Title:
"Electronic signatures in on-line transactions:
legal issues in Greece and the European Union".

SPYROPOULOS CHRISTOS, Attorney at
Law, Athens Bar Association

T ABLE OF CONTENTS

I. Introduction

a. General approach

Attempting to assess the impact of using electronic signatures while transacting on-line on the whole e-commerce regime that was created afetr the expansion of the Internet in the early ‘90s 1, what has to be initially estimated is the field of activities that such a way of signing covers. From a legal perspective, various parameters have to be taken into account, such as the contradiction between new techniques of trade with the traditional commerce and the special consequences that follow this fact-e.g. on-line/intangible v. paper-based contracts-, the universal nature of doing business via the Web with all the jurisdictional and applicability of law issues that arise automatically, the need of thje stablishment of a consumer-friendly system based on trust while striking a fair balance 2 between the companies’ desire for success and the customers’ request for protection against methods totally new to them and often used to take advantage of their “net-ignorance”.

Problems like the abovementioned have become of great interest for the European Union’s Member States as the economic integration in a Single Market where every european citizen will be free to move, work, provide services and buy goods is the ultimate purpose as set out in the EC Treaty 3. Bearing in mind that Europe has always been struggling for creating a more competitive market in compariosn to the undoubted leading US market, the development of modern ways of trade seems to be essential for the first. Decisions, regulations, directives, are some of the weapons in the European Commission’s arsenal that help in the process of harmonisation of standards between the Member States and guarantee a minimum legal framework on which special State legislation must be based.

Greece, as a Member State of the European Union and while being located at a geographically crucial point (at the south-end of Europe and close to the emerging markets of the Balkan countries), has a dual role: on the one hand, it is obliged to adopt the European policy intiatives on e-commerce by implementing in a satisfactory extent the European Commission’s directives and legislation in general, ensuring in that way its compliance with basic standards that warranty secutiry and progress; on the other hand, although one could argue that e-commerce has no borders, Greece could play a leading role in the Balkans, a territory where it has traditionally been a key-player, in relation to electronic transactions by setting up a reputation of stability, secure trade and fair contracting policies.

Having referred, in general terms, to some controversial aspects of transacting on-line as well as to the milestone of the European Union;s motivation when creating primary law and to Greece’s twofold mission, we may assume that any attempt to legislate on electronic commerce has its origins in the first place at political (harmonisation, unification) and economic reasons (integration, creation of competitive markets based on consumer trust); the analysis of purely technical issues and their adaptation in a more comprehensible language through European or statutory legislation is a latter stage of action following the realisation of the need for legislative intervention.

b. The electronic commerce’s notion

Electrronic signatures are frequently used, inter alia 4, in the field of elecrtronic commerce as well as in the public administration system, in governmental organisations, in intelligent agencies e.t.c. The comprehension of the first presupposes the definition of the latter; as in the world of traditional trade the act of signing a paper-based contract from which obligations originate for both the contracting parties should be regarded as part of a set of legal rules that regulate the contracting procedure (imposition of rules of formality that guarantee the validity of certain

categories of transactions-e.g. transactions on immovable things, last wills e.t.c.-v. absolute freedom of contracting-e.g. transactions on movable things-, designation of further rules that interpret the meaning/spirit of the primary law in cases of legislative gaps-e.g. in situations of modern ways of commercial activity that override the long-established ones, as often is the case in e-commerce-or formation of rules that solve problems arisen in special circumstances-e.g. fraud or use of threat while contracting), in the same sense signing electronically should be considered as a special facet of the entire on-line commercial practice.

Electronic commerce has habitually been defined as "doing business electronically" 5; light is shed on this obscurely over-simplyfying and laconic description if we categorise the on-line commercial modus operandi, which is "based on the electronic porocessing and transmission of data, including text, sound and video" 6, in accrodance with two criteria, namely the type of the parties involved in it (businesses, governments, consumers) and the commercial activities covered by it (e.g. on-line delivery of digital content, on-line sourcing, direct consumer marketing, electronic share trading e.t.c.) 7. Consequently, a number of transaction types is being shaped after the multiple combinations of the upper categories, such as the business-to-business (B2B) model which contains, for example, the electronic trading of products and services, the business-to-consumer (B2C) model that encloses teleshopping, telebanking, electronic bookings (e.g. holiday or plane tickets), pay-TV or video-on-demand services, the consumer-to-consumer (C2C) model that includes virtual market place and electronic donation services, the administration-to-administration (A2A) model that refers, for instance, to electronic exchange of gorvernment information, the business-to-administration (B2A) model that is related, for example, to the electronic exchange of statistical information and the consumer-to-administration (C2A) model that emraces, for example, the provision of electronic tax forms services 8.

