CENTRAL EUROPEAN UNIVERSITY

LEGAL STUDIES

INTERNATIONAL BUSINESS LAW

DIGITAL SIGNATURES IN THE E-COMMERCE

by Khalilova Sabina

LL.M. SHORT THESIS
COURSE: Legal aspects of Internet and Electronic Commerce
PROFESSOR: Vladimir Pavic
Central European University
1051 Budapest, Nador utca 9.
Hungary

Abstract

The increasing use of e-commerce generally is considered a positive trend that should be promoted. The security in the electronic transactions over the Internet is regarded as one of the most crucial issues in the digital world. During the last decade, national and international legislators have been trying to promote the use of electronic signatures in the e-commerce and set forth a common legal framework for electronic authentication over the Internet. However, many lawyers believe that laws requiring signatures to authenticate certain transactions represent obstacles to e-commerce and threaten to keep it from reaching its full potential.

The given topic is chosen as the computerization of almost all fields, including the legal field, has nowadays become an increasingly acute problem for the professionals of each field who are not familiar with the technology novelties, which can cause problems in their own field. One such novelty appearing in recent years is digital signature, which has become more and more frequently used in the legal field for document authentication.

The thesis is aimed at facilitating the work of practitioners dealing with digital signatures by theoretical analyses of the practical and legislative problems in order to avoid obstacles that may arise in future. The national and international laws adopted in this area are quite new and not confirmed by long practice, for this reason there are gaps which should be filled and issues which can be better regulated. This work analyzes a number of international legislative efforts, their interpretations and proposals of their perfection as well as evaluates their effectiveness.

TABLE OF CONTENTS

Introduction 1

Chapter 1 - Digital Signatures: what they are and how they work 4

1.1 Legal functions and requirements of signatures.. 4

1.2 Electronic signatures 9

1.3 Encryption as an electronic signature technology.. 13

1.4 Definition, meaning, legal effects of digital signatures 19

Chapter 2 - International initiatives relating to electronic signatures 27

2.1 UNCITRAL Model Laws 33

2.2 EU Electronic Signature Directive.. 40

2.3 US Uniform Electronic Transactions (UETA) and Electronic Signatures in Global and National Commerce (E-SIGN).. 53

2.4 EU v. US legal approach towards electronic signatures 63

Conclusion.. 67

Bibliography... 70

Introduction

Nowadays, in the era of widespread electronic communications and predominant commercial environment, establishing a framework for the authentication of computer-based information, it is required to be familiar with concepts and professional skills from both the legal and computer security fields. Conjunction of these two fields may seem unfeasible, since notions from the information security field, even in cases of terminological similarity, usually hardly correspond to notions from the legal field.[1]

The historical legal concept of ‘signature’ is very broad; it admits any mark made with the intention to authenticate the marked document. The term ‘electronic signature’ has different meanings and is defined by most of the legislative acts of various countries differently. Thus many recent studies have focused on a discussion over what constitutes a valid signature in the electronic environment. However, from the information security viewpoint, ‘electronic signatures’ are distinct from ‘digital signatures’, though the latter is sometimes used to mean any form of computer-based signature. Digital signature is recognized as a result of certain specific technical processes application to specific information.

In order to establish transparency in existing term ambiguity between ‘electronic’ and ‘digital’ signatures and further to analyze their legal effects, this paper will refer to previous works of such well-known researchers as Jos Dumortier, who has dozen of articles related to the topic, Lorna Brazell, Christopher Reed, Ian Lloyd and others.

The given topic is chosen as the computerization of almost all fields, including the legal field, has nowadays become an increasingly acute problem for the professionals of each field who are not familiar with the technology novelties, which can cause problems in their own

[1] Digital Signature Guideline Tutorial, http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

field. One such novelty appearing in recent years is digital signature, which has become more and more frequently used in the legal field for document authentication. While most of the national and international acts and scholars recognize that digital signatures are the ones based on the use public key cryptology technology, there are also some radically critical views to such definition. For instance, Bruce Schneier, an internationally renowned security technologist and author, denies consideration of digital signatures as signatures at all and claims that the laws on digital signatures are 'a mistake' stating that 'calling whatever Alice creates a "digital signature" was probably the most unfortunate nomenclature mistake in the history of cryptography…... The problem is that while a digital signature authenticates the document up to the point of the signing computer, it doesn't authenticate the link between that computer and Alice… When the judge sees a digital signature, he doesn't know anything about Alice's intentions. He doesn't know if Alice agreed to the document, or even if she ever saw.'[2]

I disagree with this purely technical approach to the digital signatures, and agree with most of the scholars and legislators in a view that as long as the digital signature in the e-commerce satisfies such functions as to identify a person and to associate that person with the content of a document as well as to provide certainty as to the personal involvement of that person in the act of signing, it constitutes an equivalent of paper-based signatures in the real world transactions.

The national and international laws adopted in this area are quite new and not confirmed by long practice, for this reason there are gaps which should be filled and issues which can be better regulated. This work will analyze a number of international legislative efforts, their interpretations and proposals of their perfection as well as evaluate their

[2] Bruce Schneier, "Why Digital Signatures Are Not Signatures", http://www.schneier.com/crypto-gram-0011.html

effectiveness.

The methodological basis of the present thesis is comprised of such methods as dialectical, historical, comparative legal methods, data commentary and case study.

In order to explain the value of digital signatures, I will start with an overview of the legal significance of signatures, which the first section is dedicated to. To understand what digital signatures are and how they work, it is relevant to have basic comprehension of electronic signatures and encryption technology, since digital signatures are a form of electronic signatures, which are created and verified by cryptography. Thus, the first chapter logically will endure with sections relating to electronic signatures, encryption technology, and further explain the essence of a digital signature itself.

The second chapter will deal with international initiatives relating to electronic signatures. The thesis will analyze the most important legislative acts and regulations in this sphere such as UNCITRAL Model Laws, ICC general usage for internationally digitally ensured commerce, OECD ministerial declaration on authentication for electronic commerce, US Uniform Electronic Transactions (UETA) and Electronic Signatures in Global and National Commerce (E-SIGN), EU Electronic Signatures Directive and eventually, will finalize providing with comparison of European and American approaches.

Chapter 1 - Digital Signatures: what they are and how they work

1.1 Legal functions and requirements of signatures

In order to explain the value of digital signatures, it is relevant to look through the meaning and the legal significance of signatures in the real world.

There are a number of requirements, such as conveyance of information ‘in writing’, by a ‘document’, or authentication of it by ‘signature’, that have been recognized as barriers to efficacious e-commerce.[3]

Writing ‘is the preservation and the preserved text on a medium, with the use of signs or symbols’.[4]

The essence of writing requirement is not limited to ink on paper, but rather to communication having a tangible form. Courts have held that telexes, faxes and even tape recordings constitute ‘writings’ for various purposes.[5]

A signature (from Latin *signare*, " sign") ‘is a handwritten (and sometimes stylized) depiction of someone's name (or some other identifying mark) that a person writes on documents as a proof of identity and will’.[6]

There exist also special signature machines capable to reproduce automatically individual's signature, which usually used by people required to sign many documents, for example celebrities, Head of state or CEO/s. Moreover, some cultures, Japanese, for example,

[3] Diane Rowland and Elizabeth Macdonald “Information Technology Law”, second edition, Cavendish Publishing Limited, London, Sydney, 2000, 347.
[4] Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Writing
[5] Thomas J. Smedinghoff and Ruth Hill Bro “ Electronic Signature Legislation”, at http://library.findlaw.com/1999/Jan/1/241481.html
[6] Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Signature

have no signatures, as such, but use name seals called inkans with the name written in tensho or ”seal script”.[7]

The essence of a requirement is presence of a ‘symbol’ accompanied by the party’s ‘intention’.[8]

In most of the cases, the main purpose of a signature is to evidence the original of the document or approval of it by a particular individual[9]. In other words, the prime function of a signature is to give evidence of the source of the document (identity) or the intention (will) of a person in respect of that document[10].

In many countries, it is required by the law that contracts must be “in writing” or “signed.” The concern can arise about the meaning of these words in the context of the Internet. This and similar issues arising in connection with records or forms, such as legal requirement of government filing can be solved by legal provisions providing that "a signature, contract or other record may not be denied legal effect, validity or enforceability solely because it is in electronic form.”[11]

Electronic communications technology requires signature methods which are different from the paper-based ones. Basically, there are two possibilities where Internet communications are concerned:

1) the incorporation of a scanned image of a paper-based signature into a word processing file, which is sent further as an email attachment;

[7] http://www.infothis.com:80/find/Signature/

[8] Thomas J. Smedinghoff and Ruth Hill Bro “ Electronic Signature Legislation”, at http://library.findlaw.com/1999/Jan/1/241481.html

[9] Ian Lloyd, ‘Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures’, LAW & THE INTERNET regulating cyberspace, edited by Lilian Edwards and Charlotte Waelde, ‘HART’ publishing, Oxford, 1997, 140.

[10] Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Signature

[11] Online eCommerce Guidance Handbooks: E-Commerce/Digital Signatures, Global Internet Policy Initiative at http://www.internetpolicy.net/e-commerce/

2) an electronic signature created by the means of a mathematical process.[12]

Signatures perform variety of functrions in the real world, not all of which are legally effective. Moreover, signatures are treated significantly differently by different legal systems.[13]

In some instances, legal requirement of a signature can serve as a prerequisite to the validity of the document. Nevertheless, case law in common-law countries broadens interpretation of this notion, so long as some physical mark attached to paper indicates its approval or adoption. In *Goodman v. Eban* the Court of Appeal held that using 'a rubber embossed with the name of the firm' by a solicitor satisfied the requirement of signed bills under the Solicitors Act 1932. It was stated that:

> "where an Act of Parliament requires that any particular document be 'signed' by a person, then, prima facie, the requirement of the Act is satisfied if the person himself places on the document an engraved representation of his signature by means of a rubber stamp…. the essential requirement of signing is the affixing in some way, whether by writing with a pen or pencil or by otherwise impressing upon the document, one's name or 'signature' so as personally to authenticate the document."[14]

In addition, in *Clipper Maritime Ltd v Shirlstar Container Transport Ltd (The "Anemone")* the Court has reached a view that 'the answerback of a telex machine could constitute a signature since this would both indicate the origin and the approval of contents by the sender'.[15]

In re a Debtor established compliance of faxed copy of a signed proxy with the statutory provisions requiring a signature:

"Once it is accepted that the close physical linkage of hand, pen and paper is not

[12] Christopher Reed 'Internet Law: Text and Materials', Butterworths, London, Edinburgh, Dublin, 2000, 154.

[13] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 11.

[14] Ian Lloyd, 'Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures', LAW & THE INTERNET regulating cyberspace, edited by Lilian Edwards and Charlotte Waelde, 'HART' publishing, Oxford, 1997, 140-141.

[15] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 21.

necessary for the form to be signed, it is difficult to see why some forms of non-human agency for impressing the mark on the paper should be acceptable while others are not."[16]

Similarly, the Supreme Court of British Columbia in Canada ruled the same conclusion on almost identical facts in *Beatty v First Explor. Fund 1987 & Co.*[17]

The Dutch Supreme Court has likewise accepted that 'a writ of summons may be valid if signed and served by fax, even though the relevant statutory provisions prescribe a written signed writ'. Nevertheless, although Dutch law has recognized a facsimile or stamp as a signature, a cross or fingerprint, unlike under the English view, has not been accepted as a valid signature.[18]

In order to resolve this term ambiguity, legislators of different countries adopt statutes defining them. UNCITRAL brought relative clarity in this issue, by adopting in its Model Law on Electronic Commerce definitions of 'writing' and 'signature'. Articles 6 and 7 states accordingly:

> "Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference."[19]
>
> "Where the law requires a signature of a person, that requirement is met in relation to a data message if:
>
> (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
>
> (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement."[20]

[16] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 21.
[17] Ibid, 23.
[18] Ibid.
[19] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, art. 6, available at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf
[20] Ibid, art. 7

The purpose of adopting these articles is described in details in ‘article-by-article remarks’ in Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996).

A signature does not constitute the substance of a transaction, but rather serves as a representation or form of it. A signature serves to such purposes as evidence, ceremony, approval, efficiency and logistics. In order to achieve these purposes, a signature must have such attributes as signer and document authentication, which means that a signature have to indicate who signed the document and what is signed making it unfeasible for others to reproduce or alter it.[21]

Basically, a handwritten signature fulfills a variety of formal functions, which are, however limited by a party autonomy principle, which means that ‘in most cases a signatory should be able to rely on an expression of his will (such as a signature) being respected and not invalidated by the legal system for failure to meet a handwriting requirement, as long as it is clear from the circumstances that he intended to be bound by it.’ The question to be solved by legal systems is to balance all mentioned interests, which becomes rather more complicated in electronic authentication cases than in traditional paper signatures.[22]

[21] American Bar Association ‘Digital Signature Guideline Tutorial’, http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

[22] Christopher Kuner and Anja Miedbrodt “Written Signature Requirements and Electronic Authentication: A Comparative Perspective”, at http://www.kuner.com/data/articles/signature_perspective.html

1.2 Electronic signatures

Online vendors and purchasers can face the barrier of securing their e-commerce transactions by authenticating the signatures coming with such transactions. Signature authentication has become the concern of majority state and international legislators, as well as a topic of debates in private organizations.[23]

The term 'electronic signature' has different meanings and is defined by most of the legislative acts of various countries differently.

In the US, Uniform Electronic Transactions Act (UETA), released by the National Conference of Commissioners on Uniform State Laws (NCCUSL) in 1999, defines it as "an electronic sound, symbol, or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."[24] The US E-SIGN Act of 2000[25] adopted most of the notions of UETA, including an electronic signature definition. While this definition may seem vague at first, in reality, most of us unknowingly use some form of electronic signature on a regular basis. Using a PIN or password access an ATM, enter a website or purchasing on-line are common examples of electronic signature usage. In such cases, a birthday, anniversary or the name of a pet can serve as your unique identifier. In addition, a name typed at the end of an e-mail or even a digitized image of one's handwritten signature could be accepted as an electronic signature under E-SIGN.[26] E-SIGN makes electronic signatures legally binding, like its handwritten counterparts, as it prohibits denial of

[23] Jonathan D. Hart, "Law of the web, a field guide to internet" publishing 2003 edition, Bradford Publishing Company, Denver, Colorado, 203.

