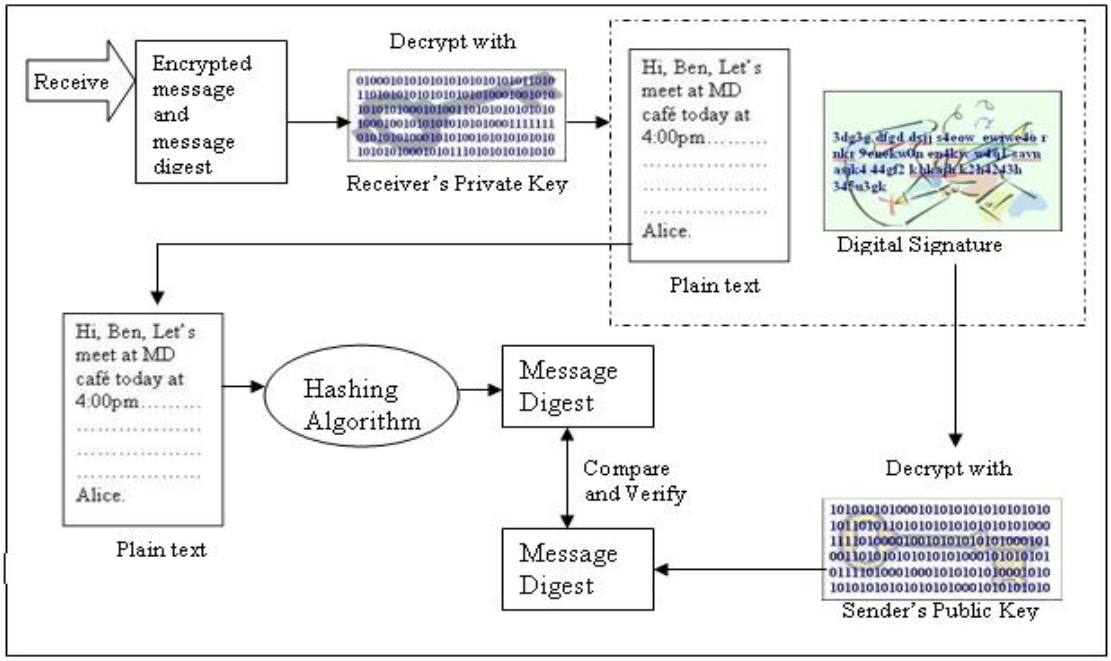


Figure 6. Verifying a Digital Signature



No doubt that digital signature is a very good authentication tool. It proves to be able to maintain the privacy and integrity of information sent through electronic networks. However, there is a possibility for someone to create a false digital signature. A hacker can always creates a pair of encryption keys and have a public key registered under Alice's name. The hacker may use the so-called Alice's private key to encrypt a message and send it to Ben. When Ben receives the message, it is stated that the message was from Alice, and the posted public key can decrypt the message successfully. This has shown that the message is from hacker although Alice actually did not send it. The content of the message might not be true, mislead Ben or it may even contain harmful executable software like virus that could harm the receiver's computer or system.

To overcome a fake digital signature, Alice can request or apply for a digital certificate. According to Laudon and Laudon (2006), digital certificate is data files used to establish the identities of users (subscribers) and electronic assets for protection of online transactions. A digital certificate is issued by a third trusted party which refers as certification authority. Certificate authority plays a role in validating a subscriber's identity. A subscriber's identity will be kept in the certification authority's server that generates the subscriber's encrypted digital certificate which contains the subscriber's information and his public key.

The certification authority will have its own public key published on the Internet. Receiver of the message (Ben, in our previous example) can use the certification authority's public key to decrypt the digital certificate, verifying that it was issued by the said certification authority. As mentioned earlier, the sender's (Alice, in this example) valid certificate will be placed on the Internet for anyone to verify her public key. The sender's digital signature (that is encrypted by her private key and can be decrypted with the matching public key) will help to verify whether or not the purported sender is the intended sender. The process above refers as Public Key Infrastructure, which is a technology of using public key cryptography working with a certification authority. This infrastructure is becoming the principle technology for providing secure authentication of identity online (Laudon & Laudon, 2006). This is the so-called asymmetric cryptosystem recognised by the Act.

