A “Concorde” about the Electronic Signature

Comparing Electronic Signature Legislations
in the EU and in the USA

Candidate number: 9
Supervisor: Maryke Silalahi Nuth
Deadline for submission: 09/01/2005

Number of words: 16,462 (max. 18.000)

Date of submission: 09/01/2005

Content

1 Introduction to the Electronic Signature System

1.1 Purposes and Legal Issues

The signature has always had fundamental legal importance. Infact many legal effects can arise from that. The technological development has changed many aspects in every sector; the legal world too has modified and refreshed the existing concepts and created new concepts. One of these changes is the introduction, in the legal systems of the developed countries, of the concept of "electronic signature"[1].

The purpose of this paper is to make a comparison between the regulations adopted in the EU and that one in force in the USA about electronic signature. Like in every comparison, some common points and differences will be uncovered. More importance will be given to the differences, and just briefly discuss some points in common.

The paper will focus on aspects of fundamental interest. Firstly the legal view in which the two regulations have been adopted will be described in the second chapter. In this way it will be possible to have a satisfying basis of knowledge for understanding the differences of the two legislations.

Secondly, the paper will focus on the concept of electronic signature in the two legislations and their limits. The following will be observed:

- the USA Act is less descriptive than the European one;
- and the EU rules allow three different levels of protection.

[1] To have an idea of the differences between the handwritten signature and the electronic one, it is usefull the read the article of McCullagh, "*Signature Stripping: a Digital Dilemma"*, in JILT 2001 (1), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/ ; it is also usefull to read the paragraph 2.3 of the article of Angel, "*Why use Digital Signatures for Electronic Commerce*" in JILT 1999 (2).

Thirdly, the paper will deal with legal rules about certification authorities which are the fundamental authority in the electronic signature system. In this relation, it will be observed a relevant difference between the two regulations: while the EU legislation deals with such authorities, we can not find similar rules in the USA legislations.

Lastly, there will be a description of the points in common between the two legislations and, in particular, a description on how the two different legal systems deal with the principle of recognition of electronic signature.

In the last chapter there will be a global comparison between the two systems. This comparison will be useful in particular because it will raise an important difference in the approach of the two legal systems about technological neutrality. The chapter will also deal with the important issue of international harmonization about electronic signature: in particular to describe how this point is regulated in the two legal systems.

Later, the structure and the possibilities of electronic signature will be also described but it is possible to say now that it is every means concluded to the electronic authentication that allows to associate data to other data[2].

1.2 Terminology

Before describing the legislations in EU and the USA, it is useful to clarify some preliminary concepts. First of all the difference between electronic signature and the digital one will be described to show that digital signature is a kind of electronic signature that uses encryption system. After that, there will be a description of the encryption systems (systems based on the concept of ”key”), their history and their uses in modern society. Lastly, there will be a brief reflection about the expression “safety of the communication”.

1.2.1 ”Electronic Signature” and ”Digital Signature”: different expressions for the same concept?

It is really important to distinguish the concept of electronic signature with the digital one.

The "electronic signature" is a general term without any technical-juridical meaning. As it was said, the electronic signature is considered every means concluded to the electronic authentication that allows to associate data to other data (for example signature and document)[3].

There are three methods of electronic authentication used for electronic signatures: the knowledge of something: (password, code pin, etc.), the use of biometric technologies[4], that identify the unique physical traits of each person, (finger prints, voice etc.) and, lastly, the possession of something (it enrolls magnetic, smart card, etc.). It can be said that those methods are the modern version of old concepts: word of order, recognition of sight, key...

On the other hand, "digital signature" is a specific term that refers to a particular electronic signature system that uses an encryption system: the one with two different keys (one public and one private). Using the words of a famous doctrine, digital signatures are “mathematical functions of the digital forms of a message; in order to act effectively as a signature they must be producible only by the sender”[5].The private key is usually memorized in a device normally constituted by a smart card (to which can be added the adoption of a code or something else: in

---

[2] Arnò & Lista, definition from “*La firma digitale nell’ordinamento italiano e comunitario*” in “Rivista di diritto civile” 2000, p. 732.

[3] See note 2.

[4]There are two risks of the use of the biometric technologies:

(i) Biometric solutions are based on statistical analysis and are, thus, not 100% reliable;

(ii) Biometric, human information is translated into binary form and this information is recorded on a tangible medium or stored in electronic or other form, which is retrievable in readable form.

[5] From Reed, Chris, & Davies, Lars, *Computer Law*, 5th edition, Oxford University press, p.340

this way there is an increase the length of the procedure but obviously also the safety).

Being sure that the two expressions do not have the same meaning, the choice of which of them to be used is full of relevant consequences. If one legislation uses the term electronic signature, the principle of technological neutrality in that regulation does not allow the description of a specific technology and therefore it is less detailed but does not need continuous updating. On the other hand, when the term digital signature is used, there is a more detailed regulation, that has a need of continous updating[6].

When the difference between electronic and digital signature is clarified, it should be noted that the digital signature technology is the most used and technologically advance form of electronic signature. It is this technology that develops the "world" of electronic signature and creates the need for regulations all around the world.

1.2.2 Encryption Systems

Using the words of Akdeniz, "Encryption is the use of some means to disguise or obscure the meaning of a message"[7].

Obviously, the encryption is not a new phenomenon. Infact the man has always used mechanisms that gave him the possibility to ensure transmission of messages. For example, it is enough to read a book about the Roman history, or even the Greek history, to realize how the society has always looked for a safe transmission of the important information. It was obtained by adopting the

[6] It can be said, for example, that the Community Directive has expressly headed to this direction by adopting "a wide approach to the various technologies and services those allow to authenticate the data in electronic way".

instruments that are able to guarantee the intelligibility and the reservation of the information, making them comprehensible only for the one who knew the code for decoding the message[8].

The techniques used for the encryption became more sophisticated with the technological evolution. An important step was the creation, during the Second World War, of the German "Enigma", a really sophisticated machine in that time, able to encrypt and decrypt military messages. According to Akadeniz, the Enigma can be considered "the forerunner of computer-aided encryption"[9].

With the evolution of the technologies the topic of the safety of the communications, from principle especially in military sector, has begun more generically and more pressing. Infact, it is possible to see an increase of the demand for more sophisticated encryption systems. Considering the big amount of telematic communication in modern society, it is possible to realize the importance of the technology tied to the development. This demand has had, as effect, the development of new algorithms[10] that could guarantee a satisfactory safety standard in the transmission of information.

There are several kinds of systems of encryption (the "Substitution", the "Transposition" and the "One Time Pad"), but the most important one is the

---

[7] Rose, "*Your Rights in the Online World*", Osborne McGraw-Hill, 1995, in Netlaw, says that "the encryption is basically an indication of users' distrust of the security of the system, the owner or operator of the system, or law enforcement authorities".

[8]Examples of "ante-litteram" cryptography in classical epoch are those narrated by Plutarco that handed down us the function of the "sciatola" (used by the Judges of Sparta to deliver a parchment to Lisandro). We could also say about Cicero, probably the first author of a real system of codification of the messages, founded on the substitution of the letters of a single word with the other, according to a pre-arranged numerical criterion.

[9] From the article of Akadeniz, *Cryptography and Liberty "Can the Trusted third Parties be Trusted?" A Critique of the recent Uk proposals"*, 1997, in JILT 1997 (2), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/ .

[10] The system of cryptography needs the the concept of algorithm. The algorithm is defined as an orderly whole pre-arranged rules that, if performed in the suitable and correct order, can solve a series of endless problems of the same genus. Departing from this definition of general character, it is easier to understand that the algorithms is the base for the operations of encryption and decryption of the actual and complex cryptograhpic systems. Using other words, the algorithms are the instructions that make the softwares able to cipher and decipher a text using the techniques of modern cryptography. Definition is taken from Borruso & Tiberi, "*L'informatica per il giurista*", Giuffrè editor, 2001.

Substitution[11]. In the Substitution “the message is encrypted by substituting one character for another. At its simplest, this might involve simply transforming each character by a certain number of letters of the alphabet according to a pre-agreed scheme. In more complex schemes the key is not a constant rotation, but differs with each character, and involves much more than simple rotation. In some instances, the letters of the keyword are used to indicate which of a series of different alphabets should be used to effect the substitution, called polyalphabetic encryption”. The key is the necessary combination of bit for the operation of electronic identification (used from the user through alphanumeric characters) that exactly corresponds to that one that the program requires for its operation (for ex. a password). In such way "the word substitutes the metallic key" in allowing the access only to the consumers that have the same one.

Having an idea of the meaning of the key, we can say that, in general, there are mainly two techniques of encryption used in the electronic signature: the system of symmetrical keys (or without public key) and that one with asymmetrical keys (with public key). The principal difference between the two systems is based on the presence of a single key (symmetrical cryptography) or of a couple of different keys (asymmetrical cryptography).

The system of symmetrical cryptography is based on a single secret key, known just from the sender and from the recipient. So if someone else possessed the secret key, he could decipher the communications.

It is important to bear in mind that this system has several lacks. Firstly, it is possible to find one defect in the moment (really important) of the communication of the secret key from the sender to the receiver. Here there is a risk of interception from third party. The existence of such risk, reduce the practical utility of the system (that is the secretiveness of the communication). Another critical point of the system consists in the fact that the genuineness of the sent text is not guaranteed: both sender and receiver (knowing the secret key), can modify the text of the message and harm the genuineness of the document. Lastly, another

[11] For an explanation about the systems of encryption read Kahn, David, *The Codebreakers*,

defect must be underlined. In the case of communications to many subjects, there is a need to assign a different key to each of them because only in this way it can be avoided that those people, having the secret key, modify the content of the messages not sent to them.