[24] Uniform Electronic Transactions Act (1999), Section 2(8), available at http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm

[25] Electronic Signatures in Global and National Commerce Act, June 30, 2000, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf

[26] John S. Stolz and John D. Cromie, "Electronic Signatures in Global and National Commerce Act", 2001, at http://www.connellfoley.com/articles/oneclick.html

the legal effect of electronic instuments of the e-commerce solely on the ground that they are not in writing, in the case of their electronic form or they are not signed, if the signature is produced by the use of electronic means.[27]

The EU Electronic Signatures Directive, approved by the European Commission in November 1999, states that ‘electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication’. [28]

Consequently, electronic signature means anything, any peace of data. The definition is so wide that even putting a name in an e-mail can be sufficient to be accepted as an electronic signature. Basically, electronic signatures are ‘computer-based personal identities’.[29]

In recent years, the terms "electronic signature" and “digital signature” have come into widespread, and somewhat confused, use. The situation is unsatisfactory in many respects, and will remain so until usage, especially in statutes and regulations, becomes more standardized. Electronic signature is often used to mean ‘either, or both, cryptographic means to add non-repudiation and message integrity features to a document, or a signature imputed to a text via one or more of several electronic means’.[30]

In law, if there is a dispute about a signature on a contract or other document, the signature must meet certain requirements which would be called in question by a court. These requirements differ from jurisdiction to jurisdiction. The offer was found to be binding in cases

[27] Jonathan D. Hart, “Law of the web, a field guide to internet” publishing 2003 edition, Bradford Publishing Company, Denver, Colorado, 204.
[28] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities, Art.2, available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf
[29] Christina Spyrelli “Electronic Signatures: A Transatlantic Bridge? – An EU and US Legal Approach Towards Electronic Authentication”, published in “Journal of Information, Law and Technology”, 16 August 2002, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/
[30] http://www.infothis.com:80/find/Electronic_signature/

where the signature was challenged, telegrams, such as ‘I accept, John’ although John never actually touched the telegraph key, and faxes of documents, even when the original was not signed by the sender.[31]

A principal issue in such cases is forgery and imitation of assent, and in these decisions, courts have found that forgery and imitation can be in practice ruled out. However, it remains still to be easily possible for many electronic methods of signature, or imputed signature, to forge or imitate assent. The ease of such forgeries is illustrated by the rapidly rising problem of identity theft. This can be applied only to ‘electronic signatures’ that have been found legally binding in some circumstances, but not to digital signatures that resolve this problem as there is cryptographic assurance of the sender's identity and integrity check on the text received.[32]

Notwithstanding the fact that electronic signature technology and legislation are relatively new, a few courts have confronted the problem of solving the issues of validity of electronic signatures.

In re Piranha, Inc. involved a dispute over corporate control and the date on which a director resigned. The form of resignation contained director’s electronic signature, which presented the essence of debate. The Court directly relied on UETA section 7a, which would not permit denial of electronic signatures solely on the grounds of its electronic form and ruled that under UETA a person is not precluded from contesting that he executed, adopted, or authorized an electronic signature that is purportedly his.[33]

In *Cloud Corporation v. Hasbro Inc.*, the Court of Appeals for the Seventh Circuit, concluded, notwithstanding the fact that it could not rely on E-SIGN, as it does not apply retroactively to contracts formed before it took effect in 2000, that the text of email plus an

[31] http://www.infothis.com:80/find/Electronic_signature/
[32] Ibid.
[33] ‘Electronic records and signatures’ available at http://www.law.uh.edu/faculty/RNimmer/contracts/supp10.pdf

apparently written notation nevertheless had satisfied the requirements of the statute of frauds.[34]

In *Sea-Land Service, Inc. v. Lozen International, LLC* the Court of Appeals for the Ninth Circuit decided that internal corporate email with signature block, forwarded to a third party by another employee, was admissible over hearsay objection as a party-admission, where the statement was apparently within the scope of the author's and forwarder's employment. It was held that an electronic signature on a document was adequate proof of its authenticity and is admissible evidence.[35]

Nevertheless, some state courts have come to opposite conclusions deciding the validity of electronic signatures issues under the statute of frauds. The Massachusetts Superior Court held in *Shattuck v. Klotzbach* that typewritten names used by the authors of the message at the end of e-mail were of equal value to written signatures and thus were in accordance with the requirements of the state's statute of frauds. On the contrary, the Washington State Court of Appeals refused the validity of some e-mails under the state's statute of frauds in *Hansen v. Transworld Wireless TV-Spokane, Inc.*, as they were sent prior to acceptance of the offer and held them as a part of 'continuing negotiations'. Moreover, the court concluded that e-mail communications would not be a sufficient proof of signature requirement anyway, as they are not in conformity with the writing requirements of Washington's statute of frauds.[36]

Consequently, it is necessary to be aware of the presumptions relating to the use of electronic signatures across jurisdictions. What might be acceptable in one jurisdiction will not necessarily be enforceable in another, unless reasonable care is used to establish whether the

[34] Cloud Corporation v. Hasbro Inc., available at http://www.emlf.org/Resources/cloud.pdf
[35] Sea-Land Service, Inc. v. Lozen International, LLC, available at http://www.admiraltylawguide.com/circt/9thsealandlozen.pdf
[36] Jonathan D. Hart, "Law of the web, a field guide to internet" publishing 2003 edition, Bradford Publishing Company, Denver, Colorado, 206.

format of a particular form of electronic signature is enforceable. For lawyers, the principal issue will be how to prove the connection between the application of the signature of any form and the person whose signature it purports to be. Even in cases where there is a presumption that the person used a digital signature whose signature it was issued to, there remains in the legislation the possibility of challenging such a presumption.[37]

1.3 Encryption as an electronic signature technology

Cryptography '(or cryptology; derived from Greek κρυπτ ός *kryptós* "hidden," and the verb γράφω *gráfo* "write") is the study of message secrecy.'[38]

"Cryptography means hidden writing: it is the art of writing messages in such ways that they cannot be read by third parties."[39] One of the main purposes of it is not usually to hide the existence of the messages, but rather their meaning.

Encryption is 'the process of transforming a readable 'plaintext' message into an unreadable form or 'cipher''.[40] It is the process of converting ordinary information, which is called plaintext, into 'unintelligible gibberish' or so called 'ciphertext'[41] or in other words, from comprehensible form into incomprehensible one.

The art of recovering the hidden meanings of messages is called cryptanalysis and the process of it – decryption.[42] Decryption is referred to the reverse process, from 'ciphertext' to the 'plaintext'. Encryption and decryption are performed by a pair of algorithms, so called

[37] Stephen Mason "ELECTRONIC SIGNATURES IN PRACTICE", published in Journal of High Technology Law 2006, http://international.westlaw.com/Welcome/WorldJournals/default.wl?blinkedcitelis

[38] Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Cryptography

[39] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 50.

[40] Ibid.

[41] Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Ciphertext

[42] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 50.

‘cypher’ (or ‘cipher’).

The most secure cipher, logically unbreakable encryption method, which has been invented even before the invention of the computer, is the ‘one-time pad’.[43] The use of it is very simple, both sender and receiver have a pad which informs them how to convert it to form the cipher for each letter.[44] There is a disadvantage of this method; it requires a key as long as the message itself, which should not be used more than one time, hence ‘one-time’. Reuse of a key is dangerous because of code-breakers who can misuse it.[45]

Cryptography is not a new art, it has thousands of years history. Julius Caesar invented Caesar’s code and used methods of cryptography to communicate with his generals during his military campaigns. He shifted three places each letter in a message to one or opposite direction (left or right) in the alphabet and had as a result a string of meaningless letters at the first glance but which could be easily read by a receiver who knew the trick.[46]

To illustrate the process, let’s place two alphabets above each other:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

XYZABCDEFGHIJKLMNOPQRSTUVW

According to Caesar’s code, the word ‘book’, for example, would read YLLG.

The other main form of encryption is produced by the use of a process of transposition. For example, taking the phrase, such as

AN INTERESTING ARTICLE

[43] Caspar Bowden and Yaman Akdeniz “Privacy II: Cryptography and Democracy – Dilemmas of Freedom”, “Liberating Cyberspace, Civil Liberties, Human Rights and the Internet” edited by Liberty (The National Council for Civil Liberties), Pluto Press, London – Sterling, Virginia, USA, 1999, 85.

[44] Lorna Brazell “Electronic Signatures Law and Regulation”, first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 50.

[45] Caspar Bowden and Yaman Akdeniz “Privacy II: Cryptography and Democracy – Dilemmas of Freedom”, “Liberating Cyberspace, Civil Liberties, Human Rights and the Internet” edited by Liberty (The National Council for Civil Liberties), Pluto Press, London – Sterling, Virginia, USA, 1999, 85.

[46] Lorna Brazell “Electronic Signatures Law and Regulation”, first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 50.

and then omitting spaces and putting the letters into blocks of five, we would receive:

ANINT EREST INGAR TICLE

Then we shift the letters in each block in a predetermined method. For example, if the first letter is moved to the third place, second to fourth, third to fifth, fourth to first and fifth to second, the result would be:

NTANI STERE ARING LETIC

Cryptographic system design is a form of art. A designer has to balance between security and accessibility, anonymity and accountability, privacy and availability.[47]

Nowadays, in the time of modern technology, obviously there is a use of more complex methods, but basically, until recent times, most of the codes were based on these two techniques.[48]

Throughout history there has been a constant battle between people who wanted to use encryption to preserve secrecy and the ones wishing to break the codes.[49] This battle became very acute during the Second World War. The Americans had great success at breaking Japanese codes, while the Japanese, unable to break US codes, assumed that their codes were also unbreakable. German codes were predominantly based on the so-called 'Enigma' machine. The group of British and Polish cryptanalysts first broke the Enigma early in WW2.[50]

In response to the vulnerability of traditional forms of encryption, modern systems rely on mathematical techniques. One of the first such cryptographic techniques was performed in

[47] Bruce Schneier "Why Cryptography Is Harder Than It Looks", http://www.schneier.com/essay-037.pdf

[48] Ian J Lloyd "Information Technology Law", third edition, Butterworths, London, Edinburgh, Dublin, 2000, 580.

[49] Ian Lloyd, 'Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures', LAW & THE INTERNET regulating cyberspace, edited by Lilian Edwards and Charlotte Waelde, 'HART' publishing, Oxford, 1997, 142.

[50] Fred Cohen & Associates, specializing in information protection since 1977, "A Short History of Cryptography", http://all.net/books/ip/Chap2-1.html

the United States Data Encryption Standard or DES, which is an example of a single key or symmetric encryption system. The same mathematical key is used to encode and decode a message.[51] The system is compared sometimes with the same key used to open and lock a door. The system is secure so long as it is known only to communication parties, the sender and recipient. [52]

An absolutely new cryptographic form was invented in 1976 by two mathematicians, Diffie and Hellman. Public key concept or asymmetric cryptography acquired widespread practical use due to three further mathematicians, Rivest, Shamir and Adleman after whom the RSA system is named. The system is based on the use of two keys, a public key and a private key. Messages can be encrypted by the use of one of them and decrypted by the use of another one. In contrast with single key technologies, this technology is much more secure although it operates more slowly. No single computer is capable to decode such a message within a period of thousands of years; nevertheless several thousand computers linked together over the Internet can successfully accomplish it in a night.[53]

Asymmetric cryptography also provides mechanisms for digital signatures, which establish with high confidence (under the assumption that the relevant private key has not been compromised in any way) that the message received was sent by the claimed sender. In law, such signatures are accepted as the digital equivalent of physical signatures on paper documents. In a technical sense, they are not as there is no physical contact or connection

[51] Ian Lloyd, ‘Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures’, LAW & THE INTERNET regulating cyberspace, edited by Lilian Edwards and Charlotte Waelde, ‘HART’ publishing, Oxford, 1997, 143.

[52] Ian J Lloyd “Information Technology Law”, third edition, Butterworths, London, Edinburgh, Dublin, 2000, 581.

[53] Ian Lloyd, ‘Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures’, LAW & THE INTERNET regulating cyberspace, edited by Lilian Edwards and Charlotte Waelde, ‘HART’ publishing, Oxford, 1997, 143.

between the 'signer' and the 'signed'. Properly used high quality designs and implementations are capable of a very high degree of assurance, even exceeding the most careful physical signature.[54]

Public-key cryptography aids to establish a secure line of communication with anyone using a compatible decryption program or other device. Sender and receiver need not a secure way to agree on a shared key anymore.[55]

A modified form of public key cryptography, still based on the RSA algorithms but which can be used on personal computers, was developed by Phil Zimmerman and is known as PGP (Pretty Good Privacy).[56]

There exist so called ‘strong’ (which cannot be cracked in a sufficiently short time, even using the most powerful computers available for the task) and ‘weak’ (which represents a significant risk as the key can be discovered by an organization that has access to sufficient computing power) encryption schemes. There are several aspects of a scheme that determine its strength. One of particular importance is the key-length needed to make it highly unlikely that a cracking attempt will be successful.[57]

There are various levels of encryption; the higher the ‘bits’, the greater the protection. Currently 256-bit encryption is a commonly used standard. Supersensitive documents will usually require higher levels. The information is decrypted by the use of a ‘key’. The key is

[54] http://www.infothis.com:80/find/Cryptography/

[55] Michael Froomkin “The Essential Role of Trusted Third Parties in Electronic Commerce”, Published at 75 Oregon L. Rev. 49 (1996), http://osaka.law.miami.edu/~froomkin/articles/trusted.htm

[56] Ian J Lloyd “Information Technology Law”, third edition, Butterworths, London, Edinburgh, Dublin, 2000, 582.