4. LEGAL EFFECTS OF DIGITAL SIGNATURE

Legal effects of a digital signature are provided in Part V of the Act (sections 62-67). A digital signature is a legally binding signature; message contained in the document is valid, enforceable and effective as if it had been written on paper. A document signed with a digital signature shall be as legally binding as a document

signed with a handwritten signature, or a thumb-print or any other mark; and a digital signature created in accordance with this Act shall be deemed to be a legally binding signature [section 62(2)(a) & (b)].

Under section 64(1), a message shall be as valid, enforceable and effective as if it had been written on paper if – (a) it bears in its entirety a digital signature; and (b) that digital signature is verified by the public key listed in a certificate which – (i) was issued by a licensed certification authority; and (ii) was valid at the time the digital signature was created. Thus it would be considered a written document for Part V of the Act and also sections 91 & 92 of the Evidence Act 1950 (Act 56) and admissible by reason of section 90 there of.

Another legal implication of a digitally signed message is provided in section 65 of the Act that a copy of which shall be as valid, enforceable and effective as the original of the message unless it is evident that the signer designated an instance of the digital signed message to be a unique original, in which case only that instance constitutes the valid, enforceable and effective message. This will correspond with the evidential law provided in sections 61, 90A, 90B and 90C of the Evidence Act 1950.

A certificate issued by a licensed certification authority, under section 66, shall be an acknowledgement of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgment appear with the digital signature and regardless of whether the signer physically appeared before the licensed certification authority when the digital signature was created, if that digital signature is – (a) verifiable by that certificate; and (b) affixed when that certificate was valid.

A valid digital signature created under the Act gives rise to some legal rebuttable presumptions in the court of law in the event of disputes. A court shall presume: (a) that a certificate digitally signed by a licensed certification authority and is issued by the licensed certification authority which digitally signed it and is accepted by the subscriber listed in the certificate; (b) that the information listed in a valid certificate and confirmed by a licensed certification authority issuing the certificate is accurate; (c) that where a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority – (i) that digital signature is the digital signature of the subscriber listed in that certificate; (ii) that digital signature was affixed by that subscriber with the intention of signing the message; and the recipient of that digital signature has no knowledge or notice that the signer – (A) has breached a duty as a subscriber; or (B) does not rightfully hold the private key used to affix the digital signature; and (d) that a digital signature was created before it was time-stamped by a recognised date/time stamp service utilising as trustworthy system (section 67 of the Act). The burden of proof is shifted onto party denying application of presumption.

Unless otherwise provided by the law of contract, the receiver of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances. Section 2(1) of the Act defines "forge a digital signature" to mean – (a) to create a digital signature without the authorisation of the rightful holder of the private key" or (b) to create a digital signature verifiable by a certificate listing as subscriber a person who either does not exist or does not hold the private key corresponding to the public key listed in the certificate. The receiver who determines not to rely on a digital signature under section 63 shall promptly notify the signer of its determination not to rely on a digital signature and the grounds for that determination.

5. WEAKNESSES ON RECOGNISED DIGITAL SIGNATURE

We will look into the weaknesses of the digital signature from its legal perspective on the following selected aspects, *i.e.* the scope of its application, limitation/restriction in recognising a sole digital signature regime, qualification and duties of the licensed certification authority and subscriber.

5.1 Issues on scope of application

There is no amendment made to the Act for about 8 years since its inception in 1998. No court case has been reported so far on the operation of the Act generally and particularly the legal effect of digital signature has also not been judicially addressed. However, being one of cyberlaw statutes enacted [others are Computer Crimes Act 1997 (Act 563), Telemedicine Act 1997 (Act 564) and Copyright (Amendment) Act 1997 (Act A994)], the scope of its application is limited. The Act only governs the Malaysian within Malaysia, unlike the Computer Crimes Act 1997 which has a wider scope. Section 9(1) of the Computer Crimes Act 1997 states that the provisions thereof shall, in relation to any person, whatever his nationality or citizenship, have

effect outside as well as within Malaysia …" Thus the Act is restrictive in its application and may not be effective in the borderless cyber world where digital documents may be transmitted over all jurisdictions.

