

Educating Businesses about Digital Signatures

AASHISH SRIVASTAVA

Aashish.Srivastava@buseco.monash.edu.au

*Department of Business Law and Taxation, Monash University,
Victoria, Australia*

Abstract

In the last two decades the Internet has not only proved itself as an efficient means of communication but also a suitable medium for businesses to conduct commercial activities. However, one area in which businesses are reluctant to use the Internet is 'electronic signatures' (ESs), including digital signatures (DSs), for entering into online contracts and agreements. So far, the business community has considered the pen to be mightier than the ESs/DSs.

This paper undertakes the role of trying to explain to businesses the advantage of using DSs and will use the Australian context as an exemplar. In doing so, it focuses on three things. First, it provides a brief overview about DSs. Second, it explains, with the aid of diagrams, the process of receiving and using DSs. Finally, the paper concludes with suggestions and recommendations as to how businesses should further educate themselves about DSs.

Key words: electronic signatures, digital signatures, Gatekeeper, business education

Introduction

In today's world businesses spend ample amount of money and time when entering into contracts with other businesses. Money is spent not only on printing and copying but also for record keeping of such contracts in the form of buying filing cabinets and hiring storage space. Extra costs as well as time are involved where the signatories to a contract are located in two different cities or countries as such contracts are either required to be mailed back and forth for signatures or representatives have to make a trip so as to meet their counterpart face to face for signing the contract. These costs and loss of time can be easily saved by businesses if they replace present day paper based contracts with electronic contracts via the Internet.

However, businesses so far have failed to use the Internet for entering into online contracts. This failure exists even though most countries have legislation that validates the use of various types of technologies for signing electronic documents. Such types of technologies are generically known as 'electronic signatures' (ESs) and digital signatures (DSs) being an important subset of ESs. So far, the business community has considered the pen to be mightier than the ESs/DSs. Why is it so?

For any product to be accepted by consumers, it must be consumer friendly. A recent study shows that 44% people delay purchasing home computers and 34% delay acquiring Internet services because of the failure to fully comprehend the technology that is necessary for their use (Metafacts, 2003). Perhaps, the same reason applies to the lack of acceptance of ESs/DSs by the business community. This is substantiated by the fact that there are reports that suggest that people are unaware of the functionality of the DS technology (Tuesday, 2002). They incorrectly confuse it with some other form of technology.

With this logic in mind this paper undertakes the role of educating businesses about DSs and will use the Australian context as an exemplar. Also this paper, unlike previous literature in this area, is not merely focussing on the technical or legal aspect of DSs but attempts to explain DSs from a user's point of view. Thus, the paper will provide: a brief overview about DSs; the key terms associated with DSs; the various types of DSs available (Australian context); the

process involved in applying and receiving DS Certificates; the implementation of DSs with the help of a hypothetical example and; finally, suggestions and recommendations to the business community for the use of DSs.

Brief overview: ESs/DSs

ES is defined as “data in electronic form, affixed to or logically associated with, a data message,¹ which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message” (Model Law on Electronic Signatures, 2001). Examples of ESs include, but are not limited to, a password, a typed name at the end of an e-mail, a personal identification number (PIN), I-Agree buttons, biometric indicators and DSs. However, amongst all the various types of ES’s, DS is the most widely referred to.

DS is often confused for ES (Shark Tank, 2003) although as shown above ES is a technology neutral term in the sense that it refers to any technology that is able to satisfy the legislative requirements; whereas, DS uses a specific type of technology. DSs are formed and verified by using cryptography, the branch of applied mathematics that concerns itself with transforming message into seemingly incomprehensible form and back again into the original and easily recognisable form (Electronic Frontiers Australia, 2001).

In order to provide legal certainty and promote user confidence in the use of ESs, most countries and organisations throughout the world have drafted an ES legislation. Australia was one of the first few countries to draft an ES legislation, known as the *Electronic Transactions Act (ETA) 1999* that validates the use of ESs. Apart from drafting the *ETA 1999* the Commonwealth Government also attempted to promote the use of ESs, especially DSs through its *Gatekeeper*² project launched in May 1998 (Boyle, 2000).