In contrast, the system of asymmetrical keys needs the presence of a couple of keys, one public (deposited in special authorities known as certification authorities) and one private (owned by single consumer), completely different and not linked with the public one. Produced in the same standard procedure (the system of validation that creates, affixes and verifies the digital signature), this couple of keys is usable with whoever, even if the consumer is not known personally.

The asymmetrical systems of encryption (also known as systems with public key) were invented by Whitfield Diffide and Martin Hellman in the 1976[12]. It worked for the first time in 1977 through the discovery of a specific algorithm, which was developed on the base of the theorem of Fermat-Eulero, that taking the name of RSA[13]. The RSA system works as follow: "an RSA key pair is created by multiplying two randomly chosen and very large (100 digit) prime numbers to arrive at their product (the modulus) and working from there. The two prime numbers are used with the modulus to create the private and public keys. The key to RSA's strength is that it is far easier to multiply two numbers than it is to factor them"[14].

The system works in a simple way: if A wants to send a message to B, without possibility for others to read it, A has just to codify the message with the public key of B. In this way B, the only holder of the key secret correspondent, can also be the only one that can decipher the message sent to him and encoded it with his public key.

Macmillan Company, New York, 1972.

[12] G. Ciacci "*La firma digitale*" in "Il Sole 24 Ore" 2002 p. 74.

[13] Such algorithm (the RSA) has been developed in 1977 by three researchers of the Massachusetts Institute of Technology (MIT) and the name RSA derived from the initials of those three researchers Rivest, Shamir and Adleman. See the Article of Akadeniz (read above).

[14] As described by Akadeniz in his article (read above).

Using the keys in different way [15], the system can also be used for authentication of a document. We should also remember that the combination of the two functions gives us double results: the secretiveness of the communication and authentication of the sender using both the keys for encrypting the message.

It should be noted that a RSA key, even a sophisticated one (for example a key with 512 bit or 1024 bit) can be broken[16]. Therefore, there is a need for a continuous technological development.

Considering that a text undersigned can be modified, it was considered to create a system that can avoid such drawback. The solution was found in the function of hash[17]. Such function automatically creates a summary of the text to send. The Hash is "a kind of synthesis that is automatically drawn by the original document applying a mathematical function of hash."[18]

Excluding the use in the military sector and to protect the government secrets, why the encryption is useful today?
First of all, the encryption guarantees private communications. The privacy of the communication is an important right and it is useful not just in the work sector, but also in any other situation from the most public to the most private one.

---

[15] The sender in this case has to encrypt the message with his private key; the receiver then will decrypt it by the public key of the sender.
[16] This is the opinion of the RSA Laboratories.
[17] The almost unique term is used because the function of hash guarantees a low probability of collisions, and the summary produced what it codified with his own deprived key (and also with the public key of the recipient to guarantee its secretiveness) and it is sent to the subject together with the document from which the imprint is drawn out. Characteristic of the imprint is therefore the wholeness of the document, which guarantees that even if the document was intercepted during the transmission, it could not be changed. In fact, if only a character of the message is changed, and when decoded with the private key of the receiver, it would totally be different at that envoy, or the imprint would not coincide anymore.
[18] The system of cryptography as described has a really high level of safety nowadays, such as to induce part of the doctrine to consider it as concept autonomous from the conceptual point of view and the technical one, and not as a frame of the category of the asymmetrical signature with public key. The high level of reliability reached has allowed the Italian legislator for example to attribute to such combination of functions (asymmetrical keys and function of hash), as we will clarify subsequently later on, the qualification of digital signature. This means that the legislator mantains such sure system because it provides certainty in relation to the identity of the author of the

Secondly, the encryptions systems, ensuring the anonymity of the messages, guarantees the possibility to express opinions (like political opinions) that in some countries is not allowed to be expressed.

Thirdly, considering that today there are big amounts of economic transaction by Internet, banks and multinational companies that need to use sophisticated systems of encryption, for example, to protect PIN numbers and other important information.

Fourthly, another use of encryption, arriving soon, is to protect the voice during the communications by GSM mobile phone. Infact at the moment it is really easy to intercept the mobile phone communication.

Lastly, the encryption system can be used with the scope of authentication. Infact by using encryption software as PGP[19], it is possible to verify "the identity of the person with whom we are communicating"[20]. In this sense, the encryption has the same effect of a hand-written signature, and this is the reason most interesting for the scope of electronic signature.

1.2.3 Safety of the Communications

In the regulations that will be analyzed in this paper and in the doctrine's articles that provides comments to the regulation, the concept of "safety of the communication" is often used. In this relation, it is important to have clear in mind that the safety may need different requirements. It is important because some countries, regulating the electronic signature, have considered just some requirements as enough; while other countries have considered it as necessary to more requirements. Infact, on one hand it can be considered as a safe

---

message and the authenticity of the content of the message. These characteristics allow the attribution of a particular juridical value to the undersigned computer document.

[19] This is the most important public key system which was developed in 1978 by Philip Zimmermann.

[20] Words of Akadeniz paragraph 4.2

communication when it can guarantee just the origin (the writer) of the message (the problem of authentication). On the other hand, it can be considered safe a message that can not be changed from someone that is not the writer (the problem of the integrity). Thirdly it can be safe a message which can not be read by someone else different from the receiver (the problem of the privacy).

1.3 International Harmonization

In relation to the international harmonization, looking into the discipline of the electronic signature in the world today, the situation appears chaotic and not homogeneous. In this situation there is the risk that this system can be a not so useful instrument for the actual and future commercial transactions.

This lack of homogeny has several reasons: from one side this situation can come from a harmonization activity that is not totally satisfactory. From the other side, it can derive from different approaches of the legislators in dealing with the digital signature[21]. From a research conducted by ILPF, three fundamental approaches can be adopted by the legislators who want to deal with a technologically developed sector [22]. The three approaches are the "minimalist" one, the "prescriptive" one the "two floors or level". The explanation about the approaches adopted in the different countries is useful for three reasons. First of all, it is interesting to have a general idea about the ways to regulate the subject. Secondly, this explanation is interesting because the choice of the approach from the EU and the USA has had direct consequences on the different levels of technological neutrality in the two legislations (this point will be discussed in the following chapters). Thirdly, the differences between the minimalist approach and

[21] The approaches used from the legislators dealing with the digital signature are similar to those used from the legislators dealing with subjects that involve the technological development in general.

[22] This analysis derives from the studies of the Internet Law and Policy Forum (ILPF) and available on the site www.ilpf.org. The ILPF is an international organization with the goal to promote the development of the electronic commerce and the communications and try to give solution to the legal problems deriving from Internet and the electronic net.

the prescriptive one will give idea of the difficulty in the harmonization of the regulations.[23]

1.3.1 "Minimalist " Approach[24].

Such approach tries to eliminate the obstacles to the adoption of electronic signature. The only condition requested for giving effects to electronic signature is that it has to observe the legal requirements foreseen by the legislation for the manual signatures[25].

This philosophy, having the scope to remove (as much as possible) the obstacles from the commercial transactions, is used mainly in the Anglosaxon countries; countries with a pragmatic culture and that give big importance to the freedom[26]. Infact this approach is used in the countries of "common law", as Great Britain, Australia, Canada and the New Zeland, and in particular in the USA with the birth of the "Electronic Signatures in Global and National Commerce" that can almost be considered as the “flag” or the framework of this philosophy.

1.3.2 "Prescriptive" Approach

The prescriptive approach, can be considered the opposite of the minimalist one. In this case the legislator wants the technology to be used exactly in the same way that he prescribes (while a minimalist legislation tries to give the maximum freedom as possible). It happens in this way: a legislator is the starring of the

---

[23] About the international approaches about the Electronic Signature, read also Mason, *The International implications of Using Electronic Signatures*, in CTLR, August 2005.
[24]Expression used by the article "*Analysis of International Electronic and Digital Signature Implementation Initiatives*" prepared for Internet Law and Policy Forum in September 2000 and available on the site www.steptoe.com.
[25] This kind of approach involves a technological neutralità. In practice the regulator prefers not to say which technology is better to use, as this choice will come from the market.
[26]Countries that have shown, during the years, to have in their own DNA the equality commerce = welfare.

system, so he fixes rigorously the requisites of the technology to arise legal effects from them.

In the case of the signature, the countries having this approach are the "civil law" countries (Germany and Italy for example), that have adopted legislations dealing with the concept of the digital signature (not the electronic one). Furthermore, especially in the starting, those countries had prescribed really inflexible requirements.

It is possible to note that the type of approach used is typical of the countries that, in general, have less trust in the market and in its ability to regulate itself.

1.3.3 "Two floors or levels" Approach

The approach of the two levels is an alternative among the precedents that can be profitable and sometimes useful considering its intermediate position. In the case of the electronic signature, it consists in the adoption of a regulation that (like the “minimalist” one), on one hand, considers the electronic signature as any technique finalized to the authentication and gives generic recognition (with every legal effects) to a technology that satisfies the requisite of the written form. But, on the other hand, the regulation, (following the “prescriptive” approach), confers remarkable legal effects to the signature, using the system of the public key (PKI) that has particular and inflexible conditions.

The law on electronic transactions of Singapore, in force since July of 1998, is a bright example of this last approach. It, infact, distinguishes between the regular electronic signature that satisfies the requisite of the signature (it requires that the origin of the document from a determined author has to be sure), and the "sure" electronic sign that possesses determined safety requirements it supposes coming

from the person to whom is associated, without necessity to give any kind of proof[27].