[57] Roger Clarke “Message Transmission Security (or ‘Cryptography in Plain Text’)”, version of 11 May 1998 at http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html, Earlier version published in Privacy Law & Policy Reporter 3, 2 (May 1996), pp. 24-27

often a passcode or another software program bound to the original encryption software. The danger is obvious, the loss of the key effectively 'loses' the document.[58]

In cryptography, the key length is a measure of the number of possible keys which can be used in a cipher. Because of the use of binary keys in modern cryptography, the length is usually specified in bits. The preferred numbers commonly used as key sizes (in bits) 'are powers of two, potentially multiplied with a small odd integer'. A key should be large enough to make a brute force attack infeasible, as it would take too long to execute. For many years the limit was 40-bit encryption. A key length of 40 bits offers little protection today against an ordinary attacker with a single computer. There are still a number of restrictions relating the export of some cryptographic products, but the limit was effectively raised to 128-bit key lengths in the end of millennium. When the DES cipher was released in 1977, a key length of 56 bits was thought to be sufficient so as to limit the 'strength' of encryption available to non-US users, but today even 56 bits is considered to be insufficient length for symmetric algorithm keys. DES has been replaced in many applications by triple DES or 3DES, which has 112-bit keys. The Advanced Encryption Standard published in 2001 uses a key size of (at minimum) 128 bits. It also can use keys up to 256 bits. 128 bits is currently thought, by many observers, to be sufficient for the foreseeable future for symmetric algorithms. [59]

To make a brute force search infeasible against asymmetric algorithm keys, there must be sufficient numbers of possible keys. The asymmetric algorithm keys must be longer for equivalent resistance to such attacks than symmetric algorithm keys. As of 2002, a key length of 1024 bits was generally considered the minimum necessary for the RSA encryption

[58] Ellen Freedman, Reid Trautz, Jim Calloway "THE LAWYER'S GUIDE TO MOBILE COMPUTER SECURITY" published in Pennsylvania Lawyer March/April, 2007, available at http://international.westlaw.com/welcome/WorldJournals/default.wl?fn=_top&rs=WLI

[59] http://www.infothis.com/find/Key_size/

algorithm. Since 2003 RSA Security has claimed that 1024-bit RSA keys are equivalent in strength to 80-bit symmetric keys, 2048-bit RSA keys to 112-bit symmetric keys and 3072-bit RSA keys to 128-bit symmetric keys.[60]

Encryption has a long and questionable history, burying governments concerned with the security of information against technological libertarians, businesses, and privacy groups pushing for more open systems of encryption use and commerce, particularly in the international arena. By the 2000s potentials of e-commerce gradually convinced governments to relax restrictions on the sale and export of encryption technologies. As a result, encryption was moving to its expected place as a key element in the development of e-commerce, finding increasing distinction in online transactions by way of digital certificates and digital signatures.[61]

1.4 Definition, meaning, legal effects of digital signatures

A digital signature is “a digital code that can be attached to an electronically transmitted message that uniquely identifies the sender.”[62]

A digital signature, properly defined, is the result of encoding and decoding information through an encryption method known as public-key cryptography. Nevertheless, many documents and legislative products use the terms ‘digital’ and ‘electronic’ signatures as synonyms.[63]

The International Standards Organization defines the concept of a digital signature as

[60] http://www.infothis.com/find/Key_size/

[61] Free Encyclopedia of Ecommerce, “Encryption – Popular Encryption Technologies, Cutting-edge Encryption Schemes, Encryption in the E-commerce Arena.”, http://ecommerce.hostip.info/pages/416/Encryption.html

[62] http://www.webopedia.com/TERM/D/digital_signature.html

[63] Jonathan D. Hart, “Law of the web, a field guide to internet” publishing 2003 edition, Bradford Publishing Company, Denver, Colorado, 203.

‘data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.’

Most of the legislative acts use technology-neutral language and do not define the term ‘digital signature’ directly. EU Electronic Signature Directive[64], for example, speaks in art.2 about ‘advanced electronic signature’ that absolutely corresponds by definition to digital signature. It is an electronic signature which meets the following four requirements:

1. uniquely linked to the signatory;

2. capable of identifying the signatory;

3. created using means that signatory can maintain under his sole control; and

4. linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

In practice, the requirements described above can be met only in electronic signatures which are based on the use of public key cryptography. These are digital signatures or any other new technique that can be developed in future. That justifies the use of technologically-neutral language by the legislators, as the technology is developing day by day and there will be no need for legislature adoption with the creation of new methods.

The term ‘digital signature’ is more commonly used when the text of a data message is encrypted in such a manner that a recipient can be confident about the certain sender of it and the fact that there was no modification or amendment of it during the course of transmission.[65]

Digital signatures are created and verified by cryptography, particularly, by so called

[64] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities, http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

[65] Ian Lloyd, ‘Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures’, LAW & THE INTERNET regulating cyberspace, edited by Lilian Edwards and Charlotte Waelde, ‘HART’ publishing, Oxford, 1997, 142.

‘public key cryptography’, which involves an algorithm using two different but mathematically related ‘keys’; one for creating and another for verifying a digital signature. The first one transforms data into hidden form and the latter returns it to the original form. This system is collectively termed an ‘asymmetric cryptosystem’. The key used to create the digital signature is called private key and is known only to the signer. Obviously, the holder of the private key may publish it or lose control of it and as a result make a forgery possible. The problem can be solved by high degree of care in safekeeping, disassociation of the subscriber from the key by revoking his certificate and publishing it in ‘certificate revocation list’ and by a use of a variety of other methods.[66] The key that is usually more widespread and used by relying parties to verify the digital signature is called public key. Although the keys are mathematically related, it is computationally infeasible to get the private key knowing the public one. This is sometimes called the principle of ‘irreversibility’.[67]

In essence, the key issues for data which have been signed electronically are whether those data have been altered between their being signed and being read or received by the intended recipient and whether those data were actually signed by the person by whom the data purport to have been signed or whether the signature attached to them is forged in some way.[68] Digital signature is a way to solve these issues.

Another fundamental process which is used in both creating and verifying a digital signature is a so called ‘hash function’. A hash function is represented by an algorithm which creates a digital ‘fingerprint’ in the form of a ‘hash value’ or ‘hash result’. It has usually

[66] Christopher Reed ‘Internet Law: Text and Materials’, Butterworths, London, Edinburgh, Dublin, 2000, 162.
[67] American Bar Association ‘Digital Signature Guideline Tutorial’, http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html
[68] Mark Taylor “USES OF ENCRYPTION: DIGITAL SIGNATURES”, published in Computer and Telecommunications Law Review 2006, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?blinkedcitelis

standard length much smaller than the message, which is however substantially unique to it. Any change of the message is detectable as it creates a different hash result.[69] Thus, the hash result can be utilized as a "test" of whether even one bit of information in a record has been changed. This is the key to the new evidentiary scheme: which have a built-in, logical test for authenticity.[70]

The most common example to illustrate the process is an example of Alice and Bob. To sign a message to Bob, Alice would use her own private key in producing the signature.[71] The private key is used to encrypt the data known as the 'message digest', which is like the fingerprint of the message. Hence, the digital signature has two characteristics similar to those of a handwritten signature: its uniqueness to the subscriber, as her private key has been used and its difference from others at each use, as it depends upon the message. Using another private key, say Bob's, to sign the same document would produce a different signature. As the signature was encrypted using Alice's private key, it can be decrypted by the use of her public key, which is not confidential. The message itself should not be necessarily confidential either: to encrypt a message and digitally sign one, are two entirely separate functions. Digital signatures derive some unique qualities from this complexity: they cannot be copied, as they would be incorrect cut-and-pasted into another message; it would be entirely different numbers from the ones produced during the original signing. It can be checked: Bob can decrypt the Alice's message using her public key and, as a result, will have a string of data which is the

[69] Mark Taylor "USES OF ENCRYPTION: DIGITAL SIGNATURES", published in Computer and Telecommunications Law Review 2006, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?blinkedcitelis

[70] George L. Paul, "The "Authenticity Crisis" In Real Evidence", http://www.lewisroca.com/uploads/The%20Authenticity%20Crisis%20In%20Real%20Evidence.pdf

[71] Caspar Bowden and Yaman Akdeniz "Privacy II: Cryptography and Democracy – Dilemmas of Freedom", "Liberating Cyberspace, Civil Liberties, Human Rights and the Internet" edited by Liberty (The National Council for Civil Liberties), Pluto Press, London – Sterling, Virginia, USA, 1999, 87.

message digest of the message Alice signed. He can calculate the message digest for the Alice's message and compare it with the one he has, if they match, he can be sure that the message was signed by the use of Alice's private key and has not been changed in transit. If the two message digests are not the same, then the message does not originate from Alice or it was sent by Alice but was changed in transit. The only way to check it is to telephone Alice.[72]

Hence, there are two processes involved in the use of digital signatures. These are digital signature creation which is performed by the signer and digital signature verification performed by the receiver of the digital signature. The former uses the hash result obtained from and unique to the signed message as well as a given private key. The latter checks the digital signature by reference to the original message and a given public key, in order to determine whether the digital signature was created for that same message using the private key that matches the referenced public key.[73]

There are a few main legal purposes which the processes of creating and verifying a digital signature are for:

1. signer authentication;
2. message authentication;
3. affirmative act;
4. efficiency.[74]

Digital signatures are used to ensure secure electronic communications through a three-party system, involving the message sender, recipient and a certification authority. The full potential of digital signatures in electronic commerce may not be realized until reasonably

[72] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 52.

[73] Christopher Reed 'Internet Law: Text and Materials', Butterworths, London, Edinburgh, Dublin, 2000, 163.

[74] American Bar Association 'Digital Signature Guideline Tutorial', available at http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

uniform rules governing the rights, obligations and liabilities of each of the three parties are established. In 1996, the American Bar Association published "Digital Signature Guidelines[75]: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce." This document is the first set of legal guidelines for cryptology, electronic signatures and authentication over open networks like the Internet.[76]

Digital signature schemes have several prior requirements without which such a signature will mean nothing, whatever the cryptographic theory or legal provision:

1) quality algorithms - some public key algorithms are known to be insecure, practicable attacks against them having been identified;

2) quality implementations - an implementation of a cryptographic algorithm with mistakes will not work;

3) the private key must remain actually secret;

4) distribution of public keys must be done in such a way that the public key claimed to belong to Bob actually belongs to Bob, and vice versa;

5) users (and their software) must carry out the signature protocol properly.[77]

While most of the scholars are debating how to regulate the use and consequences of digital signatures better, some of them insist that the laws and regulations on digital signatures are ‘a mistake’, arguing that digital signatures are not signatures, and they cannot fulfill the promises of legislators. Understanding why requires understanding how they work. The math is complex, but the mechanics are simple. Mathematical calculations are used to encrypt and decrypt a message. Consequently, the result of these calculations is called a ‘signature’. While

[75] American Bar Association ‘Digital Signature Guideline Tutorial’, available at http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

[76] James Hill “Lock and Load: Document security on the Net”, Business Law Today November/December 1998 at http://www.abanet.org/buslaw/blt/8-2lock.html

[77] http://www.infothis.com/find/Digital_signature/

mathematically it works beautifully, semantically it fails miserably. There's nothing in the abovementioned that constitutes signing. In fact, ‘calling whatever Alice creates a "digital signature" was probably the most unfortunate nomenclature mistake in the history of cryptography’.[78] In law, a signature serves to indicate agreement to, or at least acknowledgment of, the document signed. When a judge sees a paper document signed by Alice, he knows that Alice held the document in her hands, and has reason to believe that Alice read and agreed to the words on the document. The signature provides evidence of Alice's intentions. When the same judge sees a digital signature, he doesn't know anything about Alice's intentions. He doesn't know if Alice agreed to the document, or even if she ever saw it. The mathematics of cryptography cannot bridge the gap between a person and a computer, as the computer is not trusted. Digital signatures prove, mathematically, that a private key was present in a computer at the time Alice's signature was calculated. It is a small step from that to assume that Alice entered that key into the computer at the time of signing. But it is a much larger step to assume that Alice intended a particular document to be signed. And without a tamperproof computer trusted by Alice, you can expect "digital signature experts" to show up in court contesting a lot of digital signatures.[79]

I disagree with this purely technical approach to the digital signatures, and agree with most of the scholars and legislators in a view that as long as the digital signature in the e-commerce satisfies such functions as to identify a person and to associate that person with the content of a document as well as to provide certainty as to the personal involvement of that person in the act of signing, it constitutes an equivalent of paper-based signatures in the real world transactions.

[78] Bruce Schneier, “Why Digital Signatures Are Not Signatures”, http://www.schneier.com/crypto-gram-0011.html

[79] Ibid.

Digital signature laws provide for various technological requirements in different parts of the world. Legislation has been enacted in several jurisdictions, which either recognizes or regulates the use of digital signatures. Nevertheless, the approaches taken regarding the legal and technical issues differ in each jurisdiction. While some countries focus on only the technical standards, others have covered variety of issues, including the establishment of a regulatory agency whose function is to supervise certificate authorities, which have different requirements in various jurisdictions. The only solution to this dilemma is the enactment of a globally recognized scheme for digital signatures. Such a scheme could replace conflicting rules and provide legislation where none exist. To promote growth in international e-commerce transactions, adequate clarity and guidance for the use of digital signatures is needed.[80]

[80] Alcolya J. L. Lester "THE DIGITAL SIGNATURE: THE NEXT STEP IN ITS EVOLUTION" published in ILSA Journal of International and Comparative Law Fall, 2000, Cyber-International Law Notes & Comments, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

Chapter 2 - International initiatives relating to electronic signatures

Over the past few years, a number of various materials concerning the problems of authentication, non-repudiation and integrity of electronic messages in the context of electronic commerce have been produced by different international organizations. The majority of these international instruments are recommendations or guidance only. European Union's Electronic Signature Directive is the only legally binding one; nevertheless, it is limited in its effect to the EU Member States. On the contrary, initiatives of the United Nations Commission on International Trade Law (UNCITRAL), the Organisation for Economic Co-operation and Development (OECD), and International Chamber of Commerce (ICC) may lack legal authority, however, they possess a significant persuasive effect among a much broader international community.[81] Initiatives of UNCITRAL and European Union as well as the ones of the other side of Atlantics and comparison between them will be provided in details below in this chapter.