¹ *UNCITRAL Model Law on Electronic Signatures 2001s 2(c)* defines data message as ‘... information generated, sent, received or stored by electronic, optical or similar means including, but not limited to electronic data interchange (EDI), electronic mail, telegram, telex or telecopy; and acts either on its own behalf or on behalf of the person it represents’.

² ‘*Gatekeeper* is a rigorous accreditation scheme for organizations and service providers willing to issue and maintain DSCs in Australia.’ See www.agimo.gov.au. Also note *Gatekeeper* has not been established by

Despite the fact that there is availability of ES/DS technologies and legislation to support their usage the business community in Australia has failed to accept the technology of ESs, including the project *Gatekeeper* accredited DSs.³

Terms associated with DSs

As with any form of technology the terminology is often specific to that technology. To gain a deeper understanding an adequate description of those terms is required.

(a) Hash Function

The ‘hash function’ is a process whereby the data message is passed through an algorithm, which can be considered as a formula or a series of mathematical steps to achieve a particular task. The result of the application of hash function to the data message results in a number which is substantially smaller than the data message and is called a ‘message digest’ or ‘hash value’ or the digital fingerprint of the data message. The process of hash function can be considered similar to the process of creating yoghurt from milk. Milk (data message) can be converted through the use of bacteria (algorithm) into yoghurt (message digest). However, as with the hash function the reverse process (i.e. creating milk from yoghurt) is not possible. It is imperative to note that two identical data messages if passed through the same algorithm will give the same hash value. However, if one data message is even changed by a single letter the hash value will change.

(b)Key

‘Key’ in cryptography is a variable value that is applied using an algorithm to the unencrypted text to produce an encrypted text, or to decrypt an encrypted text. The length of the key is measured in bits and is a factor in considering how difficult it will be to decrypt the text in a given message. The length of the key can be considered similar to the number of lever

Commonwealth legislation but by a head agreement between the National Office for the Information Economy (NOIE). NOIE has been replaced by Australian Government Information Management Office (AGIMO) in early 2004.

³ The only area in which ESs have received some success is the Australian Taxation Office-Digital Certificate (ATO-DC) and *Integrated Cargo System* DSs of the Australian Customs Service. In both the cases the usage of such ESs has been made mandatory by the respective bodies.

in a padlock. The higher the lever (bits) a lock (algorithm) has the greater the strength of that lock.

(c) Symmetric-key Cryptography

'Symmetric-key cryptography' is a process whereby a single key is shared between the sender and the recipient. The key is not known to the third person. The sender encrypts the data message to be sent to the recipient through a key and the recipient decrypts the data message through the same shared key. It works like a lock with two duplicate keys, one with the sender and other with the recipient.

(d) Asymmetric-key Cryptography

In 'asymmetric-key cryptography' there are two keys; a private key and a public key. The private key and the public key are unique to the user and work together as a functioning key pair. The private key can be considered as an electronically generated random number which is secret to the user just like a password or PIN, whereas the public key is known to the public and can be found on a web server following a similar process to finding a person's name in a telephone directory but in an online world. It is important to note that unlike symmetric-key cryptography the keys are not duplicates but correspond to each other. A data message encrypted with a private key can only be decrypted by the corresponding public key and vice versa.

(e) Certification Authority (CA)