Also the UNCITRAL[28] has adopted this approach in the "Draft Uniform Rules on Electronic Signatures"which is the project of regulations that establishes rules conform in the sector of electronic signature.

In general we can say that this approach found a favorable opinion in the EU. Under the prescriptive profile, the EU Members States have to attribute legal effect to the "advanced electronic signatures" that are based on " a qualified certificate" and that have been created through devices for the creation of a sure signature. Under the profile minimalist, the community directive[29] prohibits the EU Members States to deny legal effects to the electronic signature simply because it is in electronic form, or because it doesn't satisfy the standards established by the directive for the "advanced electronic signatures".

Obviously, the hope is that a unitary legislation can be dominant all over the world instead of the actual plethora of not homogeneous legislations. However it is realistically more right to hope that the various legislations will not hinder the transactions and will recognize the validity of the electronic signature in the closed systems. As such, it appears definitely like a good second best for the legislations all over the world.

1.4 Analysis Instruments

In the comparison that we are going to do we will use several legal texts coming from the EU legislation and from the USA.

---

[27] In the “Electronic Transaction Act” of Singapore, “Electronic Signature” is defined as "any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record. “Secure Electronic Signature”: “If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made: (a) unique to the person using it; (b) capable of identifying such person; (c) created in a manner or using a means under the sole control of the person using it; and (d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated, such signature shall be treated as a secure electronic signature.

[28] United Nations Commissions on International Trade Law. For more infrmations, visit the website www.uncitral.org.

In particular it will be used, as instruments of comparison, the Directive 93/99 EC from the EU legislation. The UETA and the E-SIGN Act from the USA legislation will be also analyzed.

The Directive 93/99, also called "Electronic Signature Directive", creates a Community framework for electronic signatures and was adopted on 13th of December 1999.

As it is written in the Directive (Art.1), scope of the text is "is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the internal market". Drawing the circle of application of the Directive, the second part of the Art.1 says: "It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents".

The articles of the "Electronic Signature Directive" that are analyzed in this paper are: article 1(scope), article 2 (definitions), article 4 (internal market principle), article 5 (legal effects of electronic signatures) and article 7 (international aspects).

As mentioned above, from the USA on the electronic signature, it will be analyzed the UETA and the E-Sign Act.

The UETA was approved by the "National Conference of Commissioners on Uniform State Laws" (in the last version) on the 15th of December 1999. Creating a link among the disciplines of the single states[30], this Act has the merit to create the the base for the adoption of a uniform discipline about the electronic

[29] Directive EC 1999/93.
[30] As also made from the European legislator.

transactions[31]. For such reason, it is the same legislators of the E-Sign Act that often use principles contained in the UETA. So the principles of UETA are globally the "hinge" of the subject.

This Act regulates the problem of electronic transactions, choosing as an approach to not consider the technologies used by the consumers, this is the technological neutrality. In practice, to remove the legal barriers among single states for the use of the computer documents undersigned (following the national rules), the American legislator uses a procedural discipline, and not a substantial one.

Already from this preamble it is possible to understand that purpose of the UETA is the facilitation of the e-commerce through a discipline that is able to take the common base in the not homogeneous national legislations.

The UETA contains 21 sections, but only section 7 that will be analyzed in particular [32].

The other American legal text interesting for this paper is the "Electronic Signatures in Global and National Commerce Act" or E-Sign Act, adopted on the 30th June 2000 from the Clinton presidency[33]. Scope of the Act is to facilitate transactions in electronic form or consummated with an electronic signatures.

---

[31]It is possible to see these things by reading the section on the "Scope of the Act and Procedural Approach" of the UETA. The text sets clearly: "The scope of this Act provides coverage which sets forth a clear framework for covered transactions, and also avoids unwarranted surprises for unsophisticated parties dealing in this relatively new media. The clarity and certainty of the scope of the Act have been obtained while still providing a solid legal framework that allows for the continued development of innovative technology to facilitate electronic transactions. With regard to the general scope of the Act, the Act's coverage is inherently limited by the definition of transaction" .

[32]Section 7 says: "This act simply assures that the signature may be accomplished through an electronic means. No specific technology need be used in order to create a valid signature. One's voice on an answering machine may suffice if the requisite intention is present. Similarly, including one's name as part of an electronic mail communication also may suffice, as may the firm name on a facsimile"... "One may use a digital signature with the requisite intention, or one may use the private key solely as an access device with no intention to sign, or otherwise accomplish a legally binding act. In any case the critical element is the intention to execute or adopt the sound or symbol or process for the purpose of signing the related record"

What is the E-Sign Act? In practice this legislation prepares a common and uniform "platform" among various States of the Union regarding the minimum standard of requirements for the electronic signatures. In this way it is possible to stimulate a better development of the electronic commerce. Coordinating the legislations of the countries of the USA (really different among themselves), this Act has the effect to overcome the legislative barriers in a way to recognize a legal validity of the documents created in respect of different government rules. The main principle of the Act is the principle of non discrimination of the documents concluded with the computer, solely because of the support used.

It could be asked what the difference between UETA and E-Sign Act is. The difference can be found in different areas of application of the legislations. The UETA scope of application is broader than the E-Sign Act. Infact the UETA regulates not just the commercial and private transactions (which are the scope of the application of the E-Sign Act), but also government transactions[34].

The interesting parts of the E-Sign Act for the purpose of the paper are: section 106 (definitions), section 101 (neutrality and not discrimination principles, limitation of the electronic sign), section 102 (duty for the member states of correct reproduction).

After the first look has been given given, it can be said that the Communitarian work[35] and the action of the American federal government[36], substantially have the same purpose. This purpose is to promote the electronic signatures and the principle of non discrimination of the documents concluded with the computer, solely because of the support used. This similarity is also confirmed by the points

---

[33] For the text of the E-Sign Act, visit the website http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f%3Apubl229.106.pdf

[34] It can be found the circle of application of the UETA in its preamble. It says:“With regard to the general scope of the Act, the Act's coverage is inherently limited by the definition of "transaction." The Act does not apply to all writings and signatures, but only to electronic records and signatures relating to a transaction, defined as those interactions between people relating to business, commercial and governmental affairs. In general, there are few writing or signature requirements imposed by law on many of the "standard" transactions that had been considered for exclusion.”

[35]With the scope to destroy the barriers of the e-commerce in the European market.

[36]Trying to create a common legal "substratum" and bringing closer the American states regulations which, before, prevented the development of the e-commerce.

in common between the two legislations and will be described in the second chapter.

2 Legal Issues of the Electronic Signature Regulations

2.1 The legal context in which the Regulation was adopted

2.1.1 The adoption of the regulations

2.1.1.1 EU: difficulties in the adoption

The necessity to give to the European community unitary norm on electronic signature has been felt from long time by all Members States but, the way to adopt a regulation has been long and difficult. It happened because the legislations of the European countries and also the fundamental guidelines on which the single laws had been written were heterogeneous. It is important infact to observe that inside the Union there were legislations in the sector adopting a prescriptive approach (as Italy or Germany), and legislations adopting a minimalist one (as UK). So, for writing the Directive, it was necessary to find a difficult balance between opposite approaches[37].

The intention of the legislator was to help the development of the e-commerce and to create similar norms in the Union. The first step on the adoption of the Directive was on 16 April 1997 when the "Communication on a European initiative in Electronic Commerce"[38] sent by the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee

[37] As example of the differences among the country legislations of the Union, read the article of Hindelang, "*No Remedy for Disappointed Trust? The Liability Regime for Certification Authorities Towards Third Parties Outhwith the EC Directive in England and Germany compared*", in JILT 2002 (1), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/ .
[38] Preamble number 1 of the Directive.

of the Regions, that underlined the importance of the digital signature in the actual and future world of commerce.

On 8th October 1997 the Commission emanated a Communication "on ensuring security and trust in electronic communication - towards a European framework for digital signatures and encryption" that has encouraged an approach inspired to coherence. We can also find in this Communication the definition of an exact figure in subject of digital signature and encryption[39].

Such communication had been welcomed favorably by the European Council that on 1st December 1997 invited the Commission to "submit as soon as possible a proposal for a Directive of the European Parliament and of the Council on digital signatures"[40].

The Commission has established, after a series of meetings with representatives groups of the Members States and cryptography industry (and with the help of the initiatives of Martin Bangemann and Mario Monti), criteria of safety and responsibility. In this way they were trying to guarantee that electronic signature shall be legally recognized in the whole European Union following the principles of free movement of services and the control in the country of origin[41].

This "long story" found a conclusion with the presentation by the European Commission of the proposal of the Directive regarding the electronic signatures on the 16th June 1998 and which later adopted on the 13 th December 1999.

2.1.1.2 USA: the delay of the federal legislation

Initially the opinion that considered it as necessary to have a legislation in the digital sector that could help the e-commerce was dominant. The legislative impulse in this sector started from the single states. Infact in the USA legal

[39] Preamble number 2 of the Directive.
[40] Preamble number 3 of the Directive,
[41] Which are the fundamental principles in the unique market but, anyway in respect of technological neutrality.

system, the legislative initiative can be taken both in the federal level and in the single states.

The first country (and also the first one in the world) that tried to regulate the systems of digital signature was the state of Utah, that, in 1995 has adopted a legislation called "Digital Signature Act."

Such law contains a technical rule on the composition of digital signature, a rule on the system with the couple of asymmetrical keys and an authorization for the state to release the digital certificates from the entrusted corporate body (then already existing in the United States).