OECD Ministerial Declaration on Authentication for Electronic Commerce

Subsequent to the OECD Ottawa Conference on "A Borderless World: realizing the potential of global electronic commerce" of 1998 the Ministers of the OECD member countries made a declaration intended to cover a number of electronic authentication issues. Adopting from other countries a non-discriminatory approach to electronic authentication is among the most significant ones. Moreover, they also declared the intention to foster authentication technologies and mechanisms development efforts and facilitate the use of those ones for electronic commerce, amend specific legal requirements that can hinder the use of electronic authentication mechanisms as well as continue an international work of global electronic

[81] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 72.

commerce facilitation.[82]

The following principles are established by OECD in order to realize the abovementioned intentions:

- Trust in cryptographic methods;
- Choice of cryptographic methods;
- Market driven development of cryptographic methods;
- Technical standards for cryptographic methods developed at a national and international level;
- Protection of privacy and personal data;
- Lawful access to encrypted data;
- Contractual or legislative liability of the Cryptography Service Providers (CSPs);
- International co-operation on cryptography policies.[83]

The Declaration is a significant international instrument in a global consensus on electronic signatures building, particularly in its non-discriminatory approach to overseas forms of electronic authentication, which is intended to be a main cross-border transactions contributor in the electronic signatures use, since OECD membership include not only European countries, among which are Switzerland, Iceland and Norway, but also such countries as Turkey, Japan, South Korea, Australia, Canada and the United States.[84]

[82] THE OECD DECLARATION AND DECISIONS ON INTERNATIONAL INVESTMENT AND MULTINATIONAL ENTERPRISES: BASIC TEXTS, available at http://www.olis.oecd.org/olis/2000doc.nsf/4f7adc214b91a685c12569fa005d0ee7/c125692700623b74c1256991003b5147/$FILE/00085743.PDF

[83] Christina Spyrelli "Electronic Signatures: A Transatlantic Bridge? – An EU and US Legal Approach Towards Electronic Authentication", published in "Journal of Information, Law and Technology", 16 August 2002, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/

[84] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 87.

Following the Declaration the OECD's Working Party for Information Security and Privacy made a survey in 2001 aimed to assess the progress of four-year implementation in member states, which did not find any country which had an express policy of discrimination against foreign authentication. The study also reviewed the authentication technologies application by Members' governments in delivery of government services. All responded countries have had some activities, such as tax or VAT services being delivered electronically, in this direction. Introduction of such services is hoped to encourage increased use of electronic signatures in the private sector as well.[85]

ICC General Usage for Internationally Digitally Ensured Commerce

The General Usage for International Digitally Ensured Commerce (GUIDEC) has been drafted by the International Chamber of Commerce (ICC) Information Security Working Party, first version of which was published in November 1997 as part of the ICC's Electronic Commerce Project. The project is an international, multidisciplinary initiative to study, facilitate and promote the emerging global electronic trading system, which gathers leading corporations and industry associations, government representatives and lawyers, as well as specialists of information technology world-wide to focus on central issues in digital commerce.[86] The second version adopted in October 2001 retains most of the issues covered by the previous one but goes further in the application field and includes a few new definitions and best practices. Among the covered issues are the rights and responsibilities of subscribers, certifiers and relying parties. The principal concern is directed to the use of digital signatures, but the other technologies are included as well.

[85] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 87.

[86] ICC General Usage for International Digitally Ensured Commerce, Preface, available at http://www.iccwbo.org/home/guidec/guidec.asp

The GUIDEC is aimed only at international business transactions, thus the goal of it is 'to enhance the ability of the international business to execute trustworthy digital transactions utilizing legal principles that promote reliable digital authentication and certification practices.'[87]

The proposed best practices are divided into two parts: authenticating a messages and certification. With regard to authentication, it imputes loss resulting from a forgery of a digital signature or change of a document which happened because of the purported signatory's failure to safeguard their key or otherwise. A signatory using a device to sign has to exercise as a minimum reasonable care to obviate its unauthorized use.[88] A certifier has to inform the relying parties about the verified or unverified information and 'must confirm the accuracy of all material facts set forth in a valid certificate, unless it is evident from the certificate itself that some of the information has not been verified.'[89] Moreover obligations of a certifier include 'use only technologically reliable information systems and processes, and trustworthy personnel in issuing a certificate and in suspending or revoking a public key certificate and in safeguarding its private key, if any; have no conflict of interest which would make the certifier untrustworthy in issuing, suspending, and revoking a certificate; refrain from contributing to a breach of a duty by the subscriber; refrain from acts or omissions which significantly impair reasonable and foreseeable reliance on a valid certificate; act in a trustworthy manner towards a subscriber and persons who rely on a valid certificate.'[90]

[87] ICC General Usage for International Digitally Ensured Commerce (version II), Preface, available at http://www.internetpolicy.net/e-commerce/guidec2001.pdf

[88] Ibid, Glossary.

[89] Ibid.

[90] Ibid.

Although the GUIDEC has no legal impact in any country, it is expected that a reasonable businessman will follow the set of established practices in it by the most senior international business forum.[91]

It can be followed from the analysis of various regulatory initiatives that most of them reflect different assumptions on e-signatures legal status and future. Variety of these views can be classified into the following categories:

1) The Minimalist Approach**,** which is adopted by the USA, is directed to uniform the use, recognition and enforceability of electronic records and electronic signatures by establishing a technologically neutral status, removing existing legal barriers from the e-commerce and by avoiding new regulations. The UNCITRAL Model Law on Electronic Commerce[92] is one of the most manifest minimalist approach examples. OECD[93] shares the same minimalist view as the UNCITRAL.

2) The Digital Signature Approach focuses only on the establishment of a legal framework for the digital signatures operation, which includes adoption of the PKI as the approved technology of generating electronic signatures, imposition of specified requirements on C.As, prescription of the key holders liability as well as definition of justified reliance on electronic signature circumstances. Examples include ABA-Digital Signature Guidelines[94] and

[91] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 86.

[92] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, art. 6, available at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

[93] THE OECD DECLARATION AND DECISIONS ON INTERNATIONAL INVESTMENT AND MULTINATIONAL ENTERPRISES: BASIC TEXTS, available at http://www.olis.oecd.org/olis/2000doc.nsf/4f7adc214b91a685c12569fa005d0ee7/c125692700623b74c1256991003b5147/$FILE/00085743.PDF

[94] American Bar Association 'Digital Signature Guideline Tutorial', http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

EU-wide standardization initiative (EESSI)[95].

3) The Two-tier Approach is a 'hybrid' method, which is adopted by the EU, setting requirements for electronic authentication methods with a certain minimum legal power (minimalist approach) and attributing greater legal effect to certain widely used techniques (digital signature approach). The UNCITRAL Model Law on Electronic Signatures[96] is as example of such a 'hybrid' approach.[97]

While digital signature and the two-tier approaches provide more legal certainty and security, but nevertheless still focus too narrowly on signatures as such, and not on formal requirements as a whole, the minimalist approach gives the opportunity for a uniform legislation on electronic signatures based on internationally harmonized criteria to develop, as it focuses on the functions of signatures and the methods in which these functions can be translated into technological applications keeping a technological neutrality.[98]

[95] Framework for EESSI Standards and Classes for Electronic Signatures, available at http://www.ictsb.org/EESSI/Documents/EESSI-ITEMA-v2.0.doc

[96] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, available at http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

[97] Christina Spyrelli "Electronic Signatures: A Transatlantic Bridge? – An EU and US Legal Approach Towards Electronic Authentication", published in "Journal of Information, Law and Technology", 16 August 2002, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/

[98] Ibid.

2.1 UNCITRAL Model Laws

The United Nations Commission on International Trade Law (UNCITRAL) is a body of the United Nations which develops legislative texts in the area of international trade law. The majority of the texts are not binding on any state, but rather represent a part of a process of gradual harmonization of laws. Harmonization at a global level is at the core of the Model Law. In order to achieve the national legislative objectives, States can choose to adopt a Model Law, 'that is, recommendations made by a body composed of government representatives and experts such as practitioners, and academics'[99], entirely or in part and modify its elements as they see fit.[100]

Model Law on Electronic Commerce

In 1996, the Commission, after several years of discussions by the Working Group on Electronic Commerce, adopted the UNCITRAL Model Law on Electronic Commerce at the 29th session of it. The main purpose was to offer national legislators a set of rules acceptable by international community and to show the way of creating a secure legal environment for electronic commerce. One of the debatable questions was the form of the contract.[101]

The terminology, which is used in the Model Law, is open and broad. Thus, the UNCITRAL aims at providing a Model Law, which is acceptable for countries with different legal systems, by leaving room for variation, while ensuring that some barriers to electronic commerce can be effectively removed.[102]

Provisions of the Model Law are technology neutral, and it has functional equivalent

[99] Indira Carr "UNCITRAL & Electronic Signatures: A Light Touch at Harmonisation", available at http://perseus.herts.ac.uk/uhinfo/library/u81985_3.pdf

[100] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 73.

[101] Ibid.

[102] Babette Aalberts and Simone van der Hof "Digital Signature Blindness", available a t http://www.buscalegis.ufsc.br/arquivos/Digsigbl.pdf

approach to such formal requirements as that a document must be in writing or signed. Consequently, Article 5 declares that "information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message."[103] Definition of 'data message' is provided by Article 2, which specifies it 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."[104]

The Model Law on Electronic Commerce 1996 as amended 1998 has received world-wide success. A number of countries from different parts of the world have based their legislation on the Model Law. There are such countries as Australia, Bermuda, Colombia, France, Hong Kong Special Administrative Region of China, India, Ireland, Philippines, Republic of Korea, Singapore and Slovenia among them.[105] The issue of signatures on electronic documents was addressed by Article 7 of the Model Law on Electronic Commerce which provides that:

> (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
>
> (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
>
> (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
>
> (2) Paragraph (1) applies where the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.[106]

This article recognizes certain functions of a paper-based signature such as to identify a person and to associate that person with the content of a document as well as to provide certainty as to the personal involvement of that person in the act of signing. The objective

[103] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, Art.5, available at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

[104] Ibid, Art.2.

[105] Indira Carr "UNCITRAL & Electronic Signatures: A Light Touch at Harmonisation", available at http://perseus.herts.ac.uk/uhinfo/library/u81985_3.pdf

[106] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, Art.7, available at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

included establishing general conditions of message authentication and electronic signature enforceability.[107]

The Model Law on Electronic Commerce also deals with such aspects of contract formation as offer, acceptance, time of sending or time of receipt of data messages and so on. The Model Law provides for expression of offer or acceptance by means of data messages, and the recipient of a data message is not permitted to deny legal effectiveness of it solely on the grounds of its electronic form. One of the most important provisions to be mentioned is Article 13 that deals with the attribution of data messages, which provides that ‘a data message is that of the originator if it was sent by the originator itself.’ The originator is defined as ‘a person by whom or on whose behalf the data message purports to have been sent or generated prior to storage’, but it does not include a person acting as an intermediary. A data message is deemed to be that of the originator if it was sent by a person who had the authority to act on behalf of the originator in respect of that data message or by an information system programmed by, or on behalf of, the originator to operate automatically. Article 13.3 states in addition that ‘an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose or the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.’[108]

[107] Lorna Brazell “Electronic Signatures Law and Regulation”, first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 73.

[108] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, Art.13, http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

The latter provision creates some ambiguity, as the only method to be used by an originator to identify data messages as its own is a digital signature, generated by a private key stored on the originator's computer system. A number of persons can have an access to this system, but only a limited number of them will in fact be authorized to send data messages on behalf of originator. In these cases, the recipient of that data message can assume that it comes from the originator and act in fact on behalf of unauthorized message.[109]

The article further deals with the issues of reasonable care exercising, transmission errors and data duplicates.

The Model Law on Electronic Commerce however did not deal with issues such as reliability, certification processes, the liability issues of the various parties involved in the creation and use of electronic signatures. Thus the drafting of the Model Law on Electronic Signatures came onto the stage.[110]

Model Law on Electronic Signatures

On July 5, 2001 the Model Law on Electronic Signatures was approved by UNCITRAL. It was mainly influenced by the American Bar Association Guidelines on Digital Signatures,[111] the variety of legislative acts on electronic signatures of the United States, and the European Directive on Electronic Signatures.[112]

Despite its name, the Model Law on Electronic Signatures is in reality based on a technology of the public key cryptography use, in other words, it deals mainly with the use of

[109] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 76.

[110] Indira Carr "UNCITRAL & Electronic Signatures: A Light Touch at Harmonisation", available at http://perseus.herts.ac.uk/uhinfo/library/u81985_3.pdf

[111] American Bar Association 'Digital Signature Guideline Tutorial', http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

[112] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities, http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

digital signatures. Although this restricted approach was a topic of debates in the drafting process, it has been justified by the increasing dominance of digital signatures in the market at the time. The main purpose of the Model Law is to 'lay down practical standards against which the technical reliability of electronic signatures can be measured.' Thus, it can be accepted as a supplement to Article 7 of the Model Law on Electronic Commerce.[113]

Although the Model Law provides a workable framework, it is by no means comprehensive; as it leaves many core legal issues such as the type and levels of liability, for example, to be worked out by the state adopting the Model Law.[114]

The Model Law preserves party autonomy principle, since it is not mandatory in character and provides for variation by agreement subject to any limitations that may be imposed by the applicable law such as public policy grounds, which is provided by Article 5. Moreover, Article 3 provides for the central principle of technology neutrality.

The UNCITRAL adopts a 'functional equivalence' approach in drafting its legislation, that 'extrapolates the functions of a paper document to create the criteria that need to be met by the paperless document for attaining a status equivalent to that of the paper document', which is applied for formulating both the Model Law for Electronic Commerce and Electronic Signatures. To ensure consistency between the Model Laws, the basic articles such as scope, definition and interpretation have been repeated. Therefore, Article 2(a) defines electronic signature as "data in an electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation the data message and indicate the signatory's approval of information contained in the data message". Data message refers to

[113] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 77.
[114] Indira Carr "UNCITRAL & Electronic Signatures: A Light Touch at Harmonisation", available at http://perseus.herts.ac.uk/uhinfo/library/u81985_3.pdf

information that is sent, generated, received or stored by electronic, optical or similar means. It includes, but is not limited to electronic data interchange (EDI), electronic mail, telegram, telex or telecopy. The definition of electronic signature is broad and does not indicate any specific technology. The electronic signature could be a digital signature, a digitized image of a handwritten signature and so on. In order to provide electronic signature with legal effectiveness, the Model Law requires electronic signatures meet the reliability requirements in the light of all the circumstances including any agreement there might be between the parties.[115]

The UNCITRAL anticipates three parties that take part in the use and creation of an electronic signature: the signatory[116], the third party (known as the certificate service provider[117]) and the party who relies on the electronic signature.[118]

Unlike other recent legislation on electronic signatures, such as EU Directive on Electronic Signatures’ for example, which provides liability only for the certification service providers (Article 6), the Model Law imposes responsibilities on all three actors engaged in the use and creation of an electronic signature that has legal effect.[119]

According to Article 8, the signatory, as the holder of a signature creation device, is expected to exercise reasonable care to avoid its unauthorized use. An objective basis determines the issue of reasonable care exercise. Similarly, the certification service provider

[115] Indira Carr “UNCITRAL & Electronic Signatures: A Light Touch at Harmonisation”, available at http://perseus.herts.ac.uk/uhinfo/library/u81985_3.pdf

[116] Defined in Article 2(d) as “a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents”.

