Digital Signatures and Liability Issues Arising Out of Their Certification

By:
Ahmad A. Al-Ghadyan
Assistant Professor, Department of Law,
College of Administrative Sciences,
King Saud University,
Riyadh, Saudi Arabia.

Abstract:

The Internet is an insecure means of communication in which to conduct business. The introduction of digital signature technology is a way of achieving security and hence, creating a secure environment in which trading could be transacted electronically.

Digital signature is a very good means of authenticity for two people who do not know each other to have dealings together. However, it is necessary to introduce a third trusted person into the digital signature operation in order to identify the two parties to each other. This third party is a Certification Authority, who issues certificates which identify the signer and give the public key to verify the signature.

Playing this role the Certification Authority encounters an extremely large liability risk arising out of the issuance of inaccurate certificates. The aim of this study is to define the nature of this liability and examine the extent of which such liability can be limited by the general principles of torts or by contractual limitation of liability or even by the enactment of legislation.

Introduction

The use of the Internet (the world wide web) in commerce is expected to increase in volume rapidly in the coming years,[1] in the wake

(1) Consumer online sales were estimated at over $7 billion in 1998 and is expected to reach $12-$18 billion in 1999. See A Report on Protecting Consumers Online, The Federal Trade Commission Staff, Dec 1999 available online at HYPERLINK "http://www.ftc.gov" www.ftc.gov at p.2-3.

of the introduction of new technology that will make authentication of computer based information possible. Describing the situation a commentator stated "the seal was replaced by the handwritten signature. With the dawn of the digital age the days of the handwritten signature are now also numbered."[2]

Although statistics indicate that fraud occurs in ordinary commercial transactions far more than it does in transactions conducted using the Internet,[3] this is not attributable to the high aspects of security on the Internet but rather mainly to the low level of use of the Internet in commercial transactions.[4] The rapid increase of use of the Internet in commercial transactions will definitely increase the fraud cases in electronic commerce. Although it is impossible at this time to obscure all the information related to the Internet account[5] the fraud may happen in many ways, such as, using an Internet account which does not belong to the communicator, either it was obtained under a false name or by hacking someone else's account or the message was sent, but before it reached its destination it was stopped and changed.

Electronic signature was introduced as a means of authentication to enhance confidence among parties using this method of communication to conclude their commercial transaction.[6]

This article will describe in part one the digital signature mechanism and it will deal in part two with the certification authorities liabilities

(2) Hindelang, S. No Remedy for Disappointed Trust-The Liability Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in England and Germany Compared, The Journal of Information, Law and Technology. J.I.L.T. 2002(1) at p.1.

(3) The Internet is an insecure environment. See Gulshan, Rai, Dubash R.K. and Chakravarti, A.K. Digital Signature Law - A Survey of the International Scenario, Oct. 1997. Information Technology Group Dept. of Electronics Govt. of India at p.4.

(4) See Marion. Larry, Who's Guarding the Till at the CyberMall? Datamation, Feb. 15 1995, at pp.38- 41.

(5) Information about the Internet address and page that is used can be obtained from the Internet. However, anonymous web proxies might be used to obscure such information. See Anonymizer FAQ, URL. http://anonymizer.cs.cmu.edu:8080/faq.html.

(6) The information communicated through the Internet is not written on papers, it is rather stored as 'bits' which can be duplicated millions of times at an insignificant cost and can be sent at very high speeds.

arising as a result of the use of Digital Signatures in electronic commerce. The discussion will mainly deal with the UNCITRAL Model Law[7] (which is the model that has an important influence on the digital signature laws in the countries of the Arab world) with reference to the EU Directives[8] and the Electronic Signature in Global and National Commerce Act,[9] and the Electronic Signature Legislation.[10] As regards to the general principles of the law, the discussion is mainly concerned with English Law and with reference to United States Law.

(7) United Nations Commission on International Trade Law (UNCITRAL), Thirty-fourth Session, Vienna, 25 June - 13 July 2001. Model Law on Electronic Signatures (hereinafter cited as UNCITRAL Model Law). On the shortage of Acts in the Arab world regarding cyberspace law see Al-Hafanawi, F. The Law of Computer Programs, (2001, Dar AlKitab, AlHadith, Cairo). At pp.38-9.

(8) Enacted by the European Union Parliament in December 1999 (Hereinafter cited as the EU Directive).

(9) Enacted by Congress in 2000 (Hereinafter cited as E-Sign).

(10) Came into force in the UK on the 8th March 2002 (hereinafter cited as Electronic Signature Legislation)

Part One
Digital Signature Mechanism

This part will discuss the digital signature operation and will then deal with the certification authority and certificates and lastly will explain the importance of digital time stamps.

1.1. Digital Signatures[11]

A digital signature[12] is defined from a legal point of view by the UNCITRAL Model Law on Electronic Signatures[13] as being;

"... data in electronic form in, affixed to or logically associated with, data message, 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..."

This operation simply started by writing the message[14] and then applying the digital signature to it by running it through a computer encryption program that requires the writers private key to generate a digital signature. The program applies a mathematical procedure that transforms the message into unintelligible form[15] and combines this

(11) The introduction of this technology will open an entirely new environment in which governments and the private sector will conduct their business.

(12) There are some types of digital signatures which are using an electronic code, symbol or character made by an electronic method and used with the intention of authenticating a message. However the digital signature described in this paper is that based on public-key cryptography. The E-Sign sec.106(5) in the USA defined the digital signature broadly to include any electronic form that is applied by a person with the intention to bind himself by the contract such as pressing the button "I Agree". So the E-Sign gives more freedom to contract than the UNCITRAL Model Law. See Brightbill, T. & Dylang, S. Barriers to International Electronic Commerce: Recent Issues and Developments, 2002, at p.4. This Article is based on "Overcoming Barriers to Global Economic Commerce" A paper presented in conjunction with a seminar at the ABA Annual Meeting in Chicago on Aug 6 2001.

(13) Article 2 Definitions. (a).

(14) Message was defined by the UNCITRAL Model Law Article 2(c) as being "...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.

(15) Electronic Commerce, Building the Legal Framework; Report of the Electronic Commerce Expert Group to the Attorney General, 31 March 1998 at p.66. Digital Signature technology is not secret and any specialist can obtain such information from algorithms textbooks and can =

result (known as the message digest or hash)[16] with the writer's digital signature.[17]

The person to whom the message was sent will run the message through a compatible computer program using the public key which corresponds with the senders private key, this will identify the writer and will certify that the message was not changed after it was signed, if it was changed the ''hash'' result will not be the same and the computer program will declare the signature as being invalid.[18]

Although the formal legal requirements for a signature vary from one legal system to another[19] they all unify in that the signature firstly, should identify the signer [i.e. can be attributed to him]. Secondly, the signers knowledge of the legal significance of his act. Thirdly, the

---

= program a computer to do such encryption. However, understanding such technology is not as important here as understanding the potential benefits that can be gained out of its use. See Digital Signature Law - A Survey of the International Scenario op.cit. at p.4. For an historical background of Cryptography see Cohen. F. A Short History of Cryptography (1995)available online HYPERLINK "http://www.all.net" www.all.net. See also W.T.V. Digital & Electronic Signatures Cryptography, (6-12-97). Encryption offers the highest form of security [where messages cannot be read unless decrypted by the senders public key]. However many governments believe that it is a threat to national security, i.e. it makes it difficult to detect organized crime such as terrorism, espionage, and money laundering. See Katz, Paul R. Electronic Documents and Digital Signatures: Changing the Way Business Is Conducted and Contracts Are Formed, E-Commerce Law Report, March 1999 at Note 30. It should be noted that the message could be digitally signed and sent without being encrypted.