After this first regulation, and as direct consequence of the strong legislative competition among the states of the American Union, there were the adoption, in a short time (almost all were adopted by only few months distance in time), of other states legislations. The problem arising from these legislations was that the single legislative choices were going in different directions: some of them followed the imprint signed by the state of Utah, others directed, in different way, toward legislations of the computer signature less "technique" (having probably the intention of stimulating its use reducing the level of technicality dictated by the norm). Other states chose an alternative amongst the two disciplines.

The adoption of legislations in this subject provoked the creation of an important problem of coordination among their rules. Infact, even if the adopted model and the technical rigidity regarding the structure of the signature are considered, every State possessed a heterogeneous and different legislation in comparison to the others (also with very distant technical solutions). This situation constituted real legislative barrier for electronic commerce.

It should also be considered that some of these legislations have assumed a greater importance, influencing the models selected from the national legislations of other countries, or from the international organizations. It can be given as example of this phenomenon, the legislation of the State of Illinois. It disciplines the subject from a technical point of view and with a minimalist approach,

creating a synthesis between the law of Utah and that one of California. Such law has been the source of inspiration for the National Conference of Commissioners on Uniform State Law for the layout of the first versions of the UETA (Uniform Electronic Transactions Act).

Despite this influence, the situation was still very confusing considering the various government legislations. And it remained the same after the first regulations of the Federal Government was adpoted. These regulations did not establish a common normative platform, but rather regulating only a particular aspect regarding financial factors.

The first regulation of the federal government was adopted in 1997 with a law (regarding the fiscal exaction) that introduced the electronic payment of taxes and the promotion of digital signatures and those electronics having the same value of the autographs signatures (at least in such sector).

Since such norm resulted as vague, a few months later, the American Federal Government adopted another regulation, regarding the financial activity[42]. With such law, the legislators in short created the first federal nucleus for the following discipline, equalizing all the techniques of signature approved by the government laws with the same requisites requested to the autograph signature.

The second footstep toward the regulation of digital signature in a federal level was in 1998 when the USA legislator introduced a regulation that allowed and stimulated the use of digital signature (in practice is known as the system of a double couple of asymmetrical keys) or other safe techniques (using the expression “electronic signatures”), following the parameters fixed by the same regulation.

[42]It tried to reduce the fragmentation that cam from government disciplines by creating a regulation that was applied to all financial operations, including any transaction of private persons and public corporate bodies.

Even when the first two steps were done, in the USA in 1998 was still not exist a common regulation with a real "corpus" of rules that could substitute (or at least guide) the single government legislations in existence.

Such "corpus" was adopted just in 1999 with the implementation of "E-sign Act" (a regulation having a strong relation in its contents with the UETA). Such Act doesn't totally substitute several national norms, but it eliminates legal conflicts between countries (that was becoming, as mentioned earlier, an unbearable barrier to the development of the use of e-commerce in the USA). It was done mainly by adopting a regulation with a minimalist approach that prescribes the principle of recognition of electronic signature[43].

Relation with the encryption systems.
EU: protection of the encryption for protecting the privacy.

In the adoption of norms on the elecronic signature, the opinion of the legislators on the encrypton systems plays a big role. In EU was not existing any fear of the encryption system (as there was in USA). Furthermore, considering that the privacy is a right protected in the EU, the encryption systems were considered a usefull instrument to protect the privacy.

Proof of this approach are the Guidelines on Control of the Encryption in March of 1997[44] of the Organisation for Economic Co-operation and Development ('OECD'). The guidelines accept the right of the Memeber States to act in defence of their national interest, but also set out two important principles: - "Users should have a right to choose any cryptographic method, subject to applicable law" (principle 2);
- "The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national

[43] A country in which the pressure towards the electronic commerce was and is the strongest in the world, with a big number of commercial transactions concluded through telematic systems and in which every form of payment can be effected (taxes from enterprises or assigns that the citizens use every day for example).
[44] Visit the website http://www.oecd.org/dsti/iccp/crypto_e.html

cryptography policies and in the implementation and use of cryptographic methods" (principle 5).

In particular the comment on the principle two is interesting: "Government controls on cryptographic methods should be no more than are essential to the discharge of government responsibilities and should respect user choice to the greatest extent possible. This principle should not be interpreted as implying that governments should initiate legislation which limits users choice".

The Guidelines show the importance given in the EU to the encryption systems; it can be said that the encrytpion is considered, as "guard of the privacy".

2.1.1.3 USA: fear of the encryption systems

The situation in the federal level was different and particular. Infact in the analysis of the American system, it is important to underline the critical approach of the American government towards the encryption systems.

In the approach of the United States, the legislator's perception on such technologies was different from those of other states because those technologies were considered as the "war weapons"and accordingly dangerous. Infact the encryption systems guarantee "almost certainty" of the secretiveness of the communications. This aspect has not always seen in a positive way, considering the possible uses for illegitimate purposes (give as example the today's terrorism)[45].

Furthermore, the USA Constitution does not protect directly the privacy. Infact the Fourth Emendament just guarantees 'the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures'. The protection of the privacy derives solely by the interpretation (the so called 'penumbra right of the Constitution') done by the US Supreme Court[46].

---

[45] Read the article of Akadeniz. See note nr.9

[46] Read the US Supreme Court such as Griswold v. Connecticut (1965) 381 US 479 and Roe v. Wade (1973) 410 US 113; those cases shows that privacy has been given constitutional status when the freedom of speech and the First Amendment is not in issue.. See also Katz v. United States (1967) 389 US 347 the main case regarding the privacy for electronic communications.

Therefore the past regulations on the encryption systems, as the International Traffic in Arms Regulation ('ITAR'--22 CFR ss 120-130) the Arms Export Control Act ('AECA' -22 USC ss 2751-2796d), restricted the export of cryptogram software or equipment which generates keys more than 40-bits in length[47].

Currently the things in USA have not changed much. Infact the current international situation and the diffusion all over the world of such technologies have made this problem more pressing than ever.

2.1.2 The Relation between Supranational Regulation and the Country Rules

2.1.2.1 EU: a clear situation.

Before analyzing single parts of the two regulations it is important to observe the relation between the Communitarian Directive and the rules of the single EU countries and between the federal (USA) regulation and the rules of the single American countries.

In the EU context when there is an adoption of a Directive, the Communitarian sources prevail on those of the single Member State, but it prevails in a particular way. Infact from the adoption of a Directive two important consequences derives:

- The single Member States have to adapt his legislation to the Directive;
- The Directive (diffently from the regulament) is not directly applicable in the single Member States.

2.1.2.2 Usa: a not totally clear situation.

In the USA the situation is not so clear. Observing the constitution of the United States, it is possible to note that the American system prescribes the prevalence of the federal rules on the norms of the single country of the Union and from this prevalence it derives a duty of application for the judges of the federal rules.

---

[47] By the way, it must be said that AECA and ITAR are challenged in the US Courts suspected of unconstitutionality and of the violation of First Amendment right to free speech. There are three current similar cases:*Karn v. US Department of State and Thomas E. McNamara*, *Bernstein v. Department of State*, and *Junger vs. US Department of State.*

The American doctrine, in the interpretation of the constitutional text, however, does not want to eliminate the autonomy of the single states in the subjects of their competence (according to the constitutional text) every time a federal law regulates the same subject. In fact, in contrast, the doctrine thinks that the article VI of the American "Bills of Rights" is a clause for saving the homogeny of the single country legislations. Having this as a scope, that article is useful as parameter of constitutionality in case of conflict among the regulations in force in the states and the federal norms[48].

From the foregoing, it can be said that the federal norms do not prevail on those of the single states of the USA except in the following cases:
if there is a norm that expressly says that;
in case of a conflict among the "country-law" and an express federal political direction;
when the federal law expressly gives exclusive competence to the federal legislator in some sectors.

Based on this general explanation, it can be observed that in the E-Sign Act there is no general disposition that gives prevalence to the federal norms. Furthermore, the way in which the norms are written suggests that is not the intention of the federal legislator to substitute his text to the single government legislations.

Perhaps, it is also necessary to analyze the single disposition. Infact the E-Sign Act can be divided into two parts. The first one, regarding the principles, is immediately applicable and in force without possibility for the states "to escape". In other words the states are forced to suit themselves to such articles (following the constitutional principle mentioned earlier)[49].

[48]Informations took from A. Gambaro e R. Sacco, "*Sistemi Giuridici Comparati*" UTET editor, 1996, pp. 164-191.
[49] For more informations, Arruda & Shestakova, *US Enacts E-Sign: The Electronic Signatures in Global and National Commerce Act*", visit the website http://www.cla.org/usenacts.pdf.

In contrast, the second part of the E-sign Act (that consists of rules of technical character) does not express general principles. Thus the states are free to conform or not their regulations[50].

For the states that do not follow the E-Sign Act, the federal legislation prescribes several obligations: the government legislators not adhering to the Act and those who want to intervene in the subject, have to include in their legislations the requisites and the procedures of the signature. The countries, in the creation of various typologies of different electronic signatures, also have to act in conformity to such principles. It is also forbidden to introduce a legislation of prescriptive type (it is like to choose a particular kind of technique and to recognize only to it value) as this would be in contrast with the principles of the E-Sign Act, and therefore unconstitutional for contrasting the principles expressed by the federal law (following the article VI of the American constitution).

In the case of adoption of a regulation after the implementation of the E-Sign Act, this new regulation has to follow the lines of the federal text, and in such way to connect itself to the same one.