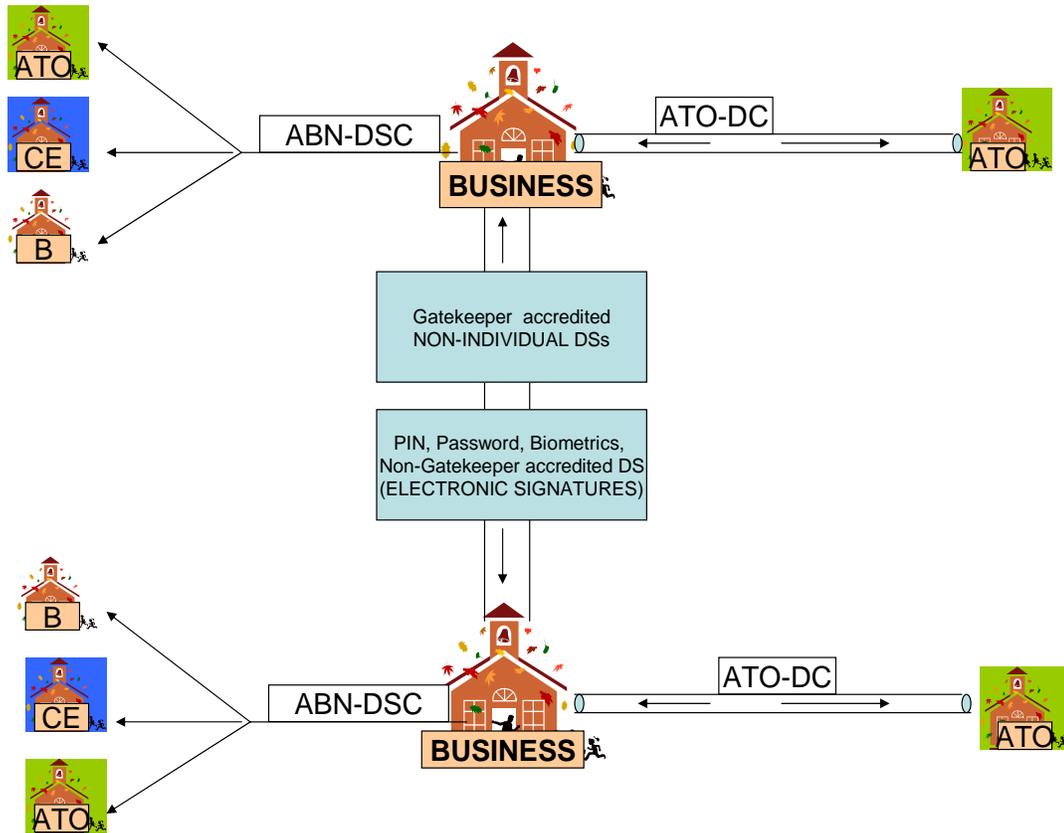
Just as in the physical world, the identity of an individual is established through the issuance of passports, identity cards, credit cards etc., the identity of an individual in cyberspace is established through digital certificates issued by a 'certification authority' (CA), also known as the 'trusted third party'. It is the CA that links the public and private key pair to an individual. This association is confirmed in a certificate known as DS Certificate (DSC). DSC is nothing but an electronic file containing all necessary information to identify the creator of a DS, which is carried out by a registration authority (RA). It is the RA's office that performs the necessary checks and formalities required for the issuance of a DSC. Once the RA has completed these checks and formalities, its outcome is reported to the corresponding CA.

Types of DSCs for businesses in Australia

There are three types of *Gatekeeper* accredited DSCs available to businesses in Australia: ATO-DC, non-individual DSCs, and Australian Business Number (ABN)-DSCs (Lim, 2001). The ATO-DC is a DSC that can be used by a business for dealing electronically with the ATO and cannot be used for online transactions with other Commonwealth entities or businesses. The non-individual DSCs are issued to businesses and organisations and can be used by them to enter into legally enforceable transactions with each other. The ABN-DSC is a DSC that can be used to deal electronically with the Commonwealth and state entities as well as for entering into legally enforceable online transactions with other businesses (Drugs and Crime Prevention Committee, 2004). However under the *ETA 1999* businesses are free to use other forms of ESs (such as PIN/password/biometrics) when dealing with each other, including DSs issued by CAs that do not have *Gatekeeper* accreditation.⁴ The following diagram 1 demonstrates the whole process.

⁴ Apart from this; the Australian government is also coming up with a government to business e-Authentication framework. See “ New Australian Business to Government e-Authentication Framework” <www.agimo.gov.au/media/2005/03/40779.html> accessed 5 June 2005

Diagram 1: Types of ESs that businesses can use when dealing with ATO, Commonwealth Entity (CE) or another business (B)