[117] Defined in Article 2(e) as “a person that issues certificates and may provide other services related to electronic signatures”.

[118] Defined in Art 2(b) as “a data message or other record confirming the link between a signatory and signature creation data”.

[119] Indira Carr “UNCITRAL & Electronic Signatures: A Light Touch at Harmonisation”, available at http://perseus.herts.ac.uk/uhinfo/library/u81985_3.pdf

has to meet a list of obligations under the provisions of Article 9. The list includes such obligations as to adhere to representations made in its policy statements, to exercise reasonable care to ensure accuracy of information included in the certificate during its life cycle, to make available to the relying party information that would be relevant to a particular certificate, ensure availability of a notification system to the signatory which the signatory can use where the signature creation data has been compromised and others. The article provides only for the minimum requirements as to the content of information in the certificate and information which may either be included in the certificate or made available elsewhere.[120]

Article 10 deals with the issue of trustworthiness. It has broad interpretation, and provides for such factors as financial resources, quality of hardware and software, extent of audit by an independent body, accreditation of the certification service provider to be taken into consideration in establishing whether the requirement of trustworthiness is met.[121]

As for the relying party, he is obliged under Article 11(a) to verify the reliability of an electronic signature. The notion is so broad as can in some circumstances include the certification service provider and even a signatory. A relying party, even if it is a consumer, is expected to take reasonable steps to verify the reliability of electronic signatures.[122]

Envisaging of legal consequences in the event of a breach is left open to be determined by the national law. Legal consequences could be criminal or civil liability, and the nature of liability could, for example, be fines or damages. This introduces the element of uncertainty in the promotion of cross border recognition of certificates and electronic signatures by the

[120] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 81.

[121] Indira Carr "UNCITRAL & Electronic Signatures: A Light Touch at Harmonisation", available at http://perseus.herts.ac.uk/uhinfo/library/u81985_3.pdf

[122] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 80.

Model Law.[123]

Following the principle of non-discrimination, the geographic location of the electronic signature creation or of an issuance of the certificate will play no role in determination of legal effectiveness of the certificate or electronic signature. What will affect its effectiveness is the level of reliability, which may vary from state to state. The Model Law adopts ‘equivalence’ rather than ‘identical’ as a measure.[124]

National laws implementing the Model Law have not been compatible in certification service providers’ or foreign-based certificates’ treatment in spite of the realization the criticality of international recognition by most of the countries.[125]

2.2 EU Electronic Signature Directive

The first steps taken by the Community towards regulating electronic signatures were represented by the Commission Communication in 1997, A *European Initiative in Electronic Commerce*. It was followed by the Commission Communication, *Towards a European Framework for Digital Signatures and Encryption,* and afterward its *Proposal for a European Parliament and Council Directive on a common framework for electronic signatures* (“the draft Directive”).[126]

As soon as the first draft national legislation on digital signatures was introduced in some EU Member States and approved in Germany and Italy during the year of 1997, the European Commission started seriously worry about the effects of these legislative initiatives

[123] Indira Carr “UNCITRAL & Electronic Signatures: A Light Touch at Harmonisation”, available at http://perseus.herts.ac.uk/uhinfo/library/u81985_3.pdf
[124] Ibid.
[125] Lorna Brazell “Electronic Signatures Law and Regulation”, first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 84.
[126] John Dickie, “Internet and Electronic Commerce Law in the European Union”, ‘Hart’ Publishing, Oxford – Portland Oregon, 1999, 36.

onto the internal market.[127] The possibility that other Member States would follow their progressive neighbors and introduce their own legislative acts regulating digital signatures and encryption which would be potentially disparate and lead to subsequent barrier to the internal market's proper functioning, motivated European legislators to adopt the regulation covering the whole area at Community level.[128] Consequently the European Commission started to draft a proposal for the Directive which was followed by issuance of the European Parliament's opinion in first reading about it on 13 January 1999 and later by nearly the same position taken by the Council in its opinion issued on 22 April 1999. The second reading's recommendations were issued by the European Parliament on 14 October 1999 and finally on 13 December 1999 the Directive[129] was signed and published in the Official Journal of 19 January 2000. Article 13 of the Directive has given Member States 18 months till 19 July 2001 for implementation, to 'bring into force the laws, regulations and administrative provisions necessary to comply with the Directive'.

The purpose of the Directive according to Art.1 (Scope) is 'to facilitate the use of electronic signatures and to contribute to their legal recognition' as well as to establish 'a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market'; the article refers to the dual objective of the Directive. The Directive does not cover an overall regulation or the issue of legal recognition of electronic signatures entirely, it only wants to 'facilitate' their use and 'to contribute' to their

[127] Jos Dumortier 'Directive 1999/93/EC on a Community framework for electronic signatures', "eDirectives: Guide to European Union law on E-Commerce" – Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection, edited by Arno R. Lodder and Henrik W.K. Kaspersen, Kluwer Law International, The Hague/London/New York, 2002, 36-37.

[128] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 87.

[129] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities, http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

legal recognition. As to the establishment of a legal framework, it was a European reaction against the legislative acts in some Member Stated, particularly in Germany and Italy, introduced in this area because the main goal of the Community is to avoid incompatible national laws and to create a common European legal framework.[130]

Before the draft Directive was issued in May 1998, all the related documents contained the term ‘digital signature’; however after its issuance the European Commission replaced it with ‘electronic’ signature.[131] As a result, the digital signature term did not appeared in the text of the Directive and the Art.2 (Definitions) describes only the terms an ‘electronic signature’ and an ‘advanced electronic signature’, which is basically referred to digital signatures. The detailed explanation of these definitions is given in the previous chapter, correspondingly in sections related to electronic and digital signatures.

The following two definitions of Art.2 are also of great importance: certificate, that means ‘an electronic attestation which links signature-verification data to a person and confirms the identity of that person’ and certification-service-provider described as ‘an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures’. Requirements for qualified certificates are given in Annex I of the Directive.

The certification services market

The principle provision concerning certification services is most likely Article 4(1), which provides that ‘each Member State shall apply the national provisions which it adopts

[130] DUMORTIER, J., LIBON, O., MITRAKAS, A., RINDERLE, R., SCHREIBER, A., VAN EECKE, P., (2000) European Electronic Signature Standardization Initiative - Certificate Path Validation , European Commission, 61, at http://www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf?where=

[131] DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G. & VAN EECKE, P. (2003) The Legal and Market Aspects of Electronic Signatures in Europe, Study for the European Commission within the eEurope 2005 framework, at http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide.' Moreover, it states that 'Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.'

Article 4 presents the "country of origin" principle for certification services. "Certification service providers are submitted to rules of the country in which they are established (their 'country of origin')."[132] They do not need to take into account the rules of European countries in which their services are provided. Respect of the rules of the country where they have been established provides their services to be considered in line with the rules of all the Member States in which they operate. [133]

The concept of establishment has been evolved by the European Court of Justice in the context of the freedom and the right of establishment provided by Article 43 of the Treaty of European Community. The Court in *Gebhard*[134] case stated that 'the concept of establishment within the meaning of the Treaty is a very broad one, allowing a Community national to participate, on a stable and continuous basis, in the economic life of a Member State other than his state of origin and to profit there from, so contributing to economic and social interpretation within the Community in the sphere of activities as self-employed persons.'[135] Consequently, the main requirements for an establishment are (1) a stable and permanent establishment, (2)

[132] DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G. & VAN EECKE, P. (2003) The Legal and Market Aspects of Electronic Signatures in Europe, Study for the European Commission within the eEurope 2005 framework. http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

[133] Ibid.

[134] Gebhard v Consiglio dell' Ordine degli Avvocati e Procuratori di Milano (Case C-55/94) [1995] ECR I-4165, para. 25

[135] Jos Dumortier 'Directive 1999/93/EC on a Community framework for electronic signatures', "eDirectives: Guide to European Union law on E-Commerce" – Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection, edited by Arno R. Lodder and Henrik W.K. Kaspersen, Kluwer Law International, The Hague/London/New York, 2002, 45-46.

for an indefinite period, (3) in another Member State than the state of origin, and (4) the actual pursuit of an economic activity.[136]

Any certification-service-provider must be allowed to provide his services without prior authorization. Prior authorization of the provision of certification services is prohibited by the Article 3.1. Recital 10 indicates that '(…) in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorization (…).'

A certification service provider can choose whether to apply for accreditation under any accreditation scheme, private or state, or not. To be accredited, it should be in line with criteria laid down for the scheme. Failure to become accredited, however, cannot be a basis under Article 5.2 for denying legal effectiveness to the signatures supported by certificates it has issued.[137]

Article 3.2 states that 'without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation[138] schemes aiming at enhanced levels of certification-service provision.' Moreover, according to the same article, 'all conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory.'

EU Member States have taken different approaches to the establishment of accreditation schemes. Some countries prefer to set up state controlled accreditation schemes,

[136] Jos Dumortier 'Directive 1999/93/EC on a Community framework for electronic signatures', "eDirectives: Guide to European Union law on E-Commerce" – Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection, edited by Arno R. Lodder and Henrik W.K. Kaspersen, Kluwer Law International, The Hague/London/New York, 2002, 45-46.

[137] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 97.

[138] Voluntary accreditation is defined by Article 2.13 as 'any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification service provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.'

while others choose privately governed ones. The public German accreditation scheme contrives strict conditions which provide an enhanced level of security. The UK scheme represents a non-statutory voluntary approvals regime for trust service providers, although it was originally intended to be a statutory one.[139]

The establishment of different accreditation schemes may be advantageous as well as disadvantageous for certification authorities. It can be problematic from the certification service providers' point of view as the application process for accreditation requires a lot of financial and administrative investment by the applying CA. Moreover, the establishment of various national accreditation schemes opened to all countries' certification service providers would lead to a heightened competition among these schemes.[140]

Article 3.3 states that 'each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.' This article is concerned to be one of the most problematic provisions of the Directive, because it is simultaneously prohibited to demand for prior authorization of the provision of the certification services. Member States have to decide how to provide for the said supervision by other means. Some Member States, such as for example Germany, Austria and Denmark, solve this problem by mandatory requirement of notification by the certification service provider

[139] DUMORTIER, Jos, (2002) 'Directive 1999/93/EC on a Community framework for electronic signatures', Lodder, A.R., Kaspersen, H.W.K.,: eDirectives: Guide to European Union Law on E-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data protection. In de reeks Law and Electronic Commerce, Vol 14, Kluwer Law International,pag. 33-65, at http://www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf?where

[140] Ibid.

established on their territory to the appropriate public authority before starting the provision of services.[141]

Legal effects of electronic signatures (Article 5)

Article 5 is the most disputable provision of the Directive. It establishes two levels of electronic signatures: the ones without qualification, which may or may not have legal effect or be admissible in legal proceedings under the national rules of each Member State and the qualified ones. An electronic signature does not have automatic legal recognition because of being electronic in form. Vice versa, Member States should not deny the legal effect as well as admissibility solely on the grounds that the signature is in electronic form and not an advanced one.[142]

The first part of the article deals with 'qualified electronic signatures' that refer to 'advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device.' According to this article, in all cases, where hand-written signatures in relation to paper document would have been sufficient, Member States should provide for the same status to qualified electronic signatures in relation to electronic data. In other words, the status of hand-written signature in relation to paper documents should be equivalent to the status of qualified electronic signature in relation to electronic data. This is explained by recital 20 as 'advanced electronic signatures which ate based on qualified certificates and which are created by a secure-signature-creation device can be regarded as legally equivalent to handwritten signatures only if the requirements for handwritten signatures are fulfilled.' Moreover, recital 21 adds that 'in order to contribute to

[141] DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G. & VAN EECKE, P. (2003) The Legal and Market Aspects of Electronic Signatures in Europe, Study for the European Commission within the eEurope 2005 framework, at http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf
[142] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 90.

the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States' and 'the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorization of the certification-service-provider involved' as well as 'national law governs the legal spheres in which electronic documents and electronic signatures may be used' and 'this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence.'[143]

Article 5.1(b) specifies that qualified electronic signatures should be admissible as legal evidence in legal proceedings. This provision seems to be excessive, since digital data, including electronic signatures, are acceptable evidence in legal proceedings in all Member States. The value of such evidence is the only variable issue between the Member States. Besides, acceptability of electronic signatures as evidence in legal proceedings is decided by the judge on a case-by-case basis. Recital 21 explicitly refers to the intent of the legislators of the Directive not to affect the role of the judge in such a situation.[144]

Article 5.2 provides that 'Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds' that it (1) is in electronic form, or (2) is not a qualified signature. The effect of the provision is that 'Member States may not draft or maintain regulation, or endorse or authorize

[143] DUMORTIER, Jos, (2002) 'Directive 1999/93/EC on a Community framework for electronic signatures', Lodder, A.R., Kaspersen, H.W.K.,: eDirectives: Guide to European Union Law on E-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data protection. In de reeks Law and Electronic Commerce, Vol 14, Kluwer Law International,pag. 33-65, at http://www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf?where

[144] DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G. & VAN EECKE, P. (2003) The Legal and Market Aspects of Electronic Signatures in Europe, Study for the European Commission within the eEurope 2005 framework, at http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

private rules with a view to condemn the use of an electronic authentication tool solely by virtue of its electronic format or non-qualified nature.'[145]

Liability (Article 6)

Article 6 of the Directive deals with liability provisions for issuers of qualified certificates. According to Article 6.1 and 6.2, a certification service provider 'issuing a qualified certificate to the public or guaranteeing such a certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate', for:

> (a) the accuracy and the completeness of the content of the qualified certificate and of the revocation lists, (b) the assurance about the possession of the private key by the certified signatory at the time of issuance and (c) the correspondence between the private and the public key in cases where the certification service provider generates both of these keys.[146]

Article 6 provides for a minimum liability for CSPs. This means that the Member States can extend the requirements of the Article in their implementation of the Directive, to introduce strict liability for CSPs, for example, or to include also CSPs issuing non-qualified certificates, but they are not permitted to lessen it.[147]

However, Article 6.3 and 6.4 contains some liability limitations that the Member States

[145] Jos Dumortier 'Directive 1999/93/EC on a Community framework for electronic signatures', "eDirectives: Guide to European Union law on E-Commerce" – Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection, edited by Arno R. Lodder and Henrik W.K. Kaspersen, Kluwer Law International, The Hague/London/New York, 2002, 56.