It is also not clear as to what specific types of transaction (personal or corporate) the Act targets. A look on the provisions of the Act shows that heavy penalties are imposed for non-compliance of the said provisions. For examples, section 4(2) of the Act provides that any person who shall carry on or operate as a certification authority without a valid licence shall be liable for a fine not exceeding RM500,000/- or to imprisonment for a term not exceeding ten years or to both. Section 83(1) provides for the general penalty of a fine not exceeding RM200,000/- or to imprisonment for a term not exceeding four years or to both if a person committed an offence under the Act (for which no penalty is expressly stated).

Looking at the harshness of the punishment provisions and the background of the Act, it is submitted that the Act is not consumer protection legislation but mainly targets those international corporations considering investment in Multimedia Super Corridor. Potential users of the Act are companies, organisations, government and non-governmental bodies. Currently, the Inland Revenue Board Malaysia has attempted to implement the e-filing of income tax return for individuals. This e-filing requires the application of digital signature to verify the identity of the taxpayer. The Inland Revenue Board hopes to fully implement this e-filing for the Year of Assessment 2007.

The Act has to be read in conjunction with other laws, regulations and policies with signature requirements. For examples, Interpretation Acts of 1948 & 1960 on the interpretation of certain terms; Evidence Act 1950 on the admissibility and evidential quality of computer records; Banking and Financial Institutions Act 1989 (BAFIA) and Payment Systems Act 2003 being regulatory frameworks for Electronic Funds Transfer authorisation; Bank Negara Malaysia Guidelines on Internet Banking, use of digital certificates and signature to establish non-repudiation; and contract law on the issue of attribution and authority to contract. The Act is also silent on addressing issues on formation of electronic contract, which can only be resolved through the general principles of contract law laid down in Contracts Act 1950.

5.2 Issues on digital signature

Unlike traditional signature which has no duration (except if a natural person has died), the recognised digital signature under the Act has a maximum duration of three years from the date of its issuance as stipulated in the digital certificate under section 59(2). There is no provision on renewal of digital certificates; presumably the subscriber may have to re-apply for a new certificate valid for another three years on the same process.

Furthermore, by restricting itself to a technology specific system (asymmetric cryptography), the Act has precluded other technologies which have been in existence such as EES (Escrowed Encryption Standard) and biometric method (fingerprint validation and retinal scans); SSL (secure socket layer) and SET (secure electronic transaction) or may be developed in future. This has raised the concern on the security issue as the hardware and software used to create digital signature may be vulnerable to unauthorised access or unauthorised modification.

The legal benefits obtained from a recognised digital signature are basically legal presumptions discussed in Part 3.3 above and the effect is to shift the evidential burden of proof to the other party. The Act does not forbid the contracting parties to agree on certain other types of digital signature using other technology, and hence the burden of proof will lie on the party who makes the allegation.

The Act creates a regime for the use and recognition of digital signature and contains a few provisions with regards to the issue of security such as duty of certification authority and subscriber to use trustworthy system (section 27) and duty of subscriber to exercise reasonable care to retain control of private key and prevent disclosure to unauthorised persons (section 43). These will be discussed in Part 4.3 below. Unfortunately, the Act does not deal with criminal elements of hacking (unauthorised access and unauthorised modification), presumably these aspects are governed by the Computer Crimes Act 1997.

5.3 Issues involving certification authority and subscriber

The Act does not set the qualifications for a licensed certification authority. There is neither education or professional qualification nor specialised training requirement to be a licensed certification authority. The only provisions available are regulations 6(h) and 41 of the Digital Signature Regulations 1998 (PU(A) 259/1998) . Regulation 6(h) mentions that a certification authority shall employ "operative personnel" who have not been convicted within the past fifteen years of an offence involving fraud, false statement or deception; and who have demonstrated "knowledge" and proficiency in following the requirements of the Act and these Regulations. On the other hand, a certified public accountant or an accredited computer security

professional intending to act as a compliance auditor under section 20 of the Act shall have the requirements stated in regulation 41, *inter alia*, at least two year experience in trusted computer information system, trusted telecommunications networking environments and professional audit techniques; at least two years experience in digital signature technology, standard and practices; and demonstrates "knowledge" of the requirements of the Act and these Regulations. It is the writers' opinion that the test should be a strict one, baring in mind that the Act requires the trustworthy persons, who may be in fiduciary relationship with the subscribers (for holding the private key of the subscriber under section 45 and have access to the transaction information), to run a trustworthy system. We could not afford to risk worrying about the internal human security issue and at the same time to safeguard the external technological security issues.