Issuing DSCs to businesses

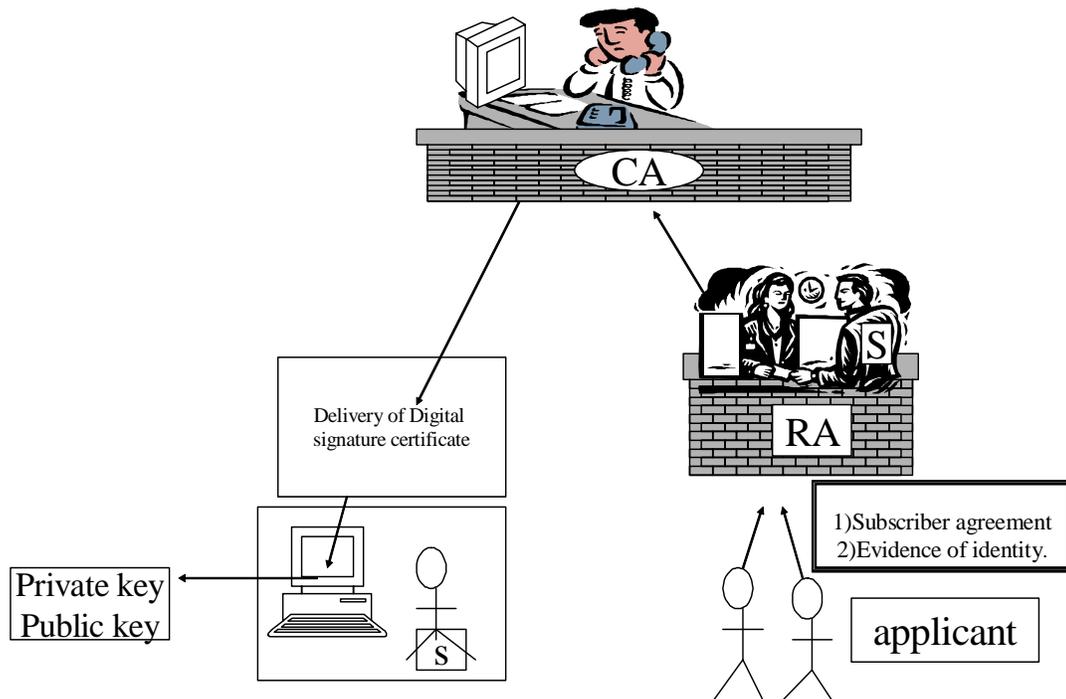
A business in Australia can either apply for a non-individual DSC or an ABN-DSC (if they have an ABN) from a *Gatekeeper* accredited CA.⁵ To apply for accredited ‘non-individual’ or an ABN-DSC a business will have to first submit an online application form by visiting the *Gatekeeper* accredited CA website. The applicant (authorised officer for an ABN-DSC) will then have to personally appear at the RA’s office and undergo a ‘personal identification check’ and will also have to satisfy the ‘organisation identification’ check. The applicant/authorised officer will then be required to sign a subscriber’s agreement and pay the requisite fees. Once these formalities have been complied with, the RA after verification of the

⁵ Apart from this a Device Certificate can also be received by businesses. However, such a DSC will only be issued by a CA when a business has obtained an ABN-DSC.

requisite documents will inform the CA. The CA will then send an email to the applicant informing him as to how the DSC and the key pairs (private and public key) are to be imported from the CAs website and installed on a computer.

The applicant (now a subscriber) will import the DSC and generate the key pairs in accordance with the instructions provided by the CA. The private key generated and installed by the subscriber is held in secret by the user and no one, not even the subscriber's CA knows what the subscriber's private key is. However, the public key, as mentioned before, is publicly available at a designated web server of the CA. The key pairs and DSC are then adequately installed on the hard disk of the computer or stored on portable devices such as smart cards or flash disks protected via a password or a pass phrase (see diagram 2).

Diagram 2: The process of applying, receiving DSC, and key pairs



Once the private key has been generated and stored by a subscriber, he/she will be able to send a data message that is signed through his/her DS, which is created through his/her private key. The following section describes this process through the help of a hypothetical example.