It becomes obvious that not only conventional methods of commerce which prima facie sound brand new (e.g. telebanking or virtual purchasing) are just the result of a successful adaptation of customary trading form the digittal environment with the help of modern technology, but also that traditional merchandising goes hand-by-hand with novel techniques seuch as webvertisement, electronic contract negotiation and electronic tax declarations. With the intention to prevent electronically transacting parties from acting in an anarchic way that would harm the e-commerce structure and, as a consequence, their own wellfare, the European Union has regulated certain aspects of on-line tradee by adopting sveral measures such as the Directive on distance selling 9 and the Directive on e-commerce 10, both of which espouse a trading policy based on consumer trust, fair terms of trade and detailed description of rules and their exemptions. Being observed under the light of the above legislative spirit and the development of e-commerce as any transacting business activity related to the trade of goods or services between parties that "are not at the same physical location and communicate through electronic means" 11, the issue of electronic signatures could be analysed in a more comprehensive way.

c. The formation of electronic contracts' concept

Aiming at understanding the functional role of electronic signatures, what should be apprehended is the legal field within which they operate. In particular, according to the "pre-Internet" legislation, a signature is used in transactions on several objects (e.g. purchase or rent of movable or immovable things or intellectual property rights); the common element of all the above deals is that persons who sign-either obliged by the law in order to breath life nd validity into their aghreement/statement or after their free concurrence on being bound by a paper-based

contract, in cases where the law is more flexible regarding formality matters-end up by confirming their will by signing at the end of a paer page or set of pages. The notion of the paper-based contract has been central in all these agreements which require that the wills of the parties must be written down in a formally unambiguous way, as, Latins said, “verba volent, scripta manent”. Therefore, signing has traditionally been relevant to paper-based deals and its task has been double, explicitly to verify the identity of the contracting parties and to confirm the fact that they are willing to be bound by the content of the text as noted down by them or a public authoriy or a legal expert.

The extended use of the Web as a means of doing business has brought into light a number of concerns far more complicated than the aforesaid formal requirements. Questions such as when are the on-line contracts formed, what terms they should include and which territory’s law governs them 12 have become a case of study for legal and information technology connoisseurs. Using the method of functional equivalence as a starting point, these experts have tried to replace the function of long-stablished rules on contract law with modern ones compatible with the on-line merchandising 13. Thus, for instance, considering the time whern an electronic contract is shaped, a webvertisement is regarded as an invitation to treat 14 and not as an offer unless it unequivocally shows the keenness of the webvertiser to be bound upon acceptance 15; in addition, the postal rule 16 applies to acceptances communicated through e-mail 17 due to the e-mail contracting procedure’s similarity to the acceptance of a contract by post while the same rule does not apply to the click wrap acceptances 18. Furthermore, considering the content of the terms a contract should include so as to be valid and not fall under consumer protection restrictions, it has been held that all contractual terms should be made known to the web client before he decides if he wants to enter in an agreement 19 and that the incorporation in the contract of terms by reference should be made in an explicit and definite way, e.g. by the provision of a “clearly marked and prominent link to the specific terms and conditions” 20, in order to help the customer to shape a full opinion on the purchase he intends to make. Moreover, in relation to which law is applicable to the contract, apart from the general principle of freedom of choice 21 that the parties have, special measures are taken when one of the parties is a “consumer”, i.e. when his on-line purchasing is “outside his trade or profession” 22, namely that he cannot “be deprived of ... the protection afforded to him by the mandatory rules of the country in which he has his habitual residence” 23. Accordingly, it becomes clear that the wisdom of the past which was gained through “trial and error” imposition of legislation or established case law is being repeatedly challenged by the rapid technological progress; thus, great effort and caution should be taken when implementing customary rules into the new way commerce is operating through the Net nowadays.