Therefore, the idea previously expressed on the possibility to classify the E-sign Act in two categories of norms is now, looking better, correct. Infact, in line of what was mentioned earlier, the federal legislator prefers to regulate expressly the principles that can not be changed and for the part changeable, it establishes when and how the modification is possible. The existence of principles that can not be changed confirms the importance that the principles of technological neutrality and non discrimination of the computer documents that have been assumed in the American system[51].

---

[50] Many states (18 states accepted and 2 states with modifications), before the introduction by the American federal government of the E-Sign Act, had already their own regulations in subject. Some were based on a "myopic vision" of the phenomenon as founded just on the comparison with the world of the papery document; others had modified and distorted some points of the UETA (with the purpose to adapt this last text with the respective normative government) not following the principle of the "precise reproduction" contained in the section 102 of the E-Sign Act. Information took from the article of, Ewing, Remick & Saul, "*New E-Signature Laws Click Into Action*", visit the website http://www.saul.com/articles/int2.htm visitated on the 20th May 2005.

[51] The federal legislator has the opinion that the best choice regarding the technique of signature of a computer document, should always be done by the market.

2.1.3 Comparing the two legal contexts.

From the description of the contexts where the norms were adopted, some points should be noted.

First of all, about the encryptions systems there were an almost opposite opinion. As mentioned above, in the EU the encryption was considered as "guard of the privacy", while in the USA the encryption was seen as a "weapon".

Probably the particular way of conceiving the danger of such techniques is the reason of the type of approach chosen by the United States. Firstly, the fear caused a delay of the federal legislation in this sector. Infact when the federal legislation was adopted, several regulations in the single countries already existed. And when the federal legislator decided to deal with this sector, it had to find a balance to harmonize all existing legislations in the USA. So the American legislator decided to adopt an approach so-called minimalist, that allows the validity of a document, even if not signed or crypted with a cryptographic complex technique[52].

About the relation between supranational regulation and the country rules, it can be said that both legislations give some freedom to the single state regarding the way to adapt their own legislation to the Union legislations. The difference is that the situation in the USA about the relation between E-Sign Act and the single country regulation is still not as clear as the one in the EU[53]. It could create an uncertainty that can be confusing.

---

[52] Information taken from Stephen E. Blythe, the Richmond Journal of Law and Technology:"*Digital Signature Law of the United Nations, European Union, United Kingdom and United States: promotion of growth in e-commerce with enhanced security*", from the legal review Westlaw.

[53] Read the Article of Arruda & Shestakova, "*US Enacts E-Sign: The Electronic Signatures in Global and National Commerce Act*", San Francisco.

2.2 Definition and limits of the e-sign

2.2.1 EU: several types of Signature

As it is written in the Directive, the electronic signature has the scope of authenticating data or, better, to guarantee the origin of one data.

In different way from the American regulation, the European Directive provides three types of electronic signature with different levels of safety: electronic signature, advanced electronic signature and sure signature[54].

The approach followed by the Directive from one side recognizes the validity of electronic signatures and does not distinguish between a mechanism using a "software or a hardware"[55]. From the other side, it attributes greater legal effect to certain widely used techniques.

The electronic signature in the Directive is defined in article 2 as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication".

From such definition it is easy to understand that the Directive expressly mentions two types of functional connection between electronic signature and the document: the signature "attached to the data" (with reference to a signature contained in the same file) and the signature "to data connected through logical association" (that it refers to a signature contained in a different file).

The effect of using "regular" electronic signature is that, at least, it[56] can not be "denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

---

[54] Gambaro & Sacco, "*Sistemi Giuridici Comparati*" UTET editor, 1996, pp. 164-220. Read also Monti, "*La crittografia, l'Europa e l'America*", visit the website http://www.interlex.it/attualit/amonti49.htm , visited on 15th of March 2005.
[55] Mechanisms using peculiar data, like codes or keys public cryptograph, attached or connected (through logical association) to other electronic data as "method of authentication".
[56] Article 5 (paragraph 2) of the Directive.

- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
not created by a secure signature-creation device."

The advanced electronic signature is "an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable".

The last point is probably that most interesting considering the specific technologies that able to show incontrovertibly if the text of the document to which the signature attached has been somehow altered. This is certainly a "plus" (one more requirement) of this particular electronic signature compared to the autograph signature: but this requirement has to be considered correctly, considering the extreme facility of change of the digital datum. The advanced electronic signature "will have the same value as a hand written signature and be admissible as evidence in legal proceedings"[57].

The third and safest level of electronic signature, the "sure signature, is characterized by a better ability to find every change of the text signed. In this way, it is made stronger than what was done for the "advanced electronics signature"[58].

---

[57] Those are the words of Hindelang commenting on the effects of the advanced electronic signature (article 5, paragraph 1 letter b of the Directive) in **"***No Remedy for Disappointed Trust? The Liability Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in England and Germany Compared"*, in JILT 2002 number 1, visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/ .

2.2.2 USA: just one definition

The norm that deals with the definitions of electronic signature is the section 106 of the E-SIGN Act.

The electronic signature is defined as an “electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record”.

A definition that, in the literal formulation, seems really wide compared to the European one; but, if it is considered better, the two definitions are generally equivalent. Infact considering that sounds, symbols and procedures are also definable as "data set in electronic form", the two definitions have the same meaning.

The section 101 of the norm prescribes, for balancing the liberty recognized by any state to regulate the phenomenon of electronic signatures with more rigid parameters, two fundamental principles of the American federal system. The first one of them recognizes the legal effect, simply for the fact that concluded on electronic support, of every transaction with electronic signature, national or not, effected in conformity to the requisites required in section 106 (the possibility to identify the holder of the signature).

The second of the two principles stems from the first one and it concerns the contracts concluded in electronic form, recognizing full legal effects to them. It is, however, not allowed to deny legal effect of such contracts simply for the reason of the electronic way of conclusion.

Reading the definition we can note the word “intent” to sign. It means that the judge has the task, in his judgment, has mainly to find the intention to sign. This is an important indication of the E-sign Act that the EU legislation does not have.

2.2.3 Comparing the definitions

From what has been said about the definitions, three points deserved to be underlined.

First of all, already from the definitions and from the several types of signatures existing in the EU Directive (in the USA there is just one type of electronic signature), it is possible to see the different approach adopted by the EU legislator from the USA one. The EU legislator, still considering the technological neutrality, in practice follows the “two floors or level” approach. Infact, the EU legislator creates a “time-resistant regulations by setting requirements for e-authentication methods with a certain minimum legal power (minimalist approach) and by attributing greater legal effect to certain widely used techniques (prescriptive approach)”. The USA legislator follows the “minimalist” approach; the regulation infact is written following really (and not just in the the declarations the principle of technological neutrality [59].

Secondly, reading the two definitions of electronic signature, it is possible to find an important difference between the two legal systems. The USA definition of signature gives more importance to the intention, while the EU one just says about a means that “serve as a method of authentication”. From this word we can see the different view of the European system on the importance of the intention of the signer for recognizing legal effects to the signature. It has relevant consequences. Infact in the case of signature composed by symbols or sounds or computer trials, the EU judge (in contrast with the USA judge) does not consider the intention to attribute to such combination of bit the meaning of "signature"; but he considers generally the reliability (in comparison to the content of the same document and its degree of reliability)[60].

Thirdly it is not totally clear if the two definitions of the electronic signature are really equivalent. One doctrine infact wonders if “the EU definition include any sounds and symbols like the US one or does it depend upon the European

[59] The technological neutrality will be discussed more in the third chapter.
[60]This is the only definition of electronic signature existing in the federal legislation of the USA .

governments to interpret this provision according to international standards. However, if this is the case, who sets up these international principles and how mandatory can they be? In addition, what if each and every Member State- for political and profitable reasons- recognizes and validates either different or exclusively specific forms of e-signatures?[61]"

2.3 Certification Authorities

The mechanism of the digital signature needs, for its operation, a "Trusted Third Party" who receives a whole of information, verifies them and guarantees them for another physical or juridical person. Therefore, the essential function of the provider is, as mentioned above, to guarantee, through the certification, the correspondence between a subject (or particular attributions of the subject) and a signature[62]. The certification, in practice, creates a correspondence in both directions between a determined subject and a determined digital certificate.

When the countries regulate the providers, it is necessary to choose between providers authorized for the emission of certificates and forms of accreditation or voluntary authorizations (in some countries an absurd situation happened where it was not clear if some Countries requires or not an Authority of Certification to be "de facto" authorized; this, for example, has happened in Malaysia and Singapore[63]).

---

[61] This is the point of view of Spyrelli, "*Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication*." In JILT 2002 (2), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/ .

[62] As Hindelang stated in the article mentioned previously:"Since our new signatures will consist only of a binary code somebody must link this code with our identity. This function is performed by CAs, stating both the identity and binary code in one electronic document called certificate".

[63] It is usefull to read Zainul " *Comparative Analysis of the Malaysia Digital Signature Act 1997 and the Singapore Electronic Transaction Act 1998*, done in the 15th BILETA Conference in the University of Warwick: "ELECTRONIC DATASETS AND ACCESS TO LEGAL INFORMATION", visit the website: http://130.159.238.165/Document%20Library/1/Electronic%20Commerce%20-%20the%20Malaysia%20Digital%20Signature%20Act%201997%20and%20the%20Singapore%20Electronic%20Transaction%20Act%201998.pdf.
In particular, on how the system of the Certification Authorities in the two countries works, Zainul states:" In Malaysia, licensing of Certification Authority is mandatory. At the moment, DigiCert is the only licensed Certification Authority in Malaysia. This approach is adopted so that there is uniformity in the certification industry, and that regulation of digital signatures can be done more

In general it can be said that the plan and also the desire of many legislators are to have Certification Authority as something in the realm of public sector. Experience has however denied such perspective. Today we in fact notice that such authorities are established and primarily operate effectively in the private sector.