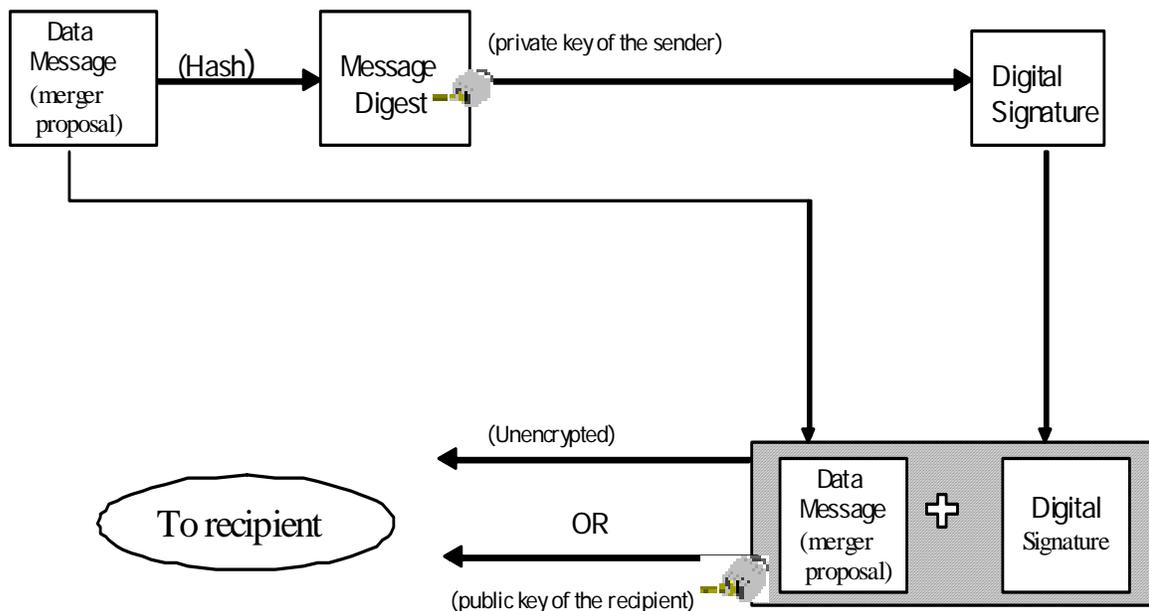
Implementation of the DS

Let us suppose 'A' is a CEO of a multinational company in Melbourne and needs to e-mail a merger proposal to 'C', a Managing Director of a company in Perth. 'A' wants the data message to not only contain his DS but also for it to remain confidential during its transmission from his computer in Melbourne to 'C's computer.

To sign the data message (merger proposal) through the use of DS and to secure the data message's confidentiality, four things will be required by 'A': 1) data message to be signed; 2) hash algorithm to create message digest; 3) private key of the sender and; 4) public key of the recipient. It is essential to mention here that only if the sender requires the data message to be confidential (encrypted transmission) then the public key of the recipient is needed.

'A' has the data message in the form of a merger proposal (an electronic file) and a hash algorithm in the form of software stored on his computer. 'A' also has his private key that he purchased for himself as a CEO (authorised officer) of the company from a *Gatekeeper* accredited CA and the public key of C from the web server. The following diagram 3, demonstrates how the implementation of a DS takes place.

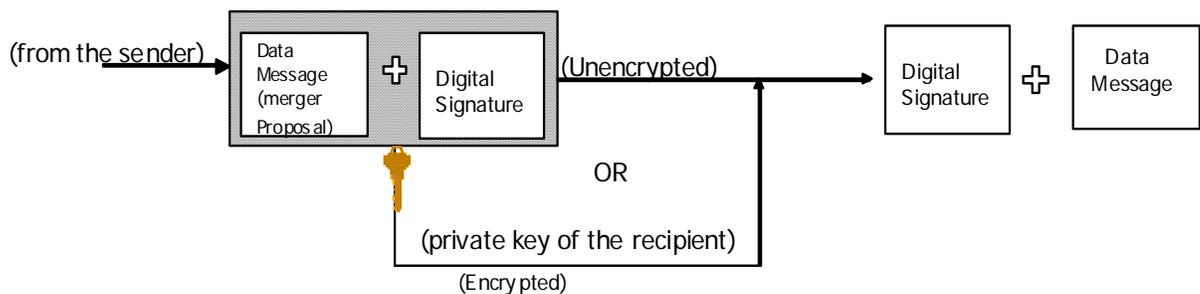
Diagram 3: The implementation of a DS



First, the data message i.e. the unencrypted merger proposal to be sent is passed or hashed through a hashing algorithm. The message digest (output) is then locked or encrypted through the private key of 'A' to obtain a DS.⁶ Once the DS is created, 'A' has two choices. Either 'A' can attach the DS to the data message and send it to the recipient C or 'A' may choose to send a confidential data message to the recipient 'C'.⁷ However, as mentioned before, 'A' has chosen that the data message should remain confidential during its transmission from Melbourne to Perth and that no one else except 'C' should be able to read it. In such a case the unencrypted data message together with DS is locked/encrypted through the recipient's, in this case 'C's public key and then send to the recipient 'C'.