[146] DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G. & VAN EECKE, P. (2003) The Legal and Market Aspects of Electronic Signatures in Europe, Study for the European Commission within the eEurope 2005 framework, at http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

[147] Jos Dumortier 'Directive 1999/93/EC on a Community framework for electronic signatures', "eDirectives: Guide to European Union law on E-Commerce" – Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection, edited by Arno R. Lodder and Henrik W.K. Kaspersen, Kluwer Law International, The Hague/London/New York, 2002, 57.

have to recognize. This part of the Article is considered to be “CSP friendly”. For the application of this provision, a number of conditions have to be fulfilled:

1) the minimum liability provisions of the Directive can only be applied if a certificate has been issued as a qualified certificate. Therefore, it is irrelevant whether the defective certificate is actually qualified or unqualified, decisive is its designation (as “qualified”) by the CSP;

2) the certificate has to be “issued to the public ” or “guaranteed to the public”, the extent of which is open to interpretation. While it can be interpreted differently, it is more reasonable to base it on recital 16 of the Directive which states that “a regulatory framework is not needed for electronic signatures that are exclusively used within systems , which are based on voluntary agreements under private law between a specified number of participants”. The expression ‘’issuing to the public’ can be interpreted as referring to certification services that are open to verifiers that do not have a prior relationship with the CSP.’A CSP can also be held liable for having “guaranteed” a qualified certificate “to the public”; the way in which this type of guarantee should be provided is not clear, but it has to cover at least requirements of first two provisions of the article.[148]

As a result of accordance to requirements of Article 6.1 of the Directive, the CSP has to control whether or not the signatory to whom the certificate is being issued, is also the holder of the private key corresponding to the public key mentioned in the certificate; that can be done, for example, by creating a sample qualified signature which can be verified by the CSP.[149]

[148] DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G. & VAN EECKE, P. (2003) The Legal and Market Aspects of Electronic Signatures in Europe, Study for the European Commission within the eEurope 2005 framework, at http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

[149] DUMORTIER, Jos, (2002) 'Directive 1999/93/EC on a Community framework for electronic signatures',

Liability of CSPs under the Directive requires “reasonable reliance” by the party who suffered the damages. The meaning of a ‘relying party’ creates ambiguity, since recipient of an electronic signature, who relies on certificates when verifying that signature, is undoubtedly included in the meaning of the term, but it is unclear whether a signatory can be referred as a „relying party“ or not.[150] However, some scholars do not agree with common interpretation of this doctrine, which gives to ‘relying party’ the meaning of ‘third party’ and thus excludes the signatory, and argue that a signatory is also a ‘relying party’.[151]

The above-mentioned provisions can be applied to the CSP ‘unless he proves that he has not acted negligently’. This precondition is typical for the relying party situations, as the recipient of a signature, unlike the CSP, usually is not able to analyze the technical issues that can arise. Thus, the burden of proof for negligence is imposed on the CSP.

Article 6.3 and 6.4 of the Directive explicitly provides for a number of liability limitations; these include limitations on the use of qualified certificate and on the value of transactions. A CSP is not liable for damage resulting from these maximum limits being exceeded. The majority of scholars interpret Article 6.4 to permit a relative liability limitation only, which means that only the maximum value per transaction can be limited. Moreover, the Directive specify the possibility to point out a limitation of use of a certificate that the certificate may only be used for a fixed type of transaction, for example, or that it may only be used within the EC, a particular country or even a company. In practice, CSPs frequently

Lodder, A.R., Kaspersen, H.W.K.,: eDirectives: Guide to European Union Law on E-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data protection. In de reeks Law and Electronic Commerce, Vol 14, Kluwer Law International,pag. 33-65, at http://www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf?where

[150] DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G. & VAN EECKE, P. (2003) The Legal and Market Aspects of Electronic Signatures in Europe, Study for the European Commission within the eEurope 2005 framework, at http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

[151] Paolo Balboni “Liability of Certification Service Providers Towards Relying Parties and the Need for a Clear System to Enhance the Level of Trust in Electronic Communication”, available at http://www.eema.org/downloads/member_news/balboni_article.pdf

use a maximum cap for liability for qualified certificates. The maximum cap often indicates a list of services that the CSP may be held liable for.[152]

Unlike the UNCITRAL Model Law or the ICC GUIDEC, the Directive does not regulate the conduct of the signatory or the relying party.[153]

International aspects (Article 7)

It is emphasized in the recitals of the Directive that the development of international electronic commerce need cross-border arrangements with the third country involvement. To ensure it Article 7 of the Directive requires the Member States to ensure 'that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognized as legally equivalent to certificates issued by a certification-service-provider established within the Community if:

(a) the certification-service-provider fulfils the requirements laid down in the Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or

(b) a certification-service-provider established within the Community which fulfils the requirements laid down in the Directive guarantees the certificate; or

(c) the certificate or the certification-service-provider is recognized under a bilateral or multilateral agreement between the Community and third countries or international organizations.'

[152] DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G. & VAN EECKE, P. (2003) The Legal and Market Aspects of Electronic Signatures in Europe, Study for the European Commission within the eEurope 2005 framework, at http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

[153] Lorna Brazell "Electronic Signatures Law and Regulation", first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004, 90.

The first of the conditions to be met in order to obtain legal equivalence for the certificates is not very clear. Unlike their EU-based competitors, third countries CSPs will not be under the scope of one of the national supervisory systems established in the Member States. Hence accreditation is provided as an additional requirement. The concern originate from the fact that voluntary accreditation schemes do not necessarily control the compliance of the CSP with the requirements of the Directive. However, Article 3.2 explicitly supports all kinds of voluntary accreditation schemes. [154]

According to Article 7.2, 'in order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organizations. The Council shall decide by qualified majority.'

Article 7.3 provides that 'whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority.'

[154] DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G. & VAN EECKE, P. (2003) The Legal and Market Aspects of Electronic Signatures in Europe, Study for the European Commission within the eEurope 2005 framework, at http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

2.3 US Uniform Electronic Transactions (UETA) and Electronic Signatures in Global and National Commerce (E-SIGN)

Any analysis of the impact of E-SIGN or UETA begins with the facile question of whether there is a requirement of a writing or a signature for the transaction or contract at issue. Both the UCC and the traditional contract approach do not expressly require writing or a signature for a contract to be enforceable. Handshake or oral agreements and clickwrap or click-through agreements can serve as examples of contacts which are not documented by traditional writing. Examples of contracts not requiring signatures include shrinkwrap licenses, tickets or click-through agreements. E-SIGN and UETA come into play only when there is a requirement by law that a contract and/or signature be in writing to be enforceable. The main source of a writing requirement for contracts is the general statute of frauds of a state. Among the examples are contracts of transfer of real estate, the ones that cannot be completed within one year, guarantees to pay the debt of another, and leases for more than one year. Writing or signature requirements may also arise under federal law. Examples include copyright assignments and exclusive licenses, trademark and patent assignments. It can be also required by other laws and regulations, particularly in the area of consumer notices and disclosures. A contract need not be in writing or be signed to be enforceable, unless there is a legal writing or signature requirement. E-SIGN and UETA will play no role in cases where there is no applicable legal writing or signature requirement. In such cases, contracts can be concluded using electronic methods. [155]

E-SIGN and UETA answer both questions of whether an electronic record satisfies the writing requirement and/or an electronic signature satisfies the signature requirement in the

[155] Charles H. Fendell and Dennis M. Kennedy of the Intellectual Property and Information Technology Practice Area, Articles - Thompson Coburn LLP, "Electronic Signatures In Missouri: Moving To UETA Or Staying With E-SIGN", Winter 2003, at http://www.thompsoncoburn.com/Articles/CHF001.aspx

affirmative. If there is a writing requirement, an electronic record will satisfy it. If there is a signature requirement, an electronic signature will satisfy it. Nevertheless, both E-SIGN and UETA are intended to be limited in scope and not to change substantive contract law. Both provide for an equivalence of electronic signatures and electronic records with writings and signatures on paper. All other requirements of the traditional written signatures, such as competency, intent to sign and the like must also be met.[156] Both UETA and E-SIGN are technology-neutral; they do not specify any technology which should be used. Both also provide basically the freedom to use or not use electronic records and electronic signatures and have common objectives with other international attempts to set standards for e-commerce: to remove perceived barriers to the free traffic of e-commerce, to increase speed in contract formation as well as notice giving and to let the parties to conduct business in a cost savings through exclusion of paper way and otherwise take full advantage of electronic commerce.[157]

The focus in E-SIGN and UETA is on the form of the record or authentication, that is, electronic versus non-electronic, and equivalency is established as to form.[158]

There have been some debates whether enactment of E-SIGN or UETA is necessary for making electronic contracts enforceable. Judicial practice have had already a negative answer to this question because the contracts without having traditional written form or a signature have been enforced by courts before the E-SIGN or UETA enactment; moreover some courts have established that electronic documents satisfy ‘writing’ requirements of statutes. One of the important points to mention is the fact that many contracts have not been required by

[156] Charles H. Fendell and Dennis M. Kennedy of the Intellectual Property and Information Technology Practice Area, Articles - Thompson Coburn LLP, “Electronic Signatures In Missouri: Moving To UETA Or Staying With E-SIGN”, Winter 2003, at http://www.thompsoncoburn.com/Articles/CHF001.aspx

[157] Ibid.

[158] Holly K. Towle “E-SIGNATURES--BASICS OF THE U.S. STRUCTURE” published in Houston Law Review Fall 2001, available at http://international.westlaw.com/welcome/WorldJournals/default.wl?fn=_top&rs=WLI

statutes to be in writing or signed; thus, electronic data and signatures have been admissible as evidence in legal proceedings even in the absence of E-SIGN and UETA.[159]

The uncertainty in the use of electronic records and electronic signatures in contracts as well as the failure of states to overcome this problem by enacting uniform state laws motivated the Congress to adopt E-SIGN. Drafted before E-SIGN, UETA is a model statute adopted to provide uniformity among state laws on electronic signatures and electronic records; nevertheless, at the time of E-SIGN enactment, many states had failed to enact UETA and, in addition, it was enacted by some states in non-uniform versions. Therefore, uniformity was necessary for further e-commerce development.[160]

Basically, E-SIGN provides for equal treatment of electronic data and signatures to paper documents and signatures related to interstate or foreign commerce and preempts all inconsistent with it state laws on electronic records and signatures. Since E-SIGN's effective date, UETA have been enacted by 40 states, introduced and at least partially considered by most of the remaining ones. [161]

UETA

The Uniform Electronic Transactions Act (UETA), proposed by the National Conference of Commissioners on Uniform State Laws (NCCUSL) is one of the several United States Uniform Acts. It was adopted by 46 States, the District of Columbia, and the U.S. Virgin Islands into their own laws. One of its the main purposes is to bring into line the differing State laws over the validity of electronic signatures, thus supporting the validity of electronic contracts as a viable means of agreement. UETA (1999) addresses the need to retain

[159] Charles H. Fendell and Dennis M. Kennedy of the Intellectual Property and Information Technology Practice Area, Articles - Thompson Coburn LLP, "Electronic Signatures In Missouri: Moving To UETA Or Staying With E-SIGN", Winter 2003, at http://www.thompsoncoburn.com/Articles/CHF001.aspx
[160] Ibid.
[161] Ibid.

paper copies of other records and contracts, effectively giving legally binding status to electronic documents and signatures.[162]

The UETA directly confronts the validity and enforceability of electronic contracting. The central legal requirements provided under the UETA are set forth in section 7, which expressly validates electronic records, signatures, and contracts.[163] A principal prerequisite of UETA is that means of a record, signature, or contract should have no impact on its legal significance. Section 7 of UETA states that:

> (a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
>
> (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
>
> (c) If a law requires a record to be in writing, an electronic record satisfies the law.
>
> (d) If a law requires a signature, an electronic signature satisfies the law.[164]

Another important term in UETA is “transaction.” “UETA does not apply to all writings and signatures, only to electronic records and signatures relating to a "transaction," which is defined as those interactions between people relating to business, commercial and governmental affairs.”[165]

UETA allows, but does not require, parties to conduct business electronically. The principle of freedom to choose electronic methods is approached by UETA differently than by E-SIGN. Section 5(b) of UETA states that “this Act applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and

[162] Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Ueta

[163] Steven Domanowski “E-SIGN: PAPERLESS TRANSACTIONS IN THE NEW MILLENNIUM” published in DePaul Law Review, Winter 2001, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

[164] Uniform Electronic Transactions Act (1999), Section 2(8), available at http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm

[165] Charles H. Fendell and Dennis M. Kennedy of the Intellectual Property and Information Technology Practice Area, Articles - Thompson Coburn LLP, “Electronic Signatures In Missouri: Moving To UETA Or Staying With E-SIGN”, Winter 2003, at http://www.thompsoncoburn.com/Articles/CHF001.aspx

surrounding circumstances, including the parties' conduct."[166] The consent may not be contained in a standard form contract unless that term is conspicuously displayed and separately consented to. Parties could also execute a separate agreement the primary purpose of which would be to consent to conducting the transaction electronically.[167] Section 5(c) gives a party that agrees to conduct a transaction by electronic means a right to refuse to conduct other transactions by electronic means, which may not be waived by agreement. Section 5(d) also provides that, with certain exceptions, the parties can vary the effect of UETA in their agreement.