2.3.1 EU: the Directive deals with this topic

In the Directive 1999/93 EC the Certification-Service-Providers are defined as: " an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;"(article 2, paragraph 1).

---

effectively, altough it was argued that licensing TTP, instead of increasing security, will in fact make electronic commerce less secure.
Therefore, in Malaysia, a digital signature is legally valid only if it is certified by a licensed Certification Authority.(…) Although in Malaysia, licensing of Certification Authority is mandatory, this does not mean that a certificate issued by an unlicensed Certification Authority is invalid. In fact, the Act specifically provides that the licensing requirements under the Act shall not affect the effectiveness, enforceability and validity of any digital signatures.The Act further provides that the liability limits for certification authorities and the effect of digital signatures, as provided for under the Act, shall not apply to unlicensed Certification Authorities.Therefore, if an unlicensed Certification Authority is used, the validity of the digital signatures would be governed by a contract between the contracting parties, instead of the Malaysia DSA.
The Singapore ETA adopts a different approach. Licensing under the Singapore ETA is voluntary so that closed network may use their unlicensed Certification Authority. But, It is not correct to assume that Unlicensed Certification Authority is not regulated. They would still have to abide with other relevant provision of the Singapore ETA, such as the duties of certification authorities. In Singapore, digital certificates are recognised if there are issued by three bodies; licensed Certification Authorities, foreign Certification Authorities recognised by the Controller of Certification Authority, Government Department or Ministries approved by the Minister and the parties may expressly agree between themselves to use digital signature which is property verified by reference to the sender's public key".
For more information about the two legal systems, read Annamalai, Nagavalli "*Cyberlaws of Malaysia - The Multimedia Super Corridor"*, 1997, 12 Journal of International Banking, p 473; Alkeniz et al "Cryptography and liberty: Can trusted third parties be trusted?", 1997 in http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_2/akdeniz/#a2.2 ; Ter, Kah Leng New Laws on "*E-Commerce: Singapore"*, 1999, Computer Law and Security Report Vol 15 No 1, p 8; Wu, Richard *"Electronic Transactions Ordinance - Bulding a Legal Framework for Ecommerce in Hong Kong"*,1999, the Journal of Information Law and Technology (JILT), http://www.law.warwick.ac.uk/jilt/00-1/wu.html ; Seng, Daniel, !"*Legal Guide to the Electronic Transactions Act"*, 1999.

It is important to observe the expression "Certification-Service-Providers". The Directive chooses a very wide and comprehensive philosophy and does not use directly the expression “Authorities of Certification”. In the similar way, the legislator also includes the suppliers of the services of temporal validation, the so-called ones "electronic notaries" and the suppliers of the services of electronic filing.

The purpose of the Directive is to list the requisites necessary for the operation of the provider of certification services. It was done with the aim to harmonize the legal view of the Member States and to help the development of the sector.

Even giving the possibility to the Members States to introduce or to maintain the systems of optional accreditation in a way that encourage a certification services of more elevated level without any limitation of numerical type (and provided that the conditions related to such systems of accreditation are objective, transparent, proportionate and not discriminatory), the Directive forbids the Members States to subordinate the performance of certification services to prior authorization.

The EC Directive in its article 3 (paragraph 1) states that the “Member States shall not make the provision of certification services subject to prior authorization”[64]. The expression "prior authorization" is important to understand the plan of the legislator. Infact, it does not only refer to a decision from national bodies that allows the providers of certification services to practice their activity, but also includes every other measure having equivalent effects.

Furthermore the Directive in article 3 (paragraph 2) allows Members States to "introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision", provided that subject to conditions that are "objective, transparent, proportionate and not discriminatory "[65].

---

[64] For example it is the case of Italy that has as authority the AIPA.

[65] Article 3.2 says: “Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent,

The Directive provides an important difference between "certificate" defined as " an electronic attestation which links signature-verification data to a person and confirms the identity of that person " and "qualified certificate" as "a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II"[66].

In general there are many kinds of certification providers, other than those mentioned in the EC Directive. For example there are the providers of certification services that issue "certified not qualified" and the providers of certification services that issue certificates which are different from the certificates of identity. But probably other certifications exist also.

2.3.2 USA: no rules about that

The role of the Certification Authorities is of extreme importance for their strategic role in the system of the signature (electronics and digital) and for the fear felt in the USA as it was mentioned above. Therefore, as we have seen, such role is fundamental in the structure of such techniques. Unfortunately it is hard understand why, in a fundamental regulation like the E-Sign Act, there is not reference to the Certification Authorities. Trying to be more precise, the problem of the creation of authorities is resolved from every single state, but there is no unitary discipline in this subject.

Missing, at the moment, a unitary regulation about the certification provider, in the USA it is felt the necessity of a federal regulation in this subject. Considering the Acts in force at the moment in the federal level, it should be considered the

---

proportionate and nondiscriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive".
In general we can say that the Directive works in the direction of the trust on the overall "development technological-market" by confiding more and more in elevated safety standard.

[66] Definition as provided in the article 2 of the Directive.

"Electronic Financial Services Efficiency Act" of 1999. This Act proposes the creation of a federal Authority that picks up the various national authorities, attributing them the possibility to offer the services of certifications qualified in a national level (or better in all the states) and forbidding the possibility to offer such services to the other authorities that stay out from this association[67]. Furthermore a committee is established for the revision of the safety standards of the authentication of the signer (the only principle required by the norm), and the adoption of a norm containing the rights and the duties that must be observe from the corporate body certifiers. But until this moment, such federal authority has not been established in the USA.

Other proposals, instead, go in the direction to recognize the right of a single state to create bodies of certification authorized or accredited by the state, or from other supranational corporate body with such power.

Trying to find a reason that explains the lack of legislation in such subject in the USA (country in which the deposit of the private key to a provider, could resolve the "fear" to use these cryptograph techniques), we can try to imagine some explanations. Probably the reason lies in the choice and, speaking in general, in the philosophy to give to the market the power to develop the system in the manner it prefers. The USA legislation heads therefore in the direction of a voluntary accreditation of the corporate body (with the liberty to choose its own standards and safety rules).

This way was chosen by the legislator because they want to avoid, in indirect way, to influence the choices about the techniques of conclusion of a contract (in respect to the liberty for the parts, established by the federal normative).[68]

---

[67]The text is available on the website: http://dreier.house.gov/efsea.html .

[68] To have an example of the way of dealing with the problem of the certificators from single country of USA, read the article of Travis Schwaer, "*Electronic Signature Laws Provide Texas Agencies Secure and Legally Binding Online Transactions*" visited on the 20th of April 2005 on the on-line search engine West law (read in particular pp. 5 and following).

2.3.3 Comparison about the Certification Authorities.

The comparison of the two regulations about the Certification Authorities is the confirmation of the different approaches of the two legislators that was explained in paragraph 2.3.3.

An interesting question is if a two floors level legislation needs an adaptation to technological development. It is certain that this is not a problem for the USA regulation, considering their minimalist approach, but it can be a problem for the EU legislation that clearly adopts an "hybrid" approach.

A part of the doctrine says that the European Directive is time-resistant because it "does not specify only one technology but leaves room for future technologies to develop and comply with extra requirements as well"[69]. Heading in the same direction is the ILPF's Analysis of International Electronic and Digital Signature Implementation Initiatives.

Those opinions are generally true but the facts leads to the opposite direction. Infact already in the year 2000 the European Council stated that the technological development probably needed the adoption of 'new and more flexible regulatory regimes' [70] . It will not be surprising if in some years the EU Directive will be modified to adapt to new technologies.

From the above, another difference arises between the two legislations. The USA regulations do not need "updating", while the EU one, referring in practice to particular technologies, can quickly become old.

2.4 Points of convergence between the EU and the USA legislation and, in particular, the Principle of the recognition of the electronic signature.

---

[69] This is the opinion of Spyrelli, see above.
[70] Presidency Conclusions of the Lisbon European Council, Rapid Press Release of 28 March 2000, PRES/00/900, visit the website http://www.europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=PRES/00/900|0|RAPID&lg= EN .

It is also possible to find many points in common between the two legislations. As it was said, for the scope of this paper, in general, it is less important to discuss about the points in common than the differences. To be brief in this part, it must be said that both legislations recognize the legal validity of an electronically signed contract.

Secondly, both legislations prescribe that the electronic signature is considered as legal equivalent of a hand-written signature only if the requirements for hand-written signatures are fulfilled[71].

Thirdly, it is important to remember that both regulations guarantee the Transnational Interoperability and Recognition of e-sign products and services (certification, archiving, storing of electronic records, trust services, etc.)[72].

Fourthly, both the US[73] and the EU[74] legislations traits of consumer protection.

---

[71] This point is expressed in the artiche 5 paragraph. 1 of the EC directive that says: "Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data"; and section 101 letter b of the E-Sign Act says "This title 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".

[72] Article 7 of EC Directive in its paragraph 1: " Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised 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 this 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 this Directive guarantees the certificate; or
(c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations."