Once the data message and DS reaches 'C's computer, 'C' can unlock or decrypt the data message and DS (if an encrypted version has been sent by 'A') through his/her private key. In this way 'C' can read the data message sent by 'A' and verify that the DS is of 'A' (see diagram 4).

Diagram 4:- The recipient verifies the identity of the sender and the content of the data message by using the private key



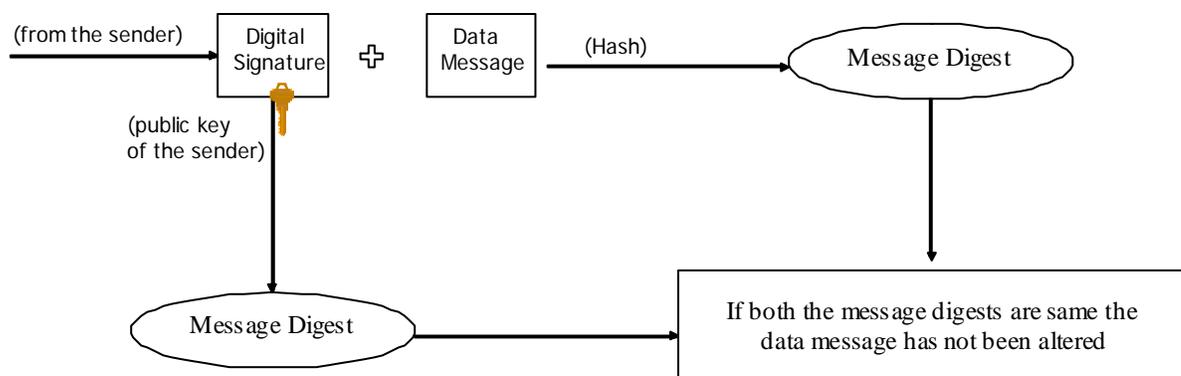
The use of DS is considered to be more secure than a manuscript signature because unlike a manuscript signature, the DS created for each data message is different; thus, ensuring authentication, integrity, and non-repudiation. DS performs the same legal functions in the

⁶ Please not that this is a reversible process. If the public key of 'A' is applied to DS it will generate the message digest.

⁷ Often the DSC is also attached to the data message so that it is easy for the recipient to know the identity and other details of the sender.

online world as a manuscript signature does in the physical world. They are: authentication,⁸ integrity,⁹ and non-repudiation¹⁰. ‘Authentication’ is achieved as DS of the sender is attached to the data message. The recipient can be assured that the data message has come from the sender and no one else, as the private key used to generate the DS is known only to the sender. The ‘integrity’ of the data message can be checked by the recipient without contacting the sender i.e. the sender can make sure that the data message has not been altered after its despatch from sender’s computer. The procedure described in the following diagram 5, explains this point.

Diagram 5: Recipient checking integrity of the data message without contacting sender



First, the recipient performs the same task as the sender did with the data message i.e. he /she passes the data message through the same hashing algorithm as applied by the sender. The product obtained is the same message digest as was generated by the sender. Secondly, to the DS of the sender the recipient applies the public key of the sender. The product generated is another message digest. Both the message digests are then compared and if they are same the recipient can be sure that the message has not been altered during its transmission from sender’s computer to his/her computer.

The process or cryptography used in signing electronic documents through DSs also ensures ‘non-repudiation’. As the private key is secret to the user and the process involved in

⁸ Authentication is defined as “broadly the act of proving that something (as a document) is true or genuine...” (Garner, 1999).

⁹ The use of the DS to sign data messages ensures that the data message retains its entirety during the transmission from the sender’s computer to the recipient’s computer and any alteration is detected.

¹⁰ “Non-repudiation is a property achieved through cryptographic methods which prevents an individual or entity from denying having performed a particular action...” (McCullagh & Caelli, 2000).

signing through DS is highly secure it "...can be used to prove that some kind of event or action has taken place [and] ...that...event or action cannot be repudiated later"(Herda, 1995).