There is no delineation of how financial accountability of certification authority and subscribers is to be determined. Under section 60 of the Act, a licensed certification authority shall specify a recommended reliance limit in the digital certificate to a subscriber. "Recommended reliance limit" means monetary amount recommended for reliance on a digital certificate (section 2 of the Act). The Act is silent on the guidelines on how will reliance be set. Further, protection granted to the licensed certification authority, as stated in section 61 of the Act that, a licensed certification authority shall not be liable, *inter alia*, for the loss caused by reliance on a false or forged digital signature of a subscriber; and punitive or exemplary damages or damages for pain or suffering.

There is also no provision for the licensed certification authority to carry the liability insurance nor any specific amount required as surety bond. The Act does not establish any testing requirement to objectively insure that the licensed certification authorities understand the full range of their responsibilities (technological process, legal and ethical duties, statutory procedures and legal liabilities).

The asymmetric cryptosystem does not reduce the risk involved in the signing of an electronic document but transfer risks to private key. The digital signature (in algorithm sequence) cannot be remembered as it is stored in computer device such as smart card, and thus the device must be kept in a safe place. The only presumption is that if a document is signed with someone's private key, the receiver may expect that this comes from that person. Pursuant to section 43, the Act only imposes the duty on the subscriber to 'exercise reasonable care' in retaining control of his private key. This standard of care is not sufficient and unsatisfactory to curb forgery or fraud. Since the private key is the personal property of the subscriber under section 44 of the Act, it is suggested that absolute liability should attach to private key holder to hold and control his own private key.

6. CONCLUSION

As part of to strategy to increase the usage of digital signature in e-business, it clearly matters that the technology should be inexpensive to introduce and to use. To ease the usage of this technology especially for those unskilled private individuals, the mechanism of the digital signature should be as comfortable and easy as – in much the same way as the average person can easily sign his own name in the physical documents. Digital signature provides a platform for the e-business. Thus, the government and all parties concerned shall ensure the mechanism to be secured and safe.

The legislative body need to look into those issues highlighted above to safeguard the interests of parties transacted in the Internet (e-business). The Act shall extend its application to transactions by any person (whether Malaysian or non-Malaysian) within Malaysia, at least to be consistent with section 9(1) of the Computer Crimes Act 1997, the other cyberlaw legislation. It would be an ideal to have all nations to discuss over and adopt the best practices universally.

Instead of having various statutes governing various aspects of the e-business transactions, it is suggested that one comprehensive statute similar to the Singapore Electronic Transaction Act 1998 should be enacted. Hence, it will govern all aspects of electronic contracts such as formation of contract generally and particularly the evidential proof of identity of contracting parties.

There should also be inserted a clear provision on the renewal of the digital certificate so that a new digital key will be issued to the existing subscribers. By having a new key from time to time, this may prevent the chances of tampering activities. Hence, this again will safeguard one aspect of the security issues. The provision on the duty imposed on the subscriber (i.e. reasonable care) to hold and control his own private key should be amended so that a higher responsibility is imposed on the subscriber to ensure his own private key to be kept intact and safe. This will remind the subscriber to be more tactful in handling his own private key and to avoid unnecessary deception incidents.

The qualification of a licensed certification authority is not satisfactory ("trustworthy person"). Thus we suggest that a much clearer guideline for qualified certification authority be laid down. Alternatively, the

Federal Government shall take up the role as the licensed certification authority in parallel with the verification of citizens' births and deaths record. This is to reduce the possibility of misuse of the data/message/information by private certification authority and to minimise the threat to national security since database is an important commodity in the current world. With the national security at stake, the Federal Government is in the better position to act as reliable centralised repository for identification purposes for any cyber world transactions.

The Act should be revised from time to time to ensure the legal equivalence among various new technological approaches. This is to ensure that the Act is not soon outdated and that the Act may survive technological changes. In other words, this will encourage the continuous improvement of the digital signature technology to curb those issues concern on digital documents transmitted over any electronic networks. To quote the saying by Lex Luthor in the movie "Superman Returns", "the one who controls the technology controls the world."