There is no need to write the full name for a signature to be valid under U.C.C.(Uniform Commercial Code) a signature can be ''stamped, written or printed and can be only initials or a thumbprint''. U.C.C., §1-201(39). In Spevak Cameron & Boyd v. National Community Bank of New Jersey. 677A.2d 1168 (App.Div. 1996) the court stated ''in the computer age the use of numbers as a means of identification has become pervasive.''

(16) Many legal systems in the last few decades has reduced the formalities required or reduced the effects of failure to satisfy them, however, people still ensure that such requirements are satisfied in order to guarantee enforceability and validity. See Braunstein, Michael. Remedy,Reason and the Statute of Frauds: A Critical Economic Analysis (1989) Utah.L.Rev.383, at pp.423-426.

(17) It is impossible to recreate the document from the hash value.

(18) On the reverse anyone could send an encrypted message to the sender using his public key and only the sender can decrypt the message using his own private key.

(19) The Common Law statute of frauds does not render a transaction to be invalid for lack of a signature of the party to be charged it only makes it unenforceable. See Corbin, A.L. Corbin on Contracts §279 at pp.20-23(1950).

approval of the content of the document and finally, that the document is final and irrevocable by the signer.(20)

The aim of a signature is firstly, to show who signed the document and that it is difficult for someone else without authorization to make such a signature,(21) or for the signer to deny his signature. On the other hand it shows the original signed document and makes it difficult to be altered after it has been signed by anyone else including the signer without being detected.(22)

This aim is fully satisfied by the digital signature technology as explained above and has been recognized and regulated by many legal systems.(23) The Model Law stated: "Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the

(20) Digital Signature Guidelines, Information Security Committee Electronic Commerce and Information Technology Division Section of Science and Technology American Bar Association (A.B.A.) (Aug.1996) cited hereinafter as A.B.A. Draft of Digital Signature Guidelines. See also Restatement (second) of contracts §110,§72 (1982). See for example the legal requirement for a signature in French and Egyptian Law, Jamaie, H. Proving Legal Actions Which Are Made Through the Internet (2000) Dar AlNadah Al-Arabia, Cairo.. at pp26-7.

(21) Hand signature can be forged but it is impossible to forge an encrypted digital signature, Katz, Paul R. Electronic Documents and Digital Signature: Changing the Way Business Is Conducted and Contracts Are Formed, op.cit.

(22) The authenticity produced by this method is as credible as a signature that is made by hand. See Baum. Michael, Information Technology and the Law. When an offer and acceptance is exchanged a contract is formed, digital signature function is only to make it easier to prove the contract.

(23) In United States, Utah was the first state to enact a legislation to regulate the commercial use of digital signatures, now about 26 states have passed legislation to that effect and another 10 states are in the process of doing so. Outside of the United States only Germany, Italy, Argentina, Russia, Singapore and Malaysia have enacted legislation related to electronic signature and there are other countries such as United Kingdom, France, South Korea, Denmark, Japan, Finland, Canada, Ireland which are in the process of enacting some regulation to that effect. See Survey of International Electronic and Digital Signature Initiatives (24-9-1999) available on "Internet Law and Policy Forum," Home Page; Johnson, James A. Enacted State Digital Signature Legislation (March 1997). See also Chang Su Han, Law and Digital Signatures in Cyberspace, Which Law Should Be Applied? (Dec. 1997) available on line http://wings.buffalo.edu/law/complaw.

purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement."[24]

1.2. Certification Authority

Certification authority was defined by the UNCITRAL Model Law as ["Certification service provider" means a person that issues certificates and may provide other services related to electronic signature.][25]

In digital signature operation there are two keys, the first is a private key[26] which the signer uses to encrypt the document using a computer program and which the signer keeps secret. The second key is the public key,[27] which is given to others to use for decrypting the document, i.e. to use through a compatible computer program to verify the authenticity of the digital signature and the integrity of the transmitted document.[28]

This process seems to provide an excellent level of security in electronic commerce. However, the question is how would the people dealing with the sender obtain his public key? If he sends it to them directly that would bring about the possibility that anyone could send it pretending to be him. Thus, people receiving the document have no reason to trust that the public key belongs to the sender because if the document sent could be incorrect so could the public key which is sent in the same manner. A Certification Authority (C.A.) concept was put forward as a solution to this problem. This is an independent entity who renders its services as a trusted third party by issuing digital certificates. So the receiver of the document instead of obtaining the public key directly from the sender will obtain it from this establishment.[29]

(24) Article 6(1) compliance with a requirement for a signature.

(25) Article 2 Definitions (e).

(26) See on private key generation and security Greenleaf, G. and Clarke, R. Privacy Implications of Digital Signatures (10-3-1997)at §2, available online at http://www.anu.edu.au/people/Roger.Clark/DV/DigSig.html.

(27) For background detail of public key cryptography, See Bradford Biddle, C. COMMENT: Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure 33 San Diego L.Rev. 1143 (1996).II(A).

(28) It is impossible to obtain any information about the private key by having knowledge of the public key.

(29) The Certification Authority depending on the agreement with the holder of the public key whether to make it available for anyone by publishing it on their internet site or demand the holder's prior consent for e-mailing the public key to whoever requests it.

However, this does not solve the problem it only shifts it from being between the sender and the receiver to being between the receiver and the certification authority because the problem now is how would the receiver ensure that the certification authority public key is correct. It has been suggested that the certification authority's public key should be certified by another certification authority.(30) But that does not, however, solve the problem either, it moves it from one level to another because then the second certifying authority needs a further authority to certify its public key and so on. The result would be that the more certification authorities in the hierarchy the more certificates the receiver would need to check, which is time consuming and could be costly. It is further suggested that the root certifying authority should be a government office which certifies the public keys of the certification authorities.(31) It can be also consolidated by publishing certification authorities public keys on a regular basis in the media.

1.3. Certificates

The UNCITRAL Model Law on Electronic Signatures defines a certificate to be:

"... a data message or other record confirming the link between a signatory and signature creation data..."(32)

The Model Law has also set out the information that should be included in the certificate. It stated:

[T] he certification service provider must...

(c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate:

(i) The identity of the certificate service provider;

(ii) That the signatory that is identified in the certificate had control of the signature data at the time when the certificate was issued;

(iii) That signature creation data were valid at or before the time when the certificate was issued;

(30) Ford, W. Advances in Public-Key Certificate Standards. SIG Security, Audit & Control Rev., July 1995 at pp. 9,10.

(31) See Utah Code Ann.§46-3-104, 46-3-201.

(32) Article 2(b), Definitions..

(d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise:

(i) The method used to identify the signatory;

(ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(iii) That the signature creation data are valid and have not been compromised;

(iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;

(v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1(b) of this Law;

(vi) Whether a timely revocation service is offered...''[33]

It is important to note that Section (d)(i) of the Article above imposed a duty on the certification authority to include in their certificates the extent of which this information is accurate, i.e. whether the certification authority has made an inquiry to ensure the accuracy of the information and what is the nature of this inquiry. However, the importance of such an inquiry to public was taken into account by some companies. For example VeriSign, issue different classes of certificates which correspond to the level of inquiry that was conducted to ensure the accuracy of the information included in the certificate. The first class certificate is the cheapest, this class of certificates does not provide an assurance of the identity of the subscriber. The second class is more expensive and offers a medium level of assurance regarding the identity of the subscriber. The third class is the most expensive and the certificate requires high levels of enquiry regarding the applicant so as to provide a high level of security in comparison with class (1) and (2).[34]

(33) Article 9. (1) Conduct of the certification service provider.

(34) VeriSign Trust Network Trust Certificate Policies, Version 1.1 Effective Date: June 11 2002, P.22 Section 1.34. Regarding these certificates see:
Class 1 URL HYPERLINK "http://www.verisign/pki/policies/vtn-cp/class1"
Class 2 URL HYPERLINK "http://www.verisign/pki/policies/vtn-cp/class2".
Class 3 URL HYPERLINK "http://www.verisign/pki/policies/vtn-cp/class3". There are two types of certificate in class 3, individual certificates and organizational certificates.