Conclusion and suggestions

As shown above, DSs through the function of authentication, integrity and non-repudiation can be a reliable alternative to manuscript signature in the online environment. *Gatekeeper* accredited DSs can be used by Australian businesses as a secure and efficient way of entering into online transactions with other businesses. It is recommended that businesses should choose ABN-DSC¹¹ as compared to other forms of DSC because it can serve as a multipurpose DSC. ABN-DSC can be used by businesses not only for entering into online transactions with other businesses but also when dealing with Commonwealth or state entities for submitting requisite documents electronically rather than sending their staff to the government office for such submission or faxing such documents.

Australian businesses can also use their DSs for entering into contracts and agreements with businesses outside Australia.¹² For example, a business in Brisbane through the use of its *Gatekeeper* accredited DSs can enter into an electronic contract with its business partner in Shanghai as China's recently passed ESs legislation gives higher legal status to DSs issued by accredited CAs such as *Gatekeeper* compared to other forms of ESs. (Srivastava, 2005).

Thus, it can be seen that DSs can be used by businesses not only within Australia but also outside Australia thereby saving them substantial cost and loss of time compared to present day paper based contracts.

Suggestions for further education

Businesses, however, in order to use DSs need to further educate themselves with the law, technology and other provisions associated with the use of DSs. Businesses need to

¹¹ For those businesses that have an ABN.

¹² The Asia PKI forum, to which Australia is a member, is one such effort where DSs issued by a CA of a member country will be accepted by another member country and vice versa (Ong, 2003).

familiarise themselves with all the relevant legal provisions associated with the use of DSs. For example the *ETA 1999* states that for the usage of ES/DS the recipient must agree to its usage. Thus, a business willing to use DS must receive the recipient's consent beforehand. These and other legal provisions in the *ETA 1999* must be looked into by businesses prior to using DSs.

Businesses should also enquire about the CA from which they are going to purchase DSC as to how trustworthy system and procedures it employs in issuing DSCs. Information such as: rights, liability and obligations of the subscriber; physical, procedural and personal security controls; technical security controls and; governing law and jurisdiction in case of a dispute are available in the *Certificate Policy* of the CA. Businesses should make sure to read the CA's *Certificate Policy* before applying for a DSC.

Apart from the above mentioned information necessities there are other information requirements in regard to DSs that businesses need to be familiar with such as: the formalities that businesses need to comply with for 'personal identification check' and 'organisation identification check'; the price of the DSC; and the duration for which DSC will be valid. All this information is available on the website of the CA and businesses should familiarise themselves with these issues before applying for a DSC.

It is recommended that businesses should especially take care of two issues with regard to DSs. First, they should ensure that the recipient's CA follows a rigorous procedure for 'personal identification check' and 'organisation identification check'. The reason for this is that there is a growing amount of identity theft these days (Crawshaw, 2005; Barker, 2002; Federal Trade Commission, 2003; Hewitt, 2003) and it is possible that a person can get a DS from a CA by satisfying the EOI points through the use of fake and fabricated documents.

Second, businesses should make sure that the private key used for the creation of a DS is kept in a secure location. If the private key is stored on the hard disk of the office computer, it must be secured not only through an adequate password but also there should be some kind of physical security for that hard disk. For example, the computer's hard disk, containing the private key should be kept behind locked doors with access only to those persons who are

authorised by the company to use the DS. Such protections will prevent unauthorised employees from using the company's DS.

It is strongly recommended that businesses should refrain from storing their private key on the hard disk of the computer. This is because most of the computers, especially those in offices, are connected to the Internet or an Intranet and hence are prone to online/external attacks (Srivastava, 2005). It is recommended that an organisation stores their key pairs and DSC on portable information storage devices (PISD) such as a smart card or a flash disk secured through a PIN or a password, as storage on such devices solves the problem of online attacks.¹³ The other advantage of storing the key pairs and DSC on a PISD is that it gives the convenience of signing through one's DSs from any computer terminal located anywhere in the world.

Businesses should also make sure that they use a corded and not a wireless key board for using their DSs because of the security issue. The usage of wireless keyboard may result in the keystrokes of the user of DS transmitted to another staff's computer in the same office or to somebody else's computer several metres away (Brandt, 2003).