UETA has in some ways even more minimalist approach than E-SIGN. In contrast to E-SIGN, UETA does not specifically exempt any types of consumer notices. "While E-SIGN requires specific and complex notice procedures, UETA takes a "context and circumstances" approach to notices and does not address specific consumer protection scenarios."[168] Moreover, UETA permits the consumer to agree to future electronic notices through a paper notice, without any confirmation requirement about the possibility of receiving electronic notice by the consumer, a concern that the E-SIGN drafters wanted to address. Besides, there are a number of issues which are addressed by UETA that are not dealt with in E-SIGN. Examples include attribution issues, evidentiary issues, applicability issues, error correction issues, and sending and receipt issues. Rules for contracts involving electronic agents in UETA are much more detailed than those in E-SIGN.[169]

[166] Uniform Electronic Transactions Act (1999), Section 2(8), available at http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm

[167] Susan Hepner Siegfried, "THE E-COMMERCE REVOLUTION: E-SIGN and UETA", http://www.vsb.org/sections/rp/articles/ESign.siegfried.html

[168] Charles H. Fendell and Dennis M. Kennedy of the Intellectual Property and Information Technology Practice Area, Articles - Thompson Coburn LLP, "Electronic Signatures In Missouri: Moving To UETA Or Staying With E-SIGN", Winter 2003, at http://www.thompsoncoburn.com/Articles/CHF001.aspx

[169] Ibid.

E-SIGN

The Electronic Signatures in Global and National Commerce Act, or E-SIGN, is a United States federal law, which was passed by the U.S.Congress on June 30, 2000. The main purpose of it is to facilitate the use of electronic records and signatures in both internal and foreign commerce by ensuring the validity and legal effect of contracts which were concluded by the use of electronic means.[170] The basic intent of the E-SIGN which is stated in the very first section (101.a) provides that a contract or signature “may not be denied legal effect, validity, or enforceability solely because it is in electronic form”.[171]

E-SIGN directly addresses the fundamental dilemma posed by the writing and signature requirements of the Statute of Frauds, validating both electronic signatures and electronic contracts as a whole.[172] It provides, as a general rule, that electronic signatures and electronic records satisfy a legal requirement for writing or signature. E-SIGN takes a minimalist and procedural approach. Section 101(b)(1) states that E-SIGN does not "limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in nonelectronic form."[173] It also adopts the principal of freedom of the parties to use electronic methods. Section 101(b)2 provides that E-SIGN does not "require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to

[170] Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Esign

[171] Electronic Signatures in Global and National Commerce Act, June 30, 2000, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf

[172] Steven Domanowski “E-SIGN: PAPERLESS TRANSACTIONS IN THE NEW MILLENNIUM” published in DePaul Law Review, Winter 2001, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

[173] Ibid.

which it is a party."[174] E-SIGN has different approach to freedom to use electronic contracting than that of UETA. The basic aim of E-SIGN is to permit contracting parties to benefit from the advantages that can be offered by the digital world. By giving legal effect to electronic contracts and signatures, it is anticipated that E-SIGN will encourage the overall improvement of e-commerce by reducing customary transaction costs and increasing the completion speed of deals. There have also been in Congress discussions to provide for e-notarization.[175]

However, E-SIGN does not apply to all writings. The definitions of E-SIGN are broad. One of the important terms under E-SIGN is the term ‘transaction’ as it relates to the conduct of business, consumer or commercial affairs between two or more persons. E-SIGN does not apply to either non-transactional or unilateral actions. Examples include standard sales, leases, exchanges, licenses or other distribution of property, while living wills and health care power of attorneys are not covered by the term as they do not involve commercial matters between two people. Moreover, as a matter of specific exclusion, E-SIGN does not apply to family law matters, court orders and certain types of legal notices. In response to UETA which raised some consumer issues, E-SIGN also includes a number of consumer protection exceptions. It requires specific consent before consumer notices that required by law can be given electronically, where the consumer has to provide with an affirmative consent which has not been withdrawn. Whereas E-SIGN is intended to provide certain consumer protections, it also provides a complicated and burdensome procedure to obtain consent to electronic transactions which can cause problems to both businesses and consumers.[176]

[174] Electronic Signatures in Global and National Commerce Act, June 30, 2000, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf

[175] John S. Stolz and John D. Cromie, “Electronic Signatures in Global and National Commerce Act”, 2001, at http://www.connellfoley.com/articles/oneclick.html

[176] Charles H. Fendell and Dennis M. Kennedy of the Intellectual Property and Information Technology Practice Area, Articles - Thompson Coburn LLP, “Electronic Signatures In Missouri: Moving To UETA Or Staying With

E-SIGN prevents barriers to electronic commerce. In addition it provides consumers with protections equivalent to those available in paper-based transactions. It makes also clear that no person is required to use electronic records, signatures, or contracts.[177]

Regarding authenticity, there must be some confidence that the person on the other end of the computer is the person he or she actually claims to be. A party relying on an electronic record has to be assured that the message is not a forgery and is attributable to a designated party. The ability to establish the authenticity of an electronic record is also important in cases where its enforceability is challenged. Moreover, it is equally important that the document sent must be the same as the one received, with no unauthorized or accidental alterations during or after delivery. The necessity of establishing authenticity and maintaining data integrity leads to the overall enforceability of an electronic transaction.[178]

E-SIGN, operating from the standpoint of technological neutrality, has left it to the contracting parties to determine the best method to ensure attribution and data integrity in a certain transaction. The most commonly used methods are, for example, the use of passwords and PINs. One of the popular forms of security measure is the use of digital signatures, which is used not only to establish authenticity, but also to protect data integrity.[179]

E-SIGN further provides that if notarization or acknowledgment of a signature or record is required, that requirement is satisfied if the electronic signature of the person notarizing the record is "attached to or logically associated with the signature or record."[180]

E-SIGN", Winter 2003, at http://www.thompsoncoburn.com/Articles/CHF001.aspx

[177] Jacob J. Lew "OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act", http://www.whitehouse.gov/omb/memoranda/m00-15.html

[178] John S. Stolz and John D. Cromie, "Electronic Signatures in Global and National Commerce Act", 2001, at http://www.connellfoley.com/articles/oneclick.html

[179] Ibid.

[180] Susan Hepner Siegfried, "THE E-COMMERCE REVOLUTION: E-SIGN and UETA", http://www.vsb.org/sections/rp/articles/ESign.siegfried.html

E-SIGN does not give any particular federal or state agency the right to interpret its provisions. Instead, E-SIGN preserves for federal and state agencies the ability to interpret the provisions of E-SIGN that apply to legal requirements those agencies currently have authorization to interpret. For example, the FRB may interpret how E-SIGN should be implemented with respect to electronic disclosures otherwise required to be "in writing" under the Truth in Lending Act, the Electronic Fund Transfers Act, the Equal Credit Opportunity Act, and the various other statutes for which the FRB has regulatory authority. Similarly, state regulators may interpret how E-SIGN should be implemented with respect to state-required consumer disclosures.[181]

The Electronic Signatures Act will also stimulate new areas of business for software vendors and service providers. The problems associated with presenting, tracking, managing, and authenticating electronic signatures and records are opportunities for the companies that can address them. Given the complexity and critical importance of being able to authenticate signatures, there will be interesting opportunities for companies that can outsource that capability for clients or that can provide customer companies with the tools and processes to manage the authentication themselves.[182]

Though both of the acts have the same general principles, there are some major differences between E-SIGN and UETA:

1) E-SIGN was drafted with some specific consumer protection issues because UETA's approach to consumer protection was proved to be unsatisfactory;

[181] Robert A. Cook, Timothy P. Meredith, Elizabeth C. Yen “THE ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT--A REVIEW oF THE ACT'S CONSUMER DISCLOSURE REQUIREMENTS”, published in Consumer Finance Law Quarterly Report, Fall, 2000, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

[182] Bill Zoellick “WIDE USE OF ELECTRONIC SIGNATURES AWAITS MARKET DECISIONS ABOUT THEIR RISKS AND BENEFITS”, published in New York State Bar Journal, November/December, 2000, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

2) E-SIGN has a broader list of exclusions from coverage of the law. These additional exclusions include family law matters, foreclosures, and similar matters;

3) UETA is generally more comprehensive than E-SIGN. UETA addresses the question of when electronic records are deemed to be sent and received. UETA covers the issue of attribution of signatures and covers the issue of admissibility of electronic records into evidence;

4) UETA provides that both parties must consent to the use of electronic methods. In addition, unlike E-SIGN, there is no requirement that the ability to receive electronic notice must be confirmed;

5) UETA explicitly defers to other substantive state law. E-SIGN's approach is not to preempt "consistent" laws;

6) Under UETA, the parties can agree not to have provisions of UETA apply, such as those relating to the timing of the receipt of electronic documents. E-SIGN does not have similar provisions;

7) UETA's approach to maintenance of records is less specific and more flexible than the approach under E-SIGN. UETA also specifically permits the use of third parties to maintain records. E-SIGN does not address this issue;

8) E-SIGN's preemption rules are complex and difficult. In some cases, it simply is not clear how the preemption will work. The adoption of UETA allows a state to avoid these preemption issues. [183]

[183] Charles H. Fendell and Dennis M. Kennedy of the Intellectual Property and Information Technology Practice Area, Articles - Thompson Coburn LLP, "Electronic Signatures In Missouri: Moving To UETA Or Staying With E-SIGN", Winter 2003, at http://www.thompsoncoburn.com/Articles/CHF001.aspx

2.4 EU v. US legal approach towards electronic signatures

The stated aim of the Directive is to "create a harmonised and appropriate legal framework for the use and legal recognition of electronic signatures within the EU." The Directive requires that member states enact legislation that affords legal recognition to "electronic signatures that are based on a ‘qualified certificate’" so long as they were "created by a ‘secure-signature-creation device’". While a contract that fulfills Article 5 is valid as such, other contracts are not necessarily invalid. The EU Directive deals with future technologies in the same way as its American counterparts. The EU Directive does not require a specific type of technology, but allows for technological adaptation that fulfills the secure-signature-creation requirement.[184]

The European Directive recognizes the validity of two types of signatures: an electronic signature and an advanced electronic signature. While the former should not be denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form, the advanced electronic signature satisfies the legal requirements of a signature in relation to electronic data in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data and is admissible as evidence in legal proceedings. The advanced signature qualifies only when it is based on a qualified certificate defined in Annex I and Annex II of the Directive. The qualified certificate must also be based on a secure signature creation device as it is required in Annex III. In order for an advanced

[184] Christopher William Pappas “COMPARATIVE U.S. & EU APPROACHES TO E-COMMERCE REGULATION: JURISDICTION, ELECTRONIC CONTRACTS, ELECTRONIC SIGNATURES AND TAXATION”, published in Denver Journal of International Law and Policy Winter, 2002, The Holland & Hart Private International Law Award, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

electronic signature to satisfy the legal requirements, it has to in accordance with the criteria of Annexes I, II and III.[185]

UETA following the principle of technological neutrality takes a different approach. Unlike the Directive, UETA does not distinguish between the different types of electronic signatures. "If a law requires a signature, an electronic signature satisfies the law."[186] An electronic signature is defined as an "electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."[187] The purpose is to equalize validate electronic signatures to writing. The key accent is the intent of the party to sign the record. On the contrary, the Directive is focused on satisfying the criteria of non-repudiation, integrity, security and confidentiality of the signature based on the identification of the signatory and the certificate issued by the certificate providers.[188]

E-SIGN states that all electronic contracts relating to transactions in or affecting interstate or foreign commerce be given the same legal force as if they were written: "A signature, contract, or other record may not be denied effect, validity or enforceability solely because it is in electronic form." Although E-SIGN is an example of Congress' application of its broad powers under the Commerce Clause of the U.S. Constitution, it does not pre-empt state laws (such as UETA) which can modify, limit, or even supersede its provisions.[189]

[185] Sylvia Mercado Kierkegaard "Corporate and Commercial E-CONTRACT FORMATION: U.S. AND EU PERSPECTIVES", published in Shidler Journal of Law, Commerce & Technology Winter, 2007, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

[186] Uniform Electronic Transactions Act (1999), Section 7(d), available at http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm

[187] Ibid, Section 2(8).

[188] Sylvia Mercado Kierkegaard "Corporate and Commercial E-CONTRACT FORMATION: U.S. AND EU PERSPECTIVES", published in Shidler Journal of Law, Commerce & Technology Winter, 2007, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

[189] Christopher William Pappas "COMPARATIVE U.S. & EU APPROACHES TO E-COMMERCE REGULATION: JURISDICTION, ELECTRONIC CONTRACTS, ELECTRONIC SIGNATURES AND

The future treatment of electronic signatures regulation is likely to continue on the same way as currently. That is, technology has taken the lead over legislation further than legislation has restrained or guided technology. The EU Electronic Signature Directive is an example of this relationship. The Directive utilizes the technology available, while remaining flexible to accept future technologies, to ensure that electronic contracts can be given the same evidentiary standing as traditional contracts. While the EU Directive allows for non-EU CSPs to offer their services within the EU, there are no international agreements for global acceptance of such electronic contract verification. A multilateral convention or international consortium outlining standards for the global recognition of CSPs would support e-commerce growth on a larger international scale.[190]

The advantage of two-tier approach, which is followed by EU, is that not only does it provide legal neutrality by recognizing most of the authentication technologies but also it defines a more innovative legal environment by ratifying the freedom of choice regarding authentication systems. It shows that notwithstanding the degree of the two-tier approach's hospitality, there is still a wide divergence of international policies which could limit the uniform recognition and the interoperability of electronic signatures and electronic records with ruinous impacts on the emerging digital market.[191]

While digital signature and the two-tier approaches provide more legal certainty and

TAXATION", published in Denver Journal of International Law and Policy Winter, 2002, The Holland & Hart Private International Law Award, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

[190] Christopher William Pappas "COMPARATIVE U.S. & EU APPROACHES TO E-COMMERCE REGULATION: JURISDICTION, ELECTRONIC CONTRACTS, ELECTRONIC SIGNATURES AND TAXATION", published in Denver Journal of International Law and Policy Winter, 2002, The Holland & Hart Private International Law Award, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

[191] Christina Spyrelli "Electronic Signatures: A Transatlantic Bridge? – An EU and US Legal Approach Towards Electronic Authentication", published in "Journal of Information, Law and Technology", 16 August 2002, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/

security, but nevertheless still focus too narrowly on signatures as such, and not on formal requirements as a whole, the minimalist approach gives the opportunity for a uniform legislation on electronic signatures based on internationally harmonized criteria to develop, as it focuses on the functions of signatures and the methods in which these functions can be translated into technological applications keeping a technological neutrality.[192]

[192] Christina Spyrelli "Electronic Signatures: A Transatlantic Bridge? – An EU and US Legal Approach Towards Electronic Authentication", published in "Journal of Information, Law and Technology", 16 August 2002, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/

Conclusion

The increasing use of e-commerce generally is considered a positive trend that should be promoted. The security in the electronic transactions over the Internet is regarded as one of the most crucial issues in the digital world. During the last decade, national and international legislators have been trying to promote the use of electronic signatures in the e-commerce and set forth a common legal framework for electronic authentication over the Internet. However, many lawyers believe that laws requiring signatures to authenticate certain transactions represent obstacles to e-commerce and threaten to keep it from reaching its full potential.