On the other hand, there is other important information that should be included in the certificate. Such as the certificate holders age, his resident address and his nationality etc.. This information has a considerable legal importance for example insuring the legal capacity of the other party before contracting with him or which legal jurisdiction governs the other party; since the internet address is not a reliable way of identifying the geographical location(35) of a person.

To give accurate information, certificate authorities have to make a thorough checking regarding millions of people, this is a heavy burden, which they have to bear. However, the burden will be heavier if they are under a legal duty to continue checking whether this information is still accurate. The risk resulting from this situation may be minimized by issuing dated certificates, stating its operational period that will not be renewed until its information has been checked by the certification authority. If within the operational period the certification authority discovered that the information given to it by an applicant initially was incorrect or he has lost control of his private key or for any other reason that leads the certification authority to believe that the certificate has become unreliable, the certification authority will revoke the certificate(36) and put it on the certificate revocation list (CRL) to warn others that these certificates are no longer reliable.

(35) The American Bar Association has put forward a suggestion to create an establishment which they called the Cyber Notary. Its role although similar to the role provided by the certification authority it does not certify only the identity of the writer of the document it also gives a higher standard of security as to the genuinity of the content of the document and the time in which it was created, therefore, playing the role of a lawyer that certifies witnessing an act or a formality such as power of attorney. See Barassi, Theodore Sedgwick. The Cyber Notary, A.B.A. Section of Science and Technology CyberNotary Committee at http://www.abanet.org/scitech/ec/cn/home.html. C.f. a transactional certificates which has been defined as "A certificate for specific transaction incorporating by reference one or more digital signatures" A.B.A. The Draft Digital Signature Guidelines §1.34.

(36) The certificate may also be temporarily suspended in situations for example where the certification authority is investigating whether to revoke the certificate or to keep it valid. See Utah Code Ann.§46-3-306, 46-3-307.

1.4. Digital Time Stamp

Digital time stamp[37] is a certificate issued by the certification authority that the document existed at an exact time and date.

This is very essential to determine whether the digital signature was made during the operational period of the certificate. It will also determine whether the document was signed after or before the revocation of the applicant's certificate or even the revocation of the certificate of the C.A. who issued the certificate.

After the writer has signed his document and obtained the "hash value" he sends it to the certification authority which will then date it and sign it and return it to the writer.[38]

As the certification authority adopts an automated method of time stamping "hash values" sent to it, it would be impossible for the certification authority to change the time and the date of a time stamp without changing all the time stamped "hash values" sent by others during that period.[39] Time stamps would be finalized and unchangeable by publishing a summary of the time stamped "hash values" on a weekly basis.[40]

(37) For more discussion on time-date stamping, See Merrill, Charles R. Time is of the Essence - Electronic documents will stand up in court if the who, what and when they represent are unassailable (March 15 2000) (C.I.O. Magazine) available online http://www.cio.com/archive/03/500-fine.html.

(38) It is impractical to rely for this matter on the personal computer time and date stated in the document since it is easy to change the computers internal clock, therefore, it is essential to use an independent entity to do such a service.

(39) Bayer, D. Improving the efficiency and Reliability of Digital Time-Stamping, in Sequences II, Methods in Communication, Security and Computer Science. 329 at pp.331-32. (1993)

(40) See Surety Technologies Home Page at URL http://www.surety.com.

Part Two
The Certificate Authority's Liability

This part will firstly deal with the liability of the certification authority, under the general principle of tort and contract, then will discuss the clauses that the certification authorities include in their contracts with the applicant to limit their liability, secondly, the discussion will focus on the effect of the legislation on such liability and finally the closed system will be examined to see whether it can be used to eliminate the difficulties arising out of the certification authority liability.

2.1. The Certification Authority Liability Under General Principles of Law

The more public confidence in the high standard of security offered by digital signature technology(41) increases, the more commercial transaction volumes will increase, both nationally and internationally.(42) It is important to examine the enormous liabilities that C.A. may be exposed to as a result of the inaccurate information given to public.

In order for the services provided to public to be of value the minimum duty which C.A. should be under, is to have a valid certificate themselves, which can be verified, to conduct an investigation about the information given by each certificate holder and accurately states this information in the certificate.

It is also under a continuing duty to ensure that this information stays accurate by updating the certificate revocation list (CRL).

The liability could arise out of many situations; firstly, a criminal could obtain a certificate in someone else's name and use it in dealing

(41) There is no absolute security however a good cryptographic program offers an acceptable level of security. See for details about cryptography, Schneider, B. Why Cryptography is Harder Than It Looks, (19-3-99) at p.2 available online http://www.counlerpane.com/publish.html.

(42) As Internet communication is global considering a unified code is an inevitable eventuality. The UNCITRAL Model Law is a step in that direction. There are also other international initiatives, such as the European Union Draft Directives and Organization for Economic Cooperation and Development, see Survey of International Electronic and Digital Signatures op.cit. at §VI.

with many third parties who will suffer loses out of relying on this erroneous certificate. Secondly, if the private key was stolen from the holder of the certificate by a criminal who made several transactions before the holder of the certificate realized that his private key had been stolen and revokes the certificate. Thirdly, the encryption technology used by the CA is weak which makes it easy for criminals to forge certificates. Fourthly, CA not updating the CRL properly, fifth, the CA's employee could be dishonest or unskilled which results in undermining the reliability of the C.A. certificates. Finally, it would be a disaster if the private key of the C.A. itself was stolen by criminals, who could commit fraud on a very wide scale. The liability arising out of such a situation, in addition to revoking and issuing new certificates to all certificate holders will be enormous.(43)

Whatever protection C.A. may take, certificates with inaccurate information will no doubt be issued and will be relied upon by third parties, the question is whether the certification authority is liable for the loss sustained by these third parties as a result of their reliance upon this inaccurate information.(44)

The possibility of establishing a contractual relationship between the C.A. and the third party which will allow them to define their liability will be examined later, however, first the general principles of tort as a possibility will be examined to define such liability.

2.1.1. CA Liability Under The General Principles of Tort

Applying the general principles of tort(45) in the United Kingdom certification authorities may be found liable for a breach of a duty of care. The principle is that, a duty of care may exist in situations outside

(43) For a comprehensive discussion of the situations where C.A.'s may be exposed to liability See Smedinghoff, Thomas J. Certification Authority Liability Analysis, American Bankers Association Information Technology and Electronic Commerce, (ITEC) Law Dept. (Feb. 1998) at §3.2. Available online www.mbc.com.

(44) The Certification Authority would be liable on contract to the applicant if he suffered a loss as a result of the inaccurate information given.

(45) It could be argued that the third party could claim under the contract between the C.A. and the certificate holder as a third party to whose benefit this contract was made.

the privity of contract if there is a special relationship which imposes on one party a duty of care about the information given.[46] This special circumstance may exist if the person giving the information knows the purpose for which it was intended to be used and knows it will be acted solely in reliance on without seeking further information. This criteria was laid down in the words of Morris:

"... it should now be regarded as settled that if someone possessed of a special skill undertakes, quite irrespective of contract, to apply that skill for the assistance of another person who relies upon such a skill, a duty of care will arise. The fact that the service is to be given by means of or by the instrumentality of words can make no difference. Furthermore, if in a sphere in which a person is so placed that others could reasonably rely upon his judgment or his skill or upon his ability to make careful inquiry, a person takes it upon himself to give information or advice to, or allows his information or advice to be passed on to, another person who, as he knows or should know, will place reliance upon it, then a duty of care will arise."[47]

This principle analysis fits squarely on the facts of the C.A.'s situation, the C.A. knows when issuing the certificate that the certificate holder's purpose is that it will be given to others[48] and knows that these others will rely on the representation stated on the certificate without seeking any further information.