[73] Read section 101 of the E-Sign Act letter c called "Consumer disclosures", number 1 and 2 letter A and B. Using the words of Arruda & Shestakova, "The Act is highly consumer-oriented and requires painstaking care to devise a program to issue acceptable consumer notices or disclosures electronically. It was Congress's intent to provide consumers with the same level of protection in the online world as they enjoy in the off-line world."In particolare are guranteed:
• right of the consumer to obtain the record on paper;
• mechanism for the withdrawal of consent;
• conditions, consequences, and fees, if any, associated with the withdrawal of consent;
• scope of information encompassed within the consumer's consent to receive it electronically;
• consumer's right to obtain information on paper; and
• hardware and software requirements to access and retain the electronic information,

The European law and the E-sign Act provide different ways of protecting the consumer such as:

- information to be disclosed in writing to the consumer, whether in electronic or other forms;
- consent of consumer is required to contract electronically with the e-sign;

the consumer, prior to consenting, is provided with a clear and conspicuous statements and information.

But probably the most important point in common between the two legislations is the Principle of recognition of the electronic signature.

2.4.1 UE: articles 1.1 and 5.2 of the Directive

The article 1, paragraph 1 says: "The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the internal market".

The principle of recognition is specified better in article 5 paragraph 2, that prescribes that "the Member States shall ensure that an electronic signature is not

---

including any changes to these requirements".

[74] In the EU context, it is the "Framework directive" that deals with this issue. For a useful explanation it is enough to read the words of Hornle, in her article called "*The European Union Takes Iniziative in the Field of E-Commerce*", in JILT 2000 (3), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/ . She says: "The Framework Directive then provides that, for (standard) contracts with consumers, the supplier must clearly set out the steps for the conclusion of the contract, unless the contract is concluded by individual communication such as e-mail (Article 10(1)(a) and (4)).[…] Furthermore the supplier must acknowledge the receipt of the consumer's order (Article 11(1), again, this provision does not apply if the contract is concluded by individual communication such as e-mail, Article 11(3)). Unlike previous proposals, the Directive now leaves open the question as to when the contract is concluded.The supplier must give the consumer a chance in the ordering process to detect and correct errors (Article 11(2), again, this provision does not apply if the contract is concluded by individual communication such as e-mail, Article 11(3)). It should not be also forgotten that the Framework Directive (art. 6.1) gives to the consumer the right of withdrawal from the electronic contract in 7 days, with the condititons and the limitations written in the artiche (art.6.3)". The issue of the consumer's protection also dealt by Chissick, Michael and Veysey, Guy, in "*The Perils of On-Line Contracting*", in CTLR Issue 5, 2000; read also Julià-Barceló, Rosa, "*A New Legal Framework for*

denied legal effectiveness an admissibility as evidence in legal proceedings solely on the grounds that it is:
- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
not created by a secure signature-creation device".

It completes the principle of recognition found in article 5 paragraph 1 letter b that says: "Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: […] (b) are admissible as evidence in legal proceedings".

The same legal effects are guaranteed when the signature is certified by a provider of certification services established outside the European Community and does not operate the conditions provided of the article 7 of the Directive. Infact the article 7 paragraph 1 says: "Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised 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 this 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 this Directive guarantees the certificate; or
(c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations".

Electronic Contracts: The EU Electronic Commerce Proposal", in Computer Law & Security Report Vol.15 no.3 1999.

2.4.2 USA: section 7th of the UETA

Section 7th of UETA deals with the principle of equivalence of the electronic signatures (or, better, of the effects of the contracts signed electronically) to the autograph signature simply because it is signed in electronic way (so not giving importance the techniques used). The only requirement requested to the signature is its univocal correlation with the document. This is also requested in many others legal system, for example, in Italy when the signature used in documents with separate computer evidence[75].

Therefore, section 7th prescribes the principle that constitutes conditions necessary for the computer signatures among the subscribers from different states of the confederation. The lack of a principle of the recognition would in fact determine in general a heavy disincentive to the transactions that use some electronic signature and particularly a considerable deceleration of the electronic commerce.

The importance of the principle of recognition, enunciated in the section 7th of the law (so similar in its contents to that one adopted by the European Commission to harmonize the disciplines of the launchings in Europe), is also understandable in the activity of the US Congress. This, in the adoption of the E-Sign Act, has encouraged Members States to adopt the UETA (and many occasions the E-sign Act cited the UETA) and creates a view of liberty (liberty that consists in the possibility to freely regulate in subject) for those States who will introduce the principles of the UETA, principles considered fundamental from the same congress.

As a proof of the importance of the principles of the UETA in the US system, it must be said that they can modify (limit or replace) the federal legislation. It can

---

[75]Section 7th says:"This act simply assures that the signature may be accomplished through an electronic means. No specific technology need be used in order to create a valid signature. One's voice on an answering machine may suffice if the requisite intention is present. Similarly, including one's name as part of an electronic mail communication also may suffice, as may the firm name on a facsimile"... "One may use a digital signature with the requisite intention, or one may use the private key solely as an access device with no intention to sign, or otherwise accomplish a legally binding act. In any case the critical element is the intention to execute or adopt the sound or symbol or process for the purpose of signing the related record"

also impose on the states not adhering to the UETA, the adoption of a series of federal acts having equivalent contents (the principle of technological neutrality contained in the UETA).

3 CONCLUSIONS

3.1 Differences between the two systems and Technological Neutrality.

The first two chapters have had the scope of underlining the differences between the Communitarian system and the American federal system, without judging the choices of the legislators, but explaining in an objective way the particular aspects of the regulations.

Analyzing the differences of the two legislations, it will be possible to focus on the effects and reasons of the choices of the two legislators. In particular it will give the possibility to deal with the issue of the technological neutrality.

By considering the definitions, it is possible to observe, as we saw, that the European legislator regulates more than the American one. Infact the European Directive introduces three levels of safety, while the American legislator considers the signature just as link between a record and a person that have the intention to sign it. What is the effect of this difference? The choice of the European legislator from one side will perhaps guide more users of the electronic signature. From the other side and in contrast, it should be underlined that the guide provided by the European Directive can reduce the freedom of the users to use the mechanism that in practice they prefer.

Another difference between the European legislation and the American one is that one concerning the certification providers. This is probably the most evident difference between the two systems. As it was shown in the second chapter, the

European Directive regulates the Certification Authorities, while the American one does not. The effect of this is that in the USA, the market will decide what the right rules are for the Certification Authorities. And when the market find another better technological means, falling in the scope of the electronic signature, it will not be necessary to modify the regulation because it is neutral.

This different approach about the certifications providers and also about the definitions of the two legislators gives the possibility to show another and probably the most important (by considering the approach of the legislator) difference between the two systems analyzed: the different level of technological neutrality obtained by the two legislations. Each of them considers themselves as technologically neutral, but the legislation of United States has, for sure, a higher level of neutrality.

As it was said, it is possible to see the different level of technological neutrality by considering the regulation of the certification providers and the definitions of the electronic signature. Infact it is possible to observe that the European legislator, stipulating the different kind of e-signs and about the Certification Authorities, refers indirectly to some technologies in particular, while the American one is totally generical and a-technical. According to the words of Spyrelli, the EU Directive moves considering that 'sole tree form the whole forest', while the USA legislation do not have this approach[76].

What is the cause of these different approaches about neutrality? It is difficult to have certain answer, but probably it derives from different economical view and from different mentalities.

In Europe, it is still possible to see today that the trust in the use of computer techniques for the conclusion of contracts is not so high. Infact, such techniques are surrounded by a halo of uncertainty from the operators. This uncertainty is perceived by the legislator, who tries to gives clarity to the system through a

[76]Spyrelli "*Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication*." In JILT 2002 (2), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/ .

discipline that deals in practice with the technology in used today, reducing the uncertainty. In this way the legislator wants to give the idea of stability, rigidity and certainty of the computer techniques to the consumer which, increasingly uses the new instrument of virtual communication. Even at the moment, the computer for concluding contracts is not used in the EU, as in USA, for the persistent preference for the traditional paper instruments.

In USA, the electronic commerce was already largely developed and used when the federal legislator adopted the E-Sign Act. The only intention of the legislator was to eliminate the legislative barriers that prevented a complete development of the electronic commerce inside the country. Then the legislator chose to act without reducing the freedom of the single state to legislate in subject. The solution was to adopt a normative with a low prescriptive profile that removed the interstate obstacles and that liberalized the market totally. Focal point of the normative is the extreme trust given to the market, giving the possibility to the operators to choose the technique to use and guaranteeing the right to be listened in trial on the motivations that have brought to such choice. The legislator does not guide the market but, in the opposite way, the market makes choices and the legislator follows them and gives them legal effects[77]. And it must be said that the American system has had great advantages from the introduction of this Act. Infact the E-Sign Act, unhooking the idea of the commerce transaction from that one of the paper document, has been able in overcoming the difficulty, diffused in the legal systems, to conceive the commerce in different ways from those traditional.

Generally it is possible to say about the technological neutrality that there is a trade-off between “to give freedom” and “to regulate”. The USA is more in the direction of the freedom, while the EU follows more a position of the regulation[78].

---

[77] R. Gates said the following about the USA law:"The new law sets up a framework for trust. The major change is this will provide a legal framework for doing things on the 'Net that heretofore didn't exist. As people try to deploy digital certificates as a way to provide more enforceability around things that happen over the Internet, you need a legal structure that still protects the same legal structure that protected them in the paper world'. Took from the Article of Spyrelli (see above).

[78] Without trying to give any judgement about the technological neutrality, the words of Nemmar “*Emerging Trends in Commercial Law: Surviving Tomorrow's Challenges*”, DePaul Business & Commercial Law Journal, 2004, deserve to be said: “Despite those who argue for rights-restriction,

3.2 Possibility of the development of the e-sign sector with an activity of international harmonization.

In this paper it is possible to see how the harmonization is considered as an important aim to achieve. It should not be forgotten that the harmonization is an aim not just inside the EU or the USA areas, but also between all countries in the world. Infact if it is considered that the electronic commerce transactions are often done by subjects in different countries, it is easy to understand the importance of adopting legislation with similar principles.