Awareness campaigns through public speeches, seminars, conferences are also needed to promote the public confidence on the usage of digital signature. With the knowledge on this technology, more feedback can be collected from the public as a source to improve the technology based on public's demand. By considering the public's input and feedbacks, the technology can be tailored according to the user's preference. Hence, it will promote the public confidence and ease the usage of this technology.

ACKNOWLEDGEMENT

Along the process of writing, the writers have visited a Malaysian Communications and Multimedia Commission and MSC Trustgate.Com and conducted interviews with their officers. The writers would like to extend their gratitude particularly to Miss Noraifizah Zainal Abidin, Product & Project Manager, MSC Trusgate.Com Sdn. Bhd. and Mr. Muhammad Razali Anuar, from Policy & Regulatory Initiatives & Development Department and Industry Development Division, Malaysian Communications and Multimedia Commission for being generous to share their knowledge on the application of digital signature.

REFERENCES

Book

Abu Bakar Munir, 1999. *Cyber Law Policies and Challenges.* Butterworths Asia, Kuala Lumpur.

Alan M. Gahtan, et al 1998. *Internet Law: A Practical Guide for Legal and Business Professionals.* Carswell, United Kingdom.

Chris Reed, 2004. *Internet Law Text and Materials* Second Edition. Cambridge University Press, London.

Claire Wright, et al, 2003. *Internet Law in Hong Kong.* Sweet & Maxwell Asia, Hong Kong.

Committee on Intellectual Property Rights and the Emerging Information Infrastructure, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, 2000. *The Digital Dilemma – Intellectual Property In the Information Age*. National Academy Press, Washington, D.C.

Davis W. and Benamati J., 2003. *E-Commerce Basics: Technology Foundations and E-Business Applications*. Pearson Education, USA.

Hammond Suddards Edge, Daniel Tunkel & Stephen York (ed), 2000. *E-Commerce: A Guide to the Law of Electronic Business* 2nd Edition. Butterworths, London.

Julian Ding, 1999. *E-commerce Law & Practice.* Sweet & Maxwell Asia, Kuala Lumpur.

Laudon K. C. and Laudon J. P., 2006. *Management Information Systems: Managing The Digital Firm.* Pearson Education, New Jersey, USA.

Lilian Edwards and Charlotte Waelde, 2002. *Law and the Internet – a Framework for Electronic Commerce* 2nd Edition. Hart Publishing, Oxford.

Pfitzmann B., 1996. *Digital Signature Schemes: General Framework and Fail-Stop Signatures*. Springer-Verlag, Berlin, Heidelberg, New York.

Whelan J. and Maxelon K., 2001. *E-Business Matters: A guide for Small and Medium-sized Enterprises*, Pearson Education, Great Britain.

Zaid Hamzah, 2005. *E-Security Law & Strategy*, LexisNexis Malayan Law Journal, Singapore.

Conference paper or contributed volume

Jorah Ramlan & Associate Professor Dr Leo D Pointon, 1998 Economic Implications of Malaysia's Digital Signature Act 1997. *Proceedings of the 1st Asia-Pacific Conference on Cyberlaw*, Putrajaya, Malaysia, pp 133-139.

Zinatul A. Zainol, 2000. Electronic Commerce: A Comparative Analysis of the Malaysia Digital Signature Act 1997 and the Singapore Electronic Transactions Act 1998. 15th BILETA Conference: "*Electronic Datasets and Access to Legal Information*" on 14 April 2000, University of Warwick, Coventry, England.

Statute

Banking and Financial Institutions Act 1989 (Act 372)

Computer Crimes Act 1997 (Act 563)

Contracts Act 1950 (Revised 1974) (Act 136)

Digital Signature Act 1997 (Act 562)

Digital Signature Regulations 1998 (PU(A) 259/1998)

Evidence Act 1950 (Act 56)

Interpretation Acts of 1948 and 1967 (Consolidated and Revised 1989) (Act 388)

Malaysian Communications and Multimedia Commission Act 1998 (Act 589)

Payment Systems Act 2003 (Act 627)

Telemedicine Act 1997 (Act 564)