(46) Hedley Byrne and Co. Ltd. v. Heller and Partners Ltd [1964] A.C. 465. For more discussions of the point, See Salmond & Heuston on the Law of Torts (20th ed.) by Heuston, R.F.V. and Buckley, R.A. (1992) London, Sweet & Maxwell Ltd. At pp. 214-9. See also Winfield and Jolowicz on Tort (20th ed.) by Rogers, W.V.H. (London Sweet & Maxwell 1984) at pp.261-292.

(47) Hedley Byrne and Co. Ltd. v. Heller and Partners Ltd. op.cit. at pp.502-3.

(48) The certificates may be published on the home page of the certificate authorities where third parties could obtain it or will be given to the applicant who will in turn pass it to third parties. The two ways make no legal difference to the C.A. liability since it has a continuous responsibility for the accuracy of the information regardless of how did the third party obtain the certificate. See Froomkin, Michael A. The Essential Role of Trusted Third parties in Electronic Commerce, Oregon Law Review. 49 (1996) at p.75.

However, applying this principle will expose the C.A. to be liable to whoever relies on their erroneous certificate which could be a large number of people indeed it could constitute a part of the worlds population. Also it may be liable for a large sum of money in compensation. For example, if an accurate certificate is being issued by a C.A. with a limit of transaction value of two million dollars a huge financial liability will be imposed on the C.A. if a large number of people relied on it and suffered loss, bearing in mind that thousands of digital signatures can be made in a very short time, in fact, it can be made in minutes or seconds, which does not give enough time for the C.A. to realize the mistake.

Although the special relationship principle was put forward as a limitation to guard against exposing a person who made a negligent misrepresentation, C.A. are still exposed "to a liability in an indeterminate amount for an indeterminate time to an indeterminate class."(49)

Similarly, in the United States section 552 of the Restatement (Second) of Torts reads as follows:

1 - One who, in the course of his business, profession or employment, or in any other transaction in which he has a pecuniary interest, supplies false information for the guidance of others in their business transactions, is subject to liability for pecuniary loss caused to them by their justifiable reliance upon the information, if he fails to exercise reasonable care or competence in obtaining or communicating the information.

2 - ...the liability stated in Subsection (1) is limited to loss suffered

(a) by the person or one of a limited group of persons for whose benefit and guidance he intends to supply the information or knows that the recipient intends to supply it; and

(b) through reliance upon it in a transaction that he intends the information to influence or knows that the recipient so intends or in a substantially similar transaction.

(49) Ultramares Corporation v. Touche 255 N.Y.Rep. 170 (1931) Per Cardozo. C.J.

It is clear that this section has been drafted in a way that limits the right of action for negligent misrepresentation only to third parties that the statement was made for their benefit and guidance.(50) Still the section does not give any limitation to the huge liability that C.A. will be exposed to since the C.A. knows that when a certificate is given to a third party it was given as guidance and that he will justifiably rely on it. Thus, it cannot be argued that C.A. could justly claim that the consequences of their misrepresentation were unexpected.

The above discussion shows that C.A. are exposed under the general principles of tort to a very huge liability that may deter anyone from playing the role of a certification authority which would in turn have a negative effect on the use of digital signature and the growth of electronic commerce.

2.1.2. C.A. Liability Under Contract

Under contractual principles there are two possibilities that may allow the relying party to recover his loss that is caused by relying on an errononous certificate. The first is a direct contractual relationship between the C.A. and the relying party. The second is the contract between the C.A. and the subscriber is made for the benefit of the relying party.

2.1.2.1. Contract between the C.A. and the relying party.

It has been suggested(51) that a contract can be constructed in two ways:

The first is that there is an offer made by the relying party when he enquired about the validity of the certificate promising to rely on it if it was valid, the C.A.'s acceptance of this offer is its confirmation that the certificate is valid.

The argument may stand if the relying party gets this information from the C.A.'s website or consulted the CRL, however, this is not

(50) See for a detailed discussion of this issue Smedinghof, Thomas J. Certification Authority Liability Analysis, op.cit. at §1.1. et.seq.

(51) Reed, C. Internet Law: Text and Materials, (2000, Butterworths. London, Edinburgh, Dublin).

always the case, since the relying party may acquire the information relied on from the certificate holder. In this case there is no communication with the C.A. thus no offer or acceptance has been exchanged.

A further obstacle encountering the formation of contract is a valuable consideration(52) moving from the relying party to the C.A. in exchange of the later confirmation that the certificate is valid.

It could be argued that the C.A. will obtain a valuable economic benefit from the increase of people that trusted their certificate to the degree of relying on it, which in turn will increase the number of people applying for their certificates in exchange for paying subscription fees.

The second is a unilateral offer made by the C.A. to the whole world promising that the information in the certificate is reliable. This offer will be considered to have been accepted by anyone who acted in accordance to, i.e. relied on the information contained in the certificate.(53)

This suggestion seems to put forward a solution to the situation where there is no direct communication between the relying party and the C.A.

However, it is essential for the formation of a legally binding contract to establish that the offerer has intended to form a contract.(54) Here it is doubted that the C.A. intended to form a contract with everyone that relied on their certificates. It can be, however, argued that the issuance of the certificate forms an act that would justifiably induce any reasonable person to believe that it intended to bind itself even if it did not intend to do so.

(52) In English Law a valuable consideration is an essential element of a valid contract. It was defined as "interest, profit or benefit occuring to one party, or some forebearance, determined, loss or responsibility given, suffered or undertaken by the other." Currie v. Misa (1875) L.R. 10Ex. 153, at 162. See generally Trietel, G.H. The Law of Contract 10th Ed. (1999, Sweet & Maxwell, London.) at pp.63-93.

(53) Reed, C. Internet Law, op.cit.

(54) See First Energy (U.K) Ltd. v. Hungarian International Bank Ltd. [1993] 2 Lloyds Rep. 195, 201, Ignazio Messina & Co. v. Polskie Linie Oceaniczne [1995] 2 Lloyds Rep. 566,571. For details see Treitel, G.H. The Law of Contract, op.cit. at pp. 9 et.seq.

A. The Contract Terms

The establishment of a contract between the C.A. and the relying party is not the only obstacle, the uncertainty still exists as to the rights and obligations of the parties of this contract.

No doubt that the main undertaking of the C.A. to the relying party is that the information in the certificate is accurate but the question is whether the C.A. accepting a strict liability i.e. it will be liable to the relying party without proof of fault on its part or it only promise that it took reasonable care so the C.A. will not be liable except if the relying party prove that it was at fault.(55)

Under the English general rules a contract for the supply of services by a professional does not impose more than a duty of care.(56) The C.A. activities which is the issuing of certificates and authenticating subscribers has been considered as a service equalizing it with a professional opinion.(57)

The EC directive seems in line with the general rules in imposing a duty of reasonable care on the C.A.(58) However, the duty imposed under this contractual relationship either between the C.A. and the subscriber or the C.A. and the relying party is being limited by the C.A. through the certification practice statements and the relying third party charter.

B. Limitation of Liability

C.A. have been providing their services in the market very cautiously. Seeking protection from liability, they included in their standard contract with the applicants for the certificate or in the trusted third party charter or in a notice on the C.A. website an overcautious

(55) Reed, C. Internet Law. op.cit. at p.139.

(56) See Treitel,G.H. The Law of Contract.op.cit. at p.780.

(57) Froomkin, 1996, III.A.1. C.f. Smedinghoff, Thomas J. Certification Authority Liability Analysis, American Bankers Association, Section 5, 5.1. It stated that " Courts may, with some Justice, view the role of the C.A. as combining elements of providing services and selling a good. In such "mixed" cases, courts consider the applicability of Article 2 of the UCC to be a question of fact concerning the nature of the transaction.

(58) E.U. Directive on Electronic Signatures, Art 6(1)(2).

disclaimer. They also include in their certificate conditions that state the maximum limit of the transaction value or the types of usage that the certificate is issued for.