This activity of harmonization can mainly be done by international agreements, conventions and organizations (as the WTO). They are the elements that can reduce the differences between the legislations of different countries. A big role can also be played by the legislations of the UE and the USA with “programmatic rules”, rules that guide the future activity of the legislators.

In EU, the need for an activity in the direction of an internatonal harmonization is expressed by the preamble 23 of the EC directive. It says: “The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial”.

Two important rules regarding the international harmonization are stated in article 7 (paragraph 2 and 3) of the EC Directive that prescribe the activity of the Commission in that sense. In particular article 7 (paragraph 2) says: ”In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the

---

the past several decades have witnessed an expansion in protected rights in intangible assets .... The first is that new information technologies and communications systems have altered the nature of value in the economy; law responds to that change”.

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 pargraph 3 is applicable when Community undertakings encounter any difficulties with respect to market access in third countries. In this case the Commission, when informed, 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"[79].

In the USA, the E-Sign Act dedicates the Title III (section 301) to the Promotion of International Electronic commerce. It stipulates the activities that the Secretary of Commerce must do in this sector[80]. In particular he "shall promote the acceptance and use, on an international basis, of electronic signatures in accordance with the principles specified in paragraph (2) and in a manner consistent with section 101 of this Act. The Secretary of Commerce shall take all actions necessary in a manner consistent with such principles to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and foreign commerce".

The principles that the Secretary of Commerce has to follow are stated in number 2 of the same section:

[79]Paragraph 3 continues to state that "Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements".

[80] It is possible to read the section 301, as amended by the H.R. 1714 on the website http://www.techlawjournal.com/cong106/digsig/hr1714tIII.htm (visited on the 24th of February 2005.

- "(A) Remove paper-based obstacles to electronic transactions by adopting relevant principles from the Model Law on Electronic Commerce adopted in 1996 by the United Nations Commission on International Trade Law.
- (B) Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced.
- (C) Permit parties to a transaction to have the opportunity to prove in court or other proceedings that their authentication approaches and their transactions are valid.
(D) Take a nondiscriminatory approach to electronic signatures and authentication methods from other jurisdictions"[81].

About the third principle in particular, it should be noted that it has to be in coordination with Section 5 and 7 of the "Model Law on Electronic Commerce" adopted by the UNCITRAL about the validity of a contract concluded in electronic way.

In making a comparison between the EU regulation and the USA one, it must be said, first of all, that section 301 is the source that inspired all regulations in the sector of international harmonization. Infact the UNCITRAL and the EU[82] regulation have followed the direction of the USA legislation[83]. Consequently, the two articles are similar, going both in the direction of the international harmonization.

Secondly, the USA legislation, describing the principles the Secretary has to follow, gives clear criteria that must be followed during this activity. These

[81] The letter b of the same part prescribes that "In conducting the activities required by this section, the Secretary shall consult with users and providers of electronic signature products and services and other interested persons".
[82] The principles introduced by the UE legislation in this sector, really similar to Usa those, went in opposite direction compared to the normative of some European country as Italy or Germany (countries developing prescriptive regulations).
[83] Information coming from Smedinghoff *"The Legal Requirements For Creating Secure And Enforceable International Electronic Transactions*", Copyright (c) 2004 Practising Law Institute, visitated the 10th of May 2005 on the research engine Westlaw, Read in particular the chapters 3 and 5 about the rules in the international tranactions.

criteria are missing in the EU legislation and concomitantly the work of the Commission will be more free, but in the same time less controllable.

Thirdly, it must be said that the scopes of the two norms are a bit different (and the USA scope is broader). Infact the scope of article 7 (paragraph 2) of the EC Directive is “to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries”. In the USA the scope of section 301 is “to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and foreign commerce”. Consequently and obviously the activity of the Secretary will be broader than that one of the Commission.

References

List of Judgements/Decisions

US Supreme Court:

Bernstein v. Department of State

Griswold v. Connecticut (1965) 381 US 479

Junger v. US Departemnt of State

Karn v. US Department of State and Thomas E. McNamara

Katz v. United States (1967) 389 US 347

Roe v. Wade (1973) 410 US 113

Treaties/Statutes

California, Electronic Signature Act

Commonwealth of Australia Electronic Transaction Act 1999

Directive 1999/93 EC, OJ L013, 19.1.2000, p.0012-0020

Directive 2000/31 EC, OJ L144, 04.06.1997

Malaysia Digital Signature Act 1997

Singapore Electronic Transaction Act 1998

Texas Electronic Signature Act

The Uniform Law Conference of Canada: The Uniform Electronic Commerce Act

UNCITRAL,"Draft Uniform Rules on Electronic Signatures"

UNCITRAL Model Law on Electronic Commerce

USA Bill of Rights

USA Constitution

USA Electronic Financial Services Efficiency Act, 1999

USA E-SIGN Act

USA Uniform Electronic Transaction Act, 1999

Utah Digital Signature Act, 1995

Secondary Literature

Akadeniz, *Cryptography and Liberty "Can the Trusted third Parties be Trusted?" A Critique of the recent Uk proposals*, 1997, in JILT 1997 (2), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/

Angel, *Why use Digital Signatures for Electronic Commerce* in JILT 1999 (2), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/

Annamalai, Nagavalli, *Cyberlaws of Malaysia - The Multimedia Super Corridor*, 1997, 12 Journal of International Banking, p 473;

Arnò & Lista, *La firma digitale nell'ordinamento italiano e comunitario*, in "Rivista di diritto civile" 2000, p. 732

Arruda & Shestakova, *US Enacts E-Sign: The Electronic Signatures in Global and National Commerce Act*, visit the website http://www.cla.org/usenacts.pdf

Blythe, the Richmond Journal of Law and Technology, *Digital Signature Law of the United Nations, European Union, United Kingdom and United States: promotion of growth in e-commerce with enhanced security*, from the legal review Westlaw

Borruso & Tiberi, *L'informatica per il giurista*, Giuffrè editor, 2001

Canavillas, *An introduction to web contracts*, in Walden & Hornle, E-commerce law and practice in Europe, Woodhead Publishing Limited, 2001

Chissick, Michael and Veysey, Guy, in *The Perils of On-Line Contracting*, in CTLR Issue 5, 2000

Ciacci, *La firma digitale*, in "Il Sole 24 Ore" 2002 p. 74

Ewing, Remick & Saul, *New E-Signature Laws Click Into Action*, visit the website http://www.saul.com/articles/int2.htm

Gambaro & Sacco, *Sistemi Giuridici Comparati*, UTET editor, 1996, pp. 164-191

Hindelang, *No Remedy for Disappointed Trust? The Liability Regime for Certification Authorities Towards Third Parties Outhwith the EC Directive in England and Germany compared*, in JILT 2002 (1), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/

Hornle, *The European Union Takes Iniziative in the Field of E-Commerce*, in JILT 2000 (3), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/

ILPF in An Analysis of International Electronic and Digital Signature Implementation Initiatives, visit the website www.ilpf.org

Julià-Barceló, Rosa, *A New Legal Framework for Electronic Contracts: The EU Electronic Commerce Proposal*, in Computer Law & Security Report Vol.15 no.3 1999

Kahn, David, *The Codebreakers*, Macmillan Company, New York, 1972

Mason, *The International implications of Using Electronic Signatures*, in CTLR, August 2005

McCullagh, *Signature Stripping: a Digital Dilemma*, in JILT 2001 (1), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/

Monti, *La crittografia, l'Europa e l'America*, visit the websitehttp://www.interlex.it/attualit/amonti49.htm , visitated on 15th of March 2005.

Nemmar, *Emerging Trends in Commercial Law: Surviving Tomorrow's Challenges*, DePaul Business & Commercial Law Journal, 2004

Presidency Conclusions of the Lisbon European Council, Rapid Press Release of 28 March 2000, PRES/00/900, visit the website http://www.europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=PRES/00/900|0|RAPID&lg= EN

Reed, *Internet Law- Text and Material*, Butterworths, 2000

Reed & Davies, *Computer Law*, 5th edition, Oxford University press, p.340

Rose, *Your Rights in the Online World*, Osborne McGraw-Hill, 1995, in Netlaw

Smedinghoff , *The Legal Requirements For Creating Secure And Enforceable International Electronic Transactions*, Practising Law Institute, 2004, find it on the on-line research engine Westlaw

Spyrelli, *Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication.* In JILT 2002 (2), visit the website http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/

Ter, Kah Leng, *New Laws on E-Commerce*: *Singapore*, 1999, Computer Law and Security Report Vol 15 No 1, p 8

Travis Schwaer, *Electronic Signature Laws Provide Texas Agencies Secure and Legally Binding Online Transactions*, 2004, find it on the on-line search engine West law

Wu, Richard *Electronic Transactions Ordinance - Bulding a Legal Framework for Ecommerce in Hong Kong*,1999, the Journal of Information Law and Technology (JILT), http://www.law.warwick.ac.uk/jilt/00-1/wu.html

Zainul, *Comparative Analysis of the Malaysia Digital Signature Act 1997 and the Singapore Electronic Transaction Act 1998*, visit the website: http://130.159.238.165/Document%20Library/1/Electronic%20Commerce%20-%20the%20Malaysia%20Digital%20Signature%20Act%201997%20and%20the%20Singapore%20Electronic%20Transaction%20Act%201998.pdf

A