It is said that "[t]he highest form of ignorance is when you reject something you don't know anything about" (Dyer, 1940). This article was a brief attempt to remove *this highest form of ignorance* amongst the business community. However, businesses need to further educate themselves in the manner suggested above in order to use DSs. Once educated businesses can replace their paper based contracts with electronic contracts thereby saving themselves fair amount of money and ample amount of time.

¹³ Key pairs and DSCs can be exported from the hard disk of the computer to PISDs.

References

- Barker, G. (2002). Stolen identity: the hidden cost. *The Age*. (Melbourne). 13 July 2002.
- Boyle, K. (2000). An Introduction to Gatekeeper: The Government's Public Key Infrastructure. *Journal of Law and Information Science*, Vol 11(1), 39-54.
- Brandt, A. (2003). Privacy watch: Wireless Keyboards that blab. *PCWorld*. Retrieved June 20, 2005 from <http://www.pcworld.com/howto/article/0,aid,108712,00.asp>.
- Crawshaw, David. (2005). Theft Fears rule out national card. *Australian IT*. 29 June 2005. Retrieved on 4 July 2005 from <http://australianit.news.com.au/articles/0,7204,15767261%5E15319%5E%5Enbv%5E15306,00.html>
- Drugs and Crime Prevention Committee, Parliament of Victoria. (2004). *Inquiry into Fraud and Electronic Commerce: Final Report*. Retrieved June 10, 2005 http://www.parliament.vic.gov.au/dcpc/Reports/DCPC_FraudElectronicCommerce_05-01-2004.pdf.
- Dyer, W. (1940). *Famous Quotes about Ignorance*. Retrieved June 20, 2005 from http://www.borntomotivate.com/FamousQuote_Ignorance.html.
- Electronic Frontiers. (2001). *Introduction to cryptography*. Retrieved June 20, 2005 from <http://www.efa.org.au/Issues/Crypto/crypto1.html>.
- Electronic Transactions Act 1999*
- Federal Trade Commission. (2003). Identity Theft Survey Report, 2003.
- Garner A Bryan, (1999). *Black's Law Dictionary* (7th ed). West Group
- Herda, S. (1995). Non-repudiation: constituting evidence and proof in digital cooperation. *Computer Standards and Interfaces*, Vol. 17, No. 1, 69-79.
- Hewitt, S. (2003). New fraud laws plan: Bid to protect identities, *Sunday Herald Sun* (Melbourne), 13 July 2003.
- Lim, L. (2001). Digital Signatures for Australian Business 3(8). *Internet Law Bulletin* 105.
- McCullagh, A. and Caelli, W. (2000). *Non-repudiation in the Digital Environment* 5(8) First Monday. Retrieved 13 March 2005 from http://firstmonday.org/issues/issue5_8/mccullagh/index.html.

- Metafacts Inc. (2003). *Roadblocks on the Information Highway: Barriers to adoption of technology products*. Retrieved June 5, 2005, from http://www.amd.com/us-en/assets/content_type/DownloadableAssets/Summary_Report_6_18_2003.pdf.
- Ong, E. (2003). *Launch of final report on legal issues in cross-border e-commerce transactions*. Asia PKI Forum International Symposium, Retrieved June 14, 2005 from <http://symposium.pki.or.kr/02program.html>.
- Shark Tank. (2003). Not exactly what the doctor ordered. *Computerworld*. Retrieved May 15 2005 from <http://www.computerworld.com/departments/opinions/sharktank/0,4885,77957,00.html>.
- Srivastava, A. (2005). Is Internet security a major issue with respect to the slow acceptance rate of Digital Signatures? *Computer Law & Security Report*, Vol 21, 392-404.
- Srivastava, A. (2005) An analysis of the Electronic Signatures Law of China, *International Journal of Law and Information Technology*. Forthcoming article in 2005.
- Tuesday, V. (2002). User Indifference thwarts electronic signature effort. *Computerworld*. Retrieved May 15 2005 from <http://www.computerworld.com/securitytopics/security/story/0,10801,67303,00.html>.
- United Nations (2001) *United Nations Commission on International Trade Law: Model law on Electronic Signatures*. Retrieved 8 June 2005 from http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html.