These clauses are admissible under the UNCITRAL Model Law article 9(d) (iv) states:

"Any limitation on the scope or extent of liability stipulated by the certification service provider; (v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law..."

For example VeriSign disclaimer and limitation of liability clauses reads as follows:

"7.DISCLAIMERS.

a... VeriSign

(i) does not warrant that nonverified subscriber information contained in verisign certificates is accurate, authentic, reliable, complete, current, merchantable, or fit for a particular purpose,

(ii) shall not incur liability to any person for representations contained in a verisign certificate, provided the certificate was prepared substantially in compliance with the cps, and provided further that the foregoing disclaimer shall not apply to verisign's liability in tort for negligent, reckless, or fraudulent conduct,

(iii) does not warrant "nonrepudiation" for any verisign certificate or any message (because nonrepudiation is determined exclusively by law and the applicable final dispute resolution mechanism), and

(iv) does not warrant the standards or performance of any hardware or software not under exclusive ownership of, exclusive control of, or licensed to verisign.....

b. general disclaimer. Except as expressly provided in the most current netsuresm protection plan and section 6,[59] and to the extent permitted by applicable law, verisign hereby disclaims any and all other express or implied warranties and obligations of any type to any person, including any warranty of merchantability, any

(59) This Section reads as follows: "... Verisign warrants to you that (i) all validated information in or incorporated by reference in a verisign IECA Certificate is accurate and (ii) Verisign has substantially complied with the CPS when issuing the certificate....."

warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided by certificate applicants, subscribers, and third parties, and further disclaims any and all liability for any acts by verisign that constitute or may be held to constitute strict liability, whether sole or jointly with any other person, including but not limited to any ''covered person'' within the meaning of the netsuresm protection plan.

8. LIMITATIONS OF LIABILITY

A. LIMITATIONS UNDER NETSURESM PROTECTION PLAN.... the most that verisign must pay you under the netsuresm protection plan is $50,000 US. The limitations on damages and payments in this section 8 (a) do not apply to general contract damages.

b. limitations on amount of damages. In the event you initiate any claim, action, suit, arbitration, or other proceeding separate from a request for payment under the netsuresm protection plan, and to the extent permitted by applicable law, verisign's liability shall be limited as follows:

(i) The total liability of verisign in tort for negligent, reckless, or fraudulent conducts in connection with a single transaction shall be limited to $1,000,000 US. The liability caps provided in this section shall be the same regardless of the number of digital signatures, acts of authentication, or encrypted messages related to, or claims arising out of, such transaction.

(ii) subject to the foregoing subsection(b)(i), the total liability of verisign for general contract, tort, or any other damages sustained by any and all subscribers and relying parties, combined with any and all damages sustained by any and all other persons caused by the use of or reliance on a specific certificate issued under this agreement (''non-netsure damages'') shall be limited to an amount not to exceed $100,000 for the total of all digital signatures, transactions, and claims related to such certificate. The liability caps provided in this subsection shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. In the event the non-netsure damages sustained by the

use or reliance on a specific certificate exceed the liability cap for such certificate, payment of non-netsure damages shall be apportioned first to the earliest claims to achieve final resolution (by settlement or otherwise), unless otherwise ordered by a court of competent jurisdiction. Subject to section 10 and the netsuresm protection plan, verisign shall not be obligated to pay more than the total liability cap for each certificate, regardless of the method of apportionment among claimants of the amount of the liability cap. This section applies to the liability under contract (including breach of warranty), tort (including strict liability), and any other legal or equitable form of claim.

This section 8(b) does not limit refund payments under section 10 or payments under the netsure protection plan. This section 8(b) applies only to the extent permitted by applicable law

c. Exclusion of certain elements of damages. Except as expressly provided in the netsuresm protection plan, and to the extent permitted by applicable law, verisign shall not be liable in contract to any person for any indirect, special, reliance, incidental, or consequential damages (including but not limited to any loss or profits or loss of data), arising from or in connection with the use, delivery, license, performance, or nonperformance of certificates, digital signatures, or any other transactions, products, or services offered or contemplated by this agreement, even if verisign has been advised of the possibility of such damages.

To the extent permitted by applicable law, verisign shall not be liable to any person for any punitive damages arising from or in connection with the use, delivery, license, performance or nonperformance of certificates, digital signatures, or any other transaction or services offered or contemplated by this agreement.(60)

The statement regarding ''non-verified subscribers'' make the certificate issued to them by such company of no value since it disclaims

(60) VeriSign Relying party agreement Terms No.7,8 available online "https://www.verisign.com/repositry.html". The same clauses are included in the Subscriber Agreement, available online https://www.verisign.com/repository/subagr.html.

any liability for the accuracy or authenticity of the information provided in the certificate.

The role played by the C.A. in electronic commerce is one of a trusted third party and manipulation of the contractual duty by these disclaimers would undoubtedly have a very serious negative effect on its role.

In England Section 3(2)(a) of the Uniform Contract Act 1977 provided that the exclusion of liability for breach of contract must be reasonable, whether such a disclaimer is reasonable is a matter which is to be decided by courts depending on the fact of each case. The court will take into account whether the party in breach has a sufficient economic ability to meet such liability and the availability of insurance against such liability.(61) Courts will also look at the position of the parties to determine who was in a better position to insure against such risk.(62)

Here the court is more likely to consider that the C.A. is in a better position to insure against such risk than the relying party, since it is doubted if there is an insurance coverage for the relying party's risk offered in the market. The court, however, might look at the situation differently and regard such a clause as being reasonable on the grounds that it is too expensive for the C.A. to obtain such an insurance cover. However, it is doubted if the court will accept the complexity of the limitation clause since it limited the liability to "...$100,000 for the total of all digital signatures, transactions, and claims related to such certificates" here the relying party has no means of knowing whether such limit has been reached through previous claims.(63)

(61) See Photo Production Ltd. v. Securicor Transport Ltd. [1980] A.C. 827, 843 per Lord Wilberforc; Smith v. Eric S. Bush [1990] 1 A.C. 831, 858-9 per Lord Griffiths; Qughton and Lowry, 1999,397.

(62) The Uniform Contract Terms Act (1977) Section 11(4).

(63) It is doubted that such disclaimer could be enforceable by law, for example Article 11 of the UNCITRAL Draft Uniform Rules on Electronic Signatures states "(1) As between a certification authority issuing a certificate and the holder of that certificate [or any other relying party having a contractual relationship with the certification authority], the rights and obligations of the parties [and any limitation thereon] are determined by their agreement [subject to applicable law]. (2) [Subject to article 10], a certification authority may, by=

It seems from the discussion above that if the C.A. followed the procedures which it has laid-down for itself in its Certification Practice Statements (CPS)[64] it will not be held in breach of its contractual duty if any loss occurred.[65] So the situation should be reconsidered to protect subscribers and relying parties from these one-sided C.A. contracts.[66]

C. Limitation of the Value of Transaction

The limitation of value of the transaction is allowed under the UNCITRAL Model Law, Article 9 (d)(ii) it reads:

"Any limitation on the purpose or value for which the sig-nature creation data or the certificate may be used..."

In examining the clauses that draw the limit of the value of the transaction that the certificate is to be used an obvious question will arise, which is that, do these clauses have the effect that the C.A. is not liable at all if the certificate has been used for transactions exceeding the maximum limit, or would it be liable only for the loss caused by the reliance on the certificate up to the designated limit and not liable for the loss caused by the reliance on the certificate in excess of the limit.

On one hand, a person that knows the limitation on the certificate, nonetheless relied on it in excess of its limitation would be regarded as reasonable to believe that the C.A. would be liable for the loss caused by

---

= agreement, exempt itself from liability for any loss resulting from reliance on the certificate. However, the clause which limits or excludes the liability of the certification authority may not be invoked to the extent that exclusion or limitation of contractual liability would [be grossly unfair][be inherently unfair and lead to an evident imbalance between the parties][unjustifiably give one party an excessive advantage], having regard to the purpose of the contract and other relevant circumstances." See also Article 5 of the UNCITRAL Model Law.