d. The electronic signatures’ conception

Regarding the electronic signatures as a special part of the aforementioned setting, the comprehension of their nature, functioning, mission and the problem caused during their use in the Internet environment becomes easier. Bearing in mind that a signature, either electronic or not, is meaningful only when connected with a contract or statement, and taking into consideration that electronic commerec is a facet of a general policy or the European Union aiming at political and financial unification ane enforcement, the brief mentioning of some portions of e-signatures’ analysis will be attempted below.

In particular, starting by describing the variety of the ways of signing whcih exist traditionally or are being invented for electronic application, the way electronic signatures are functioning and the differences between habitual and modern

techniques, the study will move on to examine the mission of signing in the contract world, to point out the several matters that are born while signing on-line and to scan the position which the European Union and Greece, in particular, have taken towards these vital issues. For instance, concerns on trust between the contracting parties are dealt with the creation of a "trusted third entity", namely the Certification Authority (CA) which guarantees for the identity of the signatory; however, this model needs to be developed through specific legislation so as questions such as which body can qualify as a Certification Authority, who will decide on it, who will sypervise the CA's function, what sort of functioning levels-if any devision is permitted by law- will appear, what kind of measures will rule the liability of the Certification Authority towards its customer and the other contracting party, can be answered safely. In addition, the fact of the separation of electronic sugnatures into two types, that is to say in the "simple/conventional e-signature" and in the "advanced/qualified one" that is legislatively recognised as equal to the handwritten signature, will be observed from a consumer policy and Certification Authority improvement point of view.

The effectiveness of the e-signing methods like PKI (Public Key Infrastructure) cryptography in relation to data security will also be scrutinized, as the influence of an insecure on-line contracting regime on the potential market players' (consumers, businesses, governments) performance can be detrimental. The matter of key-escrowing will also be indicated as, by including by its very nature an offensive position against personal data protected by international 25, European 26 and national 27 legislation, it could create a negative conduct towards e-commercing. Finally, the measures protecting the consumers against on-line abuse of the existing legislation as well as the motivation given to companies to do business electronically will be commented in order to appreciate the extent to which a balance between consumer wellbeing and businesses' welfare is actually present and, if this is not the case, to propose some advanced solutions.

Focusing on Greece's activity relatively to the above, three views should be considered: firstly, that Greece is bound by having signed in several European Union agreements and, in that sense, obliged to follow up with the other Member States in the economic integration procedure. Secondly, that in order to achieve that purpose, Greece has to create law based on the European Direcrtive's on electronic signatures minimum legal framework by specifying the Directive's provisions which are the products of several influencies such as the Uncitral's Model Law on Electronic Signatures 28, the ABA's Digital Signature Guidelines 29 or Germany's Digital Signature Law 30. Thirdly, that the adjustment of internationally standardised rules to the greek legal system must comply with a number of social, cultural and economic needs of this State.

II. Analysis

I. Traditional and modern signatures: sorts and legal definition

Despite the fact that neither the European Directive 1999/93 nor the greek Ministerial Decree 150/2001 31 that adopts the above Directive refer to the conventional or modern modes of signing in detail, probably because they take the firsts' existence as self-evident and already sufficiently regulated by contract law and they prefer encouraging the development of new forms of e-signing than limitating it by recognising only a certain kind as legally valid for the latters 32, it is useful to denote them for two reasons; firstly, to understand how functional equivalence can be achieved for the benefit of e-commerce players. Secondly, to appreciate how they are being treated by the law, and comprehend the reasoning for that treatment.