Computerization of almost all fields, including the legal field, has nowadays become an increasingly acute problem for the professionals of each field who are not familiar with the technology novelties, which can cause problems in their own field. One such novelty appearing in recent years is digital signature, which has become more and more frequently used in the legal field for document authentication. While most of the national and international acts and scholars recognize that digital signatures are the ones based on the use public key cryptology technology, there are also some radically critical views to such definition.

In most of the cases, the main purpose of a signature is to evidence the original of the document or approval of it by a particular individual[193]. In other words, the prime function of a signature is to give evidence of the source of the document or the intention of a person in respect of that document. Electronic signatures can serve an equavalent to paper-based ones as long as they satisfy the legal requirements for paper signatures. Modern methods of technology provide for such solution.

[193] Ian Lloyd, ‘Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures’, LAW & THE INTERNET regulating cyberspace, edited by Lilian Edwards and Charlotte Waelde, ‘HART’ publishing, Oxford, 1997, 140.

In many countries, it is required by the law that contracts must be “in writing” or “signed.” The concern can arise about the meaning of these words in the context of the Internet. This and similar issues arising in connection with records or forms, such as legal requirement of government filing can be solved by legal provisions providing that “a signature, contract or other record may not be denied legal effect, validity or enforceability solely because it is in electronic form.”[194]

The necessity for the new laws on electronic signatures adoption was born by the diverse practice. While some courts have accepted electronic records and signatures as valid counterparts of its paper-based ones, the others have refused to give them legal recognition. Various courts have concluded different results that created the legislative concern. Due to the significance of new emerged technology and difficulties with the recognition of it a lot of international initiatives have been adopted and legislators around the world struggle to find the best regulatory scheme in order to legally equalize e-signatures to the handwritten ones. Statutes that merely extend legal recognition to electronic signatures can best foster electronic commerce on the Internet, while statutes that, in the name of security, favor one emerging technology over another will hinder the natural growth of an efficacious market.

The main purpose of the thesis is to facilitate the work of practitioners dealing with digital signatures by theoretical analyses of the practical and legislative problems in order to avoid obstacles that may arise in future. The national and international laws adopted in this area are quite new and not confirmed by long practice, for this reason there are gaps which should be filled and issues which can be better regulated. This work has analyzed a number of international legislative efforts, their interpretations and proposals of their perfection as well as

[194] Online eCommerce Guidance Handbooks: E-Commerce/Digital Signatures, Global Internet Policy Initiative at http://www.internetpolicy.net/e-commerce/

evaluated their effectiveness.

Bibliography

a) Literature

1. Ian J Lloyd “Information Technology Law”, third edition, Butterworths, London, Edinburgh, Dublin, 2000.

2. Ian Lloyd, ‘Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures’, LAW & THE INTERNET regulating cyberspace, edited by Lilian Edwards and Charlotte Waelde, ‘HART’ publishing, Oxford, 1997.

3. Thomas J. Smedinghoff and Ruth Hill Bro “ Electronic Signature Legislation”, http://library.findlaw.com/1999/Jan/1/241481.html

4. Christopher Kuner and Anja Miedbrodt “Written Signature Requirements and Electronic Authentication: A Comparative Perspective”, at http://www.kuner.com/data/articles/signature_perspective.html

5. Jonathan D. Hart, Law of the web, a field guide to internet publishing 2003 edition, Bradford Publishing Company, Denver, Colorado.

6. John S. Stolz and John D. Cromie, “ Electronic Signatures in Global and National Commerce Act”, 2001, at http://www.connellfoley.com/articles/oneclick.html

7. Christina Spyrelli “Electronic Signatures: A Transatlantic Bridge? – An EU and US Legal Approach Towards Electronic Authentication”, published in “Journal of Information, Law and Technology”, 16 August 2002, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/

8. Stephen Mason “ELECTRONIC SIGNATURES IN PRACTICE”, published in Journal of High Technology Law 2006, http://international.westlaw.com/Welcome/WorldJournals/default.wl?blinkedcitelis

9. Lorna Brazell “Electronic Signatures Law and Regulation”, first edition, Bird & Bird, Thomson, Sweet & Maxwell, Great Britain, London 2004.

10. Caspar Bowden and Yaman Akdeniz “Privacy II: Cryptography and Democracy – Dilemmas of Freedom”, “Liberating Cyberspace, Civil Liberties, Human Rights and the Internet” edited by Liberty (The National Council for Civil Liberties), Pluto Press, London – Sterling, Virginia, USA, 1999.

11. Bruce Schneier “Why Cryptography Is Harder Than It Looks”, http://www.schneier.com/essay-037.pdf

12. Fred Cohen & Associates, specializing in information protection since 1977, “A Short History of Cryptography”, http://all.net/books/ip/Chap2-1.html

13. Michael Froomkin “The Essential Role of Trusted Third Parties in Electronic Commerce”, Published at 75 Oregon L. Rev. 49 (1996), http://osaka.law.miami.edu/~froomkin/articles/trusted.htm

14. Roger Clarke “Message Transmission Security (or ‘Cryptography in Plain Text’)”, version of 11 May 1998 at http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html, Earlier version published in Privacy Law & Policy Reporter 3, 2 (May 1996), pp. 24-27

15. Ellen Freedman, Reid Trautz, Jim Calloway “THE LAWYER'S GUIDE TO MOBILE COMPUTER SECURITY” published in Pennsylvania Lawyer March/April, 2007, available at http://international.westlaw.com/welcome/WorldJournals/default.wl?fn=_top&rs=WLI

16. Christopher Reed ‘Internet Law: Text and Materials’, Butterworths, London, Edinburgh, Dublin, 2000.

17. Mark Taylor “USES OF ENCRYPTION: DIGITAL SIGNATURES”, published in Computer and Telecommunications Law Review 2006, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?blinkedcitelis

18. George L. Paul, “The "Authenticity Crisis" In Real Evidence”, http://www.lewisroca.com/uploads/The%20Authenticity%20Crisis%20In%20Real%20Evidence.pdf

19. James Hill “Lock and Load: Document security on the Net”, Business Law Today November/December 1998 at http://www.abanet.org/buslaw/blt/8-2lock.html

20. Alcolya J. L. Lester “THE DIGITAL SIGNATURE: THE NEXT STEP IN ITS EVOLUTION” published in ILSA Journal of International and Comparative Law Fall, 2000, Cyber-International Law Notes & Comments, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

21. Bruce Schneier, “Why Digital Signatures Are Not Signatures”, http://www.schneier.com/crypto-gram-0011.html

22. Indira Carr “UNCITRAL & Electronic Signatures: A Light Touch at Harmonisation”,

available at http://perseus.herts.ac.uk/uhinfo/library/u81985_3.pdf

23. Babette Aalberts and Simone van der Hof “Digital Signature Blindness”, available at http://www.buscalegis.ufsc.br/arquivos/Digsigbl.pdf

24. John Dickie, “Internet and Electronic Commerce Law in the European Union”, ‘Hart’ Publishing, Oxford – Portland Oregon, 1999.

25. Jos Dumortier ‘Directive 1999/93/EC on a Community framework for electronic signatures’, “eDirectives: Guide to European Union law on E-Commerce” – Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection, edited by Arno R. Lodder and Henrik W.K. Kaspersen, Kluwer Law International, The Hague/London/New York, 2002.

26. DUMORTIER, J., LIBON, O., MITRAKAS, A., RINDERLE, R., SCHREIBER, A., VAN EECKE, P., (2000) European Electronic Signature Standardization Initiative - Certificate Path Validation , European Commission, 61 http://www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf?where=

27. DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G. & VAN EECKE, P. (2003) The Legal and Market Aspects of Electronic Signatures in Europe, Study for the European Commission within the eEurope 2005 framework, at http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

28. DUMORTIER, Jos, (2002) 'Directive 1999/93/EC on a Community framework for electronic signatures', Lodder, A.R., Kaspersen, H.W.K.,: eDirectives: Guide to European Union Law on E-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data protection. In de reeks Law and Electronic Commerce, Vol 14, Kluwer Law International,pag. 33-65, at http://www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf?where

29. Paolo Balboni “Liability of Certification Service Providers Towards Relying Parties and the Need for a Clear System to Enhance the Level of Trust in Electronic Communication”, available at http://www.eema.org/downloads/member_news/balboni_article.pdf

30. Charles H. Fendell and Dennis M. Kennedy of the Intellectual Property and Information Technology Practice Area, Articles - Thompson Coburn LLP, “Electronic Signatures In Missouri: Moving To UETA Or Staying With E-SIGN”, Winter 2003, at http://www.thompsoncoburn.com/Articles/CHF001.aspx

31. Holly K. Towle “E-SIGNATURES--BASICS OF THE U.S. STRUCTURE” published in Houston Law Review Fall 2001, available at http://international.westlaw.com/welcome/WorldJournals/default.wl?fn=_top&rs=WLI

32. Steven Domanowski “E-SIGN: PAPERLESS TRANSACTIONS IN THE NEW MILLENNIUM” published in DePaul Law Review, Winter 2001, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

33. Susan Hepner Siegfried, “THE E-COMMERCE REVOLUTION: E-SIGN and UETA”, http://www.vsb.org/sections/rp/articles/ESign.siegfried.html

34. Jacob J. Lew “OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act”, http://www.whitehouse.gov/omb/memoranda/m00-15.html

35. Robert A. Cook, Timothy P. Meredith, Elizabeth C. Yen “THE ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT--A REVIEW oF THE ACT'S CONSUMER DISCLOSURE REQUIREMENTS”, published in Consumer Finance Law Quarterly Report, Fall, 2000, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

36. Bill Zoellick “WIDE USE OF ELECTRONIC SIGNATURES AWAITS MARKET DECISIONS ABOUT THEIR RISKS AND BENEFITS”, published in New York State Bar Journal, November/December, 2000, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

37. Christopher William Pappas “COMPARATIVE U.S. & EU APPROACHES TO E-COMMERCE REGULATION: JURISDICTION, ELECTRONIC CONTRACTS, ELECTRONIC SIGNATURES AND TAXATION”, published in Denver Journal of International Law and Policy Winter, 2002, The Holland & Hart Private International Law Award, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

38. Sylvia Mercado Kierkegaard “Corporate and Commercial E-CONTRACT FORMATION: U.S. AND EU PERSPECTIVES”, published in Shidler Journal of Law, Commerce & Technology Winter, 2007, available at http://international.westlaw.com/Welcome/WorldJournals/default.wl?tc=2&docsample

39. Diane Rowland and Elizabeth Macdonald “Information Technology Law”, second edition, Cavendish Publishing Limited, London, Sydney, 2000.

b) Legislative and Regulatory Acts

1. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities, http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

2. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, available at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

3. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, available at http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

4. American Bar Association ‘Digital Signature Guideline Tutorial’, http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

5. Uniform Electronic Transactions Act (1999), available at http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm

6. Electronic Signatures in Global and National Commerce Act, June 30, 2000, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf

7. THE OECD DECLARATION AND DECISIONS ON INTERNATIONAL INVESTMENT AND MULTINATIONAL ENTERPRISES: BASIC TEXTS, available at http://www.olis.oecd.org/olis/2000doc.nsf/4f7adc214b91a685c12569fa005d0ee7/c125692700623b74c1256991003b5147/$FILE/00085743.PDF

8. ICC General Usage for International Digitally Ensured Commerce, Preface, available at http://www.iccwbo.org/home/guidec/guidec.asp

9. ICC General Usage for International Digitally Ensured Commerce (version II), Preface, available at http://www.internetpolicy.net/e-commerce/guidec2001.pdf

10. Framework for EESSI Standards and Classes for Electronic Signatures, available at http://www.ictsb.org/EESSI/Documents/EESSI-ITEMA-v2.0.doc

c) Cases

1. In re Piranha, Inc., 2003 WL 21468504

2. Cloud Corporation v. Hasbro Inc., 314 F.3d 289 (7th Cir., 2002)

3. Sea-Land Service, Inc. v. Lozen International, LLC, 285 F.3d 808 (9th Cir., 2002)

d) Other sources

1. Online eCommerce Guidance Handbooks: E-Commerce/Digital Signatures, Global Internet Policy Initiative at http://www.internetpolicy.net/e-commerce/

2. Electronic records and signatures' available at http://www.law.uh.edu/faculty/RNimmer/contracts/supp10.pdf

3. Free Encyclopedia of Ecommerce, "Encryption – Popular Encryption Technologies, Cutting-edge Encryption Schemes, Encryption in the E-commerce Arena.", http://ecommerce.hostip.info/pages/416/Encryption.html

4. Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Writing

5. Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Signature

6. Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Cryptography

7. Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Ciphertext

8. Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Ueta

9. Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Esign

10. http://www.infothis.com:80/find/Signature/

11. http://www.infothis.com:80/find/Cryptography/

12. http://www.infothis.com/find/Key_size/

13. http://www.infothis.com/find/Digital_signature/

14. http://www.webopedia.com/TERM/D/digital_signature.html