(64) The American Bar Association (Electronic Commerce Division) issued a draft guidelines to determine whether the C.A.'s CPS satisfies a set of defined criteria. See ABA (Information Security Committee, Electronic Commerce Division) PKI Assessment Guidelines, June 18 2001.

(65) Harrison, R. Public Key Infrastructure. Risks of Being Trusted. 2000 11 C.& L. at p.28. See also Parkinson, A. Tougher line needed on digital signatures, Computerworld, 29 January 2001.

(66) Sneddon, M. Legal Liability & E-Transactions: A scoping study for the National Electronic Authentification Council, Aug. 2000, at p.43. Available online at HYPERLINK "http://www.dcita.gov.au" or http://noie.gov.au

the reliance up to the designated limit and his reliance on the certificate in excess of its limit would be at his own risk.(67) This understanding seems to coincide with Article 6.4 of the EC Directive on Electronic Signature which reads as follows:

"Member States shall ensure that a certificate-service-provider may indicate in the qualified certificate a limit on the value of transaction for which the certificate can be used, provided that the limit is recognizable to third parties. The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded."

But on the other hand, it is equally reasonable to question protecting a person who knows the limit of the value of the transaction that is permitted by the certificate and nonetheless relied on it in excess of such limit.

D. Burden of Proof

The general rules are that whoever is owed a duty of care by another has to prove that the latter has failed to take a reasonable care. Accordingly the relying party has to prove that the C.A. is in breach of its duty to him. The lack of knowledge of the ordinary person of the complicated technological operation of the C.A. made it almost impossible for the relying party to succeed in proving the C.A.'s breach of its duty, due to this reasoning the burden of proof was shifted, Article 4(1)(d) of the Electronic Signatures Regulations stated 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."(68)

(67) Reed, C. Internet Law. op.cit. at p.145.

(68) This is in line with Article 6(1)(c) of the EU Directive which stated: "... certification-service-providers are liable...unless the certification-service-provider proves that he has not acted negligently."

2.1.2.2. Contracting for the Benefit of a Third Party

The general principles of privity of contract in English Law is that a person who is not a party to a contract cannot enforce it. In the case of Dunlop Pneumatics Tyre Co. Ltd. v. Selfridge & Co.[69] Viscount Haldane stated that: "...in the Law of England certain principles are fundamental. One is that only a person who is party to a contract can sue on it."

However, the Rights of Third Parties Act 1999 made several exceptions to this principle. Article 1(1) of the Act allowed third party to enforce a contract if the contract expressly stated that he has such right or the terms of the contract stated that it was made for his benefit unless it can be understood from the contract's terms that the intention of the parties is not to allow him to enforce it. It is very unlikely that a C.A. would include in its agreement with the subscriber a term that expressly allows anyone that relies on the certificate to enforce the contract. Considering the huge liability that the C.A. may face, it is very difficult to imply that it has intended that the contract is to be enforced by third parties.

The question now is could the problem be solved through legislation?

2.2. Legislation

One of the main motives behind drafting digital signature legislation is to deal with the obstacles hindering the growth of the use of digital signatures, i.e. it is to deal with the enormous liability that prevents the establishment of certification authorities from being commercially feasible.

The information security committee of the American Bar Association (A.B.A.) initial plan in 1995 was to issue a digital signature act. However, the idea was abandoned and they settled for the issuance of "a digital signature guidelines" it was described as "not intended for

(69) [1915] A.C. 847 at p.853. See in general Treitel, G.H. The Law of Contract. op.cit at p.559 et.seq.

adoption as the text of a statute or regulation... These guidelines are intended to assist in the drafting and interpretation of such legislation.''[70]

In March 1995 the state of Utah enacted its digital signature legislation that was clearly influenced by the A.B.A. guidelines. It imposed duties and allocated liabilities on the parties in accordance to that set up in the guidelines. Similar legislation to that of Utah was enacted in many other states in the United States,[71] and in other countries.[72]

In 1998 the Uniform Electronic Transactions Act (UETA) was drafted by a committee appointed by the National Conference of Commissioners on Uniform State Law (NCCUSL). In 2000 congress enacted the Electronic Signatures in Global and National Commerce Act which is very similar to (UETA).[73]

In Europe, the European Union enacted Electronic Signature Directive 1999 which shares some similarities to that of the provision of (UETA) and which required the EU member states to adopt this directive in their national legislations.[74]

In 2001 the United Nations Commission on International Trade Law (UNCITRAL) issued a Model Law which was recommended to be adapted by countries as part of their national law. The Model Law is an attempt to unify the rules of digital signatures worldwide, to serve the transnational nature of the electronic commerce. To ensure that it will be more acceptable the UNCITRAL suggested that some of the Model Law

(70) A.B.A. Guidelines op.cit at p.23.

(71) E.g. Washington and Minisotta. However, the Electronic Signature in Global and National Commerce Act superceded the Utah Signature Law and all States that acted similar Signature Law.

(72) E.g. Malaysia. The countries that followed Utah Signature Act are considering the change to unify their rules with other countries rules to be able to electronically contract with people in other countries.

(73) For a detailed comparison between these Acts see Brumfield Fry P. A Preliminary Analysis of Federal and State Electronic Commerce Laws, 2000.

(74) For example in Germany, Act for a Basic Framework for Electronic Signature (2000). In the UK the Electronic Signature Regulations 2002.

provisions can be omitted or modified and other provisions can be added to suit each individual country's needs.[75]

The UNCITRAL Model Law played a significant role in the development of the digital signature legislation in many countries. In the Arab world for example, Tunisia enacted the Law of Electronic Commercial Transaction (No.83)(2000)[76]. In the United Arab Emirates the Law of Electronic Commercial Transactions (No.2)(2002). In Egypt, a Draft Law on Digital Signature (2001). In Bahrain, the Law of Electronic Transactions (2002). In Jordan, Draft Law on Electronic Transactions (2001).[77] In Kuwait, a Draft Law on Electronic Commerce.[78] Saudi Arabia among other Arab countries are working at the present time on similar regulation.

The legislators made considerable efforts in answering the question of who should bear the liability risk emerging out of erroneous certificates. There are only three persons which can bear such liability, the holder of the certificate,[79] the person who relied on the certificate and the certification authority. Allocating the liability risk on the holder of the certificate will deter any rational person from subscribing for a certificate. On the other hand allocating it to the relying party will undermine the aim of the role played by the certification authority, lastly, allocating the liability risk on the C.A. will defeat the object of the drafting of legislation in the first place.

It is worth giving a brief look at the liability of the C.A. under the Utah Act for completeness as being the first law to be enacted on digital

(75) Other reasons for issuing the Model Law are to assist countries with limited knowledge about this technology. See Guide to Enactment of the UNCITRAL Model Law on Electronic Signature 2001. See for details Sorieul, R. Establishing a legal framework for electronic commerce: the work of the United Nations Commission on Internationl Trade Law (UNCITRAL). Paper presented on 15 Feb. 2001 at Cairo Conference.

(76) It was influenced mainly by UNCITRAL draft rules on digital signature 1999.

(77) On recognition of electronic records in Jordanian Law see Olwan, R. Contracting and Proving Contracts in Cyberspace, Journal of Law, Kuwait University. No4 Vol.26 Dec 2002. 229, at pp.278-80.

(78) Lutfi, M. The Legal Framework for Electronic Transactions (Cairo, 2002, Al-Nassra Al-Dhahabi) at pp.85et.seq.

(79) Or the victim whose name was used by a criminal to obtain a certificate.

signature.[80] According to this Act the certificate holder is presumed[81] to have signed the document, if he alleged otherwise, he has to prove firstly, that he has not signed it and secondly, to prove that he has exercised a reasonable care to protect his private key, in order not to be liable for the loss that occurred as a result of the fraudulent use of his private key. The burden of proof is very heavy and the risk is so high that no one with a reasonable mind would accept it. However, what if the certificate holder was able to prove that he has not signed the document and that he has exercised a reasonable care to protect his private key? Who will bear the loss? The C.A., or the relying party, neither of whom has anything to do with the whole situation and has no means of preventing its occurrence.[82]

Similarly if the C.A. lost its own private key and proved to have exercised a reasonable care in protecting it, or it has issued a certificate to a criminal who used someone else's name without fault on the C.A. part. Who will bear the loss in both situations?

The UNCITRAL Model Law dealt with the issue by placing various obligations on the subscriber, the C.A. and the relying party and imposed liability on each party where they fail to meet their obligations. The relevant articles read:

---

(80) It is superceded by E-Sign (2000), the Utah Act was widely criticized in many respects. See Biddle, B. A Short History of "Digital Signature" and Electronic Signature" Legislation, 2001 available online at http://bradbiddle.com.

(81) Utah Code Art. 46-3-406, which states "If a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority:
(a)that digital signature is the digital signature of the subscriber listed in that certificate;
(b)that digital signature was affixed by the signer with the intention of signing the message; and (c) the recipient of that digital signature has no knowledge or notice that the signer:
(i)breached a duty as a subscriber; or
(ii)does not rightfully hold the private key used to affix the digital signature; and A digital signature was created before it was time stamped by a disinterested person utilizing a trustworthy system.
See also UNCITRAL Draft Uniform Rules on Electronic Signatures, Article 3. For more discussion on this point in regard to Washington Electronic Authentication Act (R.C.W.) 19. 34. See Ritter, Daniel B. and Rodin, M. Digital Signature Risks available online at http://www2.wsba.org/default.htm.

(82) W.T.V.Digital & Electronic Signatures op.cit.

Article 8. Conduct of the signatory

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

(a) Exercise reasonable care to avoid unauthorized use of its signature creation data;

(b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

(i) The signatory knows that the signature creation data have been compromised; or

(ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

(c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.

2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Article 9. Conduct of the certification service provider

1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:

(a) Act in accordance with representations made by it with respect to its policies and practices;

(b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;

(c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate:

(i) The identity of the certification service provider;

(ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(iii) That signature creation data were valid at or before the time when the certificate was issued;

(d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise:

(i) The method used to identify the signatory;

(ii) Any limitation on the purpose or value for which the sig-nature creation data or the certificate may be used;

(iii) That the signature creation data are valid and have not been compromised;

(iv) Any limitation on the scope or extent of liability stipulated by the certification service provider; (v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law;

(vi) Whether a timely revocation service is offered;

(e) Where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service;

(f) Utilize trustworthy systems, procedures and human resources in performing its services.

2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Article 11. Conduct of the relying party

A relying party shall bear the legal consequences of its failure

(a) To take reasonable steps to verify the reliability of an electronic signature; or

(b) Where an electronic signature is supported by a certificate, to take reasonable steps:

(i) To verify the validity, suspension or revocation of the certificate; and

(ii) To observe any limitation with respect to the certificate.

EU Directive Article 6 imposed on the C.A. liability for damage caused to any person that reasonably relies on the qualified certificate issued by them, the Article reads:

1....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;

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 that he has not acted negligently.

In the UK the Electronic Signature Regulations 2002 Section 4 stated regarding the C.A. liability the following:

Liability of certification-service-providers

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.

(3) Where -

(a) a certification-service-provider issues a certificate as a qualified certificate to the public,

(b) a person reasonably relies on that certificate,

(c) that person suffers loss as a result of any failure by the certification-service-provider to register revocation of the certificate, 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.

(4) For the purposes of the certification-service-provider's liability under paragraph (3) above there shall be a duty of care between that certification-service-provider and the person referred to in paragraph (3)(b) above.

The USA E-Sign Act does not contain rules applicable to the certification authority's liability.

It can be said at this stage that there is no satisfactory answer to this problem because the liability arising out of the use of a C.A. in digital signature is very large that it cannot be managed satisfactorily. However, the allocation of liability in theses provisions may prove in the future to be a significant step towards enhancing public confidence in the use of digital signatures.(83)

2.3. The Closed System

The above discussed system which is the open system, presumes that a person obtains only one certificate from one C.A. and uses it for all his

(83) The EU Directive and the Electronic Signature Legislations are dealing only with what they called a "qualified certificate" so the none-qualified certificates will be governed by the general rules.

dealings. The closed system, on the other hand, has been defined by a commentator as being a system "where public key mechanisms are used within a specific, bounded context."(84)

An example of the closed system environment may clarify the picture, a digital signature could be issued by a company to its employees to be used internally, or a trader could issue digital signature certificates to its customers to be used only when dealing with him. It can also be implemented in business-to-business trading.(85)

In these situations the liability risk is very small comparing with the liability in the open system and therefore can be easier to manage. Whoever acts as a C.A. in the closed system will know relatively the value of the transaction which the certificate will be used for and accordingly could estimate the liability risk. It could then distribute this liability risk between the two parties by stipulating it in its contract with them and add a margin to the subscription to cover the undistributed cost of liability.

The closed system therefore offers a practical solution for the time being until these regulations that define the parties respective rights and duties and their potential liabilities prove practically that it is effective in enhancing the trust in international electronic commerce.

Conclusion

According to the digital signature mechanism, it is necessary for any two people who do not know each other and want to conduct their business through the Internet to have a third person who is trusted by both, to identify them to each other.

This third person is a Certification Authority, who issues certificates which identify and authenticate the transacting parties' signatures. The

(84) The "CyberSign" and "CyberTrust" are examples of the closed system. See Bradford Biddle, C. Legislating Market Winners, Digital Signature Laws and Electronic Commerce op.cit at p.9. also Value Added Networks (VANs) is now in use for business to business transactions. See Gulshan Rai, Dubash, R.K. and Chakravarti, A.K. Digital Signature Law - A Survey of the International Scenario, op.cit at p.4.

(85) Under this system an individual may need to obtain several certificates from different C.A.'s but that should not constitute any problem.

problem preventing the development of the certification authority industry is its exposure to the uncertain and potentially enormous liability arising out of erroneous certificates.

Under the general principle of torts they will be liable with no limitation for a breach of their duty of care. On the other hand, the inclusion of a limitation clause in the certificate authority's contracts with both parties will undermine its role as a trusted third party.

Legislation was enacted in many countries in attempts to balance the liability between the parties, and reversed the burden of proof upon the C.A. which is more capable of doing so since they know more than the other parties regarding the technology which they use. However, this may seem to give a solution to the problem from a legal standpoint but in practice the effect of such legislation is still to be seen since the liability is more in size than can be managed satisfactorily, at least at the present time.

However it may be beneficial to consider the possibility of not restricting the development of the industry by legislation and leave the market to resolve the problem of C.A.'s liability by a trade usage or courts' decisions,(86) since at the time of writing this article the certification authority market is still new. Accordingly, at the present time a certified digital signature is not as trusted as described to be by some, so a person using the technology and seeking a high level of security should buy an adequate insurance cover.(87)

Until the liability problem of the open certification authority system is solved the practical system to be used for authentication (despite its disadvantages) is the closed certification authority system, which deals with a very limited number of people and hence reducing the size of the liability risk to a size which can be managed, by being distributed between the parties in advance through their contractual relationship. This will no doubt provide a temporary solution giving time for the industry to be firmly established and to the open system authentication technology to be developed.

(86) In the USA the E-Sign Act did not deal with the C.A.'s liability issue.

(87) Wheatman, V. PKI Authentication Liability in a Litigious World, Gartner, 2001.

Bibliography

- Al-Hafanawi, F. The Law of Computer Programs, (2001, Dar AlKitab, AlHadith, Cairo).
- American Bar Association (ABA) (Information Security Committee, Electronic Commerce Division) PKI Assessment Guidelines, June 18, 2001.
- American Bar Association (ABA) Digital Signature guidelines, Information Security Committee Electronic Commerce and Information Technology Division, Section of Science and Technology (Aug. 1996).
- American Bar Association, Digital Signature Guidelines Tutorial, (1996) available online at http://www.abanet.org/scitech/ec/ics.html.
- Anonymizer FAQ, http://anonymizer.cs.cmu.edu:8080/faq.html.
- Barassi, Theodore Sedwick The Cyber Notary, ABA Section of Science and technology, Cyber Notary Committee available online at http://www.abanet.org/scitech/ec/cn/home.html.
- Baum, Michael. Information Technology and the Law.
- Bayer, D. Improving the efficiency and Reliability of Digital Time-Stamping, in sequences II, Methods in Communication, Security and Computer Science, 1993.
- Bradford Biddle, C. COMMENT: Misplaced Priorities: The Utah Digital Signature act and Liability Allocation in a Public Key Infrastructure, 33 San Diego L. Rev. 1143 (1996).
- Bradford Biddle, C. A Short History of "Digital Signature" and Electronic Signature" Legislation, [published in Simon Garfinkel, WEB SECURITY, PRIVACY AND COMMERCE (2nd Edition, O'Reilly, 2001)]
- Bradford Biddle, C. Legislating Market Winners, Digital Signature Laws and Electronic Commerce Marketplace, World Wide Web Journal (27-5-1997) available online www.w3journal.com/7/s3.biddle.-wrap.html.
- Braunstein, Michael, Remedy, Reason and the Statute of Frauds: A critical Economic Analysis, (1989) Utah Law Review 383.

- Brightbill, T. & Dylang, S. Barriers to International Electronic Commerce: Recent Issues and Developments, 2002. This article is based on "Overcoming Barriers to Global Economic Commerce" A paper presented in conjunction with a seminar at the ABA Annual Meeting in Chicago on Aug 6, 2001.
- Brumfield Fry P. A Preliminary Analysis of Federal and State Electronic Commerce Laws, 2000.
- Chang Su Han, Law and Digital Signatures in Cyberspace: Which Law Should be Applied? (Dec. 1997), available online at http://wings.buffalo.edu/law/complaw.
- Cohen, F. A Short History of Cryptography, (1995) available online http://www.all.net/.
- Corbin, A.L. Corbin on Contracts. (St. Paul, Minn. West Publishing Co., 1952).
- Electronic Commerce, Building the Legal Framework, Report of the Electronic Commerce Expert Group to the Attorney General, (31-3-1989) available online http://www.law.gov.au/aghome/advisory/eceg/eceg.htm.
- Electronic Signature Legislation, UK. 8th March 2002.
- Electronic Signatures in Global and National Commerce Act. Enacted by Congress in 2000.
- E.U. Directive enacted by the European Union Parliament in December 1999.
- Ford, W. Advances in Public-Key Certificate Standards, SIG Security, Audit & Control Rev., July 1995.
- Froomkin, A. Micheal The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Oregon Law review. 49 (1996).
- Greenleaf, G. and Clarke, R. Privacy Implications of Digital Signatures, (10-3-1997) available online at http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html.
- Gulshan, Rai., Dubash, R.K. and A.K. Chakravarti, Digital Signature Law - A Survey of the International Scenario, Oct. 1997. Information Technology Group Dept. of Electronics Govt. of India.

- Harrison, R. Public Key Infrastructure. Risks of Being Trusted, 2000 IIC & L 28.
- Heuston, R.F.V. and Buckley, R.A. Salmond & Heuston, The Law of Torts, (20th ed.) (1992, London, Sweet & Maxwell Ltd).
- Hindelang, S. N Remedy for Disappointed Trust - The Liability Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in England and Germany Compared, The Journal of Information, Law and Technology. J.I.L.T. 2002(1).
- Jamaie, H. Proving Legal Actions Which Are Made Through the Internet, (2000) Dar AlNadah Al-Arabia, Cairo.
- Johnson, James A. Digital Signature Legislation, Enacted State Digital Signature Legislation (March 1997) available online at http:// nii.nist.gov/pubs/entsign.html.
- Katz, Paul R. Electronic Documents and Digital Signatures: Changing the Way Business Is Conducted and Contracts Are Formed, E-Commerce Law Report, March 1999 at Note 30.
- Lutfi, M. The Legal Framework for Electronic Transactions, (Cairo, 2002, Al-Nassra Al-Dhahabi).
- Marion, Larry, Who's Guarding the Till at the CyberMall?, Datamation, Feb. 15, 1995.
- Merrill, Charles R. Time Is of The Essence - Electronic Documents Will Stand Up in Court Only If the Who, What and When They Represent are Unassailable. (March 15, 2000) (C.I.O. Magazine) available online http://www.cio.com/archive/03/500_fine.html.
- Olwan, R. Contracting and Proving Contracts in Cyberspace, Journal of Law, Kuwait University. No 4 Vol.26 Dec 2002.
- Parkinson, A. Tougher line needed on digital signatures, Computer-world, 29 January 2001.
- Reed, C. Internet Law: Text and Materials, (2000, Butterworths. London, Edinburgh, Dublin).
- Restatement (second) of contracts (1982).
- Ritter, Daniel B. and Rodin, M. Digital Signature Risks, (March 1998) available online at gttp://www2.wsba.org/default.htm.

- Rogers, W.V.H. Winfield and Jolowicz on Tort, (20th ed.) (London, Sweet & Maxwell 1984).
- Schneier, B. Why cryptography is Harder Than It Looks, (19-3-99) available online at http://www.counlerpane.com/publish.html
- Smedinghof, Thomas J. Certification Authority Liability Analysis, American Bankers Association Information Technology and Electronic Commerce, (ITEC) Law Department (Feb. 1998) available online www.mbc.com.
- Sneddon, M. Legal Liability & E-Transactions: A scoping study for the National Electronic Authentification Council, Aug. 2000. Available online at http://www.dcita.gov.au or http://noie.gov.au.
- Sorieul, R. Establishing a legal framework for electronic commerce: the work of the United Nations Commission on International Trade Law (UNCITRAL), Paper presented on 15 Feb. 2001 at Cairo Conference.
- SuretyTechnologies, Home Page available on-line http://www.surety.-com.
- Survey of International Electronic and Digital Signature Initiatives, (24-9-1999) available online "Internet Law and Policy Forum" Home Page.
- The Federal Trade Commission Staff, Report on Protecting Consumers Online, Dec 1999 available online at http://www.ftc.gov.
- The Uniform Contract Terms Act (1977).
- Trietel, G.H. The Law of Contract, 10th Ed. (1999, Sweet & Maxwell, London).
- U.C.C. (Uniform Commercial Code) United States of America.
- Uniform Electronic Transactions Act (UETA) 1998.
- United Nations Commission on International Trade Law (UNCITRAL), Working group on Electronic Commerce, Thirty-fourth session, Draft Uniform Rules on Electronic Signatures. Vienna, 8-19 Feb. 1999.
- United Nations Commission on International Trade Law (UNCITRAL) Thirty-fourth Session, Vienna, 25 June - 13 July 2001. Model

law on Electronic Signatures (hereinafter cited as UNCITRAL Model Law).

- Utah Code. (1995) amended in 1996 Digital Signature Act, 52nd Leg. Gen. Sess. 1996, Utah Law 188. available online at http://www.state.ut.us/ccj/digsig/dsut-act.htm.
- VeriSign Public Certification Services, Server Certificate Agreement, available online at http://www.verisign.com/partner/legal.html.
- Washington Electronic Authentication act (R.C.W.).
- Wheatman, V. PKI Authentication Liability in a Litigious World, Gartner, 2001.
- W.T.V. Digital & Electronic Signatures Cryptography, (6-12-1997).