A. Signing formulae

a. Handwriting

What traditionally has been regarded as a typical example of a handwritten signature is the writing of the name of the signatory at the bottom of the final page of the contract, deed or statement 33. However, variant types have been created among the years, like crosses, initials, pseudonyms, identifying phrases, printed names or rubber stamps 34. The clear resemblance which ties the above kinds is the fact that they are being transmitted, through the ink and the common knowledge of a particular alphabet, to a paper; nevertheless, in the absence of any intention of the signatory to sign and to be bound by any contractual obligations ("mental element"), his signature has no legal meaning 35. Apart from the writing procedure and the medium on which they appear, the above signing models are alike due to the fact that they are the products of formality requirements set by the law; thus, their functionality is not examined in the first place 36.

b. Modern applications

On the other hand, the innovative trend of the technology is being reflected by the several ways of signing on-line. For reasons of completeness, what has to be clarified is the distinction between "electronic" and "digital" signatures. The first term is technologically neutral and covers the whole sum of techniques used for signing an electronic record 37. The second covers electronic signatures created by the use of cryptography 38. Some of the premature kinds of electronic signing have been the putting of the signatory's e-mail address under the document 39, the use of a secret code (PIN code) in debit/credit cards transactions through cash dispensers 40 or the "simple put of a name under an electronic mail" 41. Moving ahead, we meet the biometrics technique which "uses physical or behavioural attributes such as your fingerprint, voice, face, iris or signature to identify you" 42. Sorts of biometrics such as hand geometrics (scanning the shape or the size of the hand) 43, iris scanners (analysis "of the ring of the coloured muscle around the pupil") 44, facial (analysis of the video image or photograph of a person) or vocal (analysis of "fundamental voice characteristics") recognition 45 and signing characteristics' recognition (examination of "the speed and acceleration rates of the pen strokes used to make the signature" on a special equipment called "digitising pad") 46 are frequently used by governments and companies to increase security in on-line transactions. Steganography, the science of "hiding secret data inside a common filer type so nobody guesses that it is there" 47, appliies to "secret messages written in invisible ink, micro dots and radio signals that resemble noisy static" 48 and is regarded as a great threat for on-line security if used by extremists or terrorists 49. Furthermore, quantum cryptography refers to messages being sent by the use of photons of different polarities that represent numbers (zeros or ones) 50 and is expected to be the safest way of on-line communication in the near future, although the fears of being attacked are always present 51.

c. Cryptography

Cryptography is being examined separately as it is the most widespread technique of electronic signing. The term originates from greek ("crypto" means secret + "grapho" means write) and encapsulates the idea of hiding the meaning of a message by writing it in another way known only to the receiver of it. 52 The above purpose is met by the enciphering of the message by the sender and its deciphering by the receiver, which in turn is attained through the use of algorithms, i.e. arithmetical processes that encode data based on mathematical calculations. In order for the message to be signed and read, both its creator and its recipient have to possess keys, in a metaphorical sense: each of them has a public key known to the other and a

private key that is kept secret. Hence, two pairs of keys are needed for the encoding and decoding of the message, and this is the example of assymetrical or public key cryptography 53. In symmetrical or private key cryptography, there is only one "private" key which the parties share to encode and decode and which they agree to keep secret 54; thus, the level of confidentiality and trust between the parties has to be remarkably high and symmetrical cryptography applies to closed networks, i.e. networks with limited participants such as pay-TV, pay-per-view or video-on-demand services 55. The open-networked nature of the Internet and the fundamental element of secure and safe web-transacting have made public key cryptography the common method for the formation of electronic signatures 56.

As mentioned above, public key cryptography is based on "the technology of sharing a public key" 57. The comprehension of its functioning could contribute in understanding a number of legal issues such as the Certification Authorities' mission towards the consumers and the governments in the course of on-line trade. Considering A as the composer and sender of an electronic message and B as the receiver of that message, the following process takes place: (i) by applying an algorithm called "digest" or "hash function" 58 to the written message, A transforms the original text into a string of bits which is unique and brief and is called the "message digest", (ii) in order to make the message digest secret to any other accidental receiver or hacker, A encrypts it with his private key 59; in particular, A performs a series of mathematical procedures between the digest and the private key, and the result is a number that forms the electronic signature 60. A can additionally encrypt his message with B's public key for extra security, (iii) in order to decrypt the message, i.e. to bring the sent message in plaintext form again, B will use A's public key; decoding will fail if someone else used A's public key but his own private key to sign the message. Furthermore, if A has encrypted the message using additionally B's public key, B will have to decrypt it using his private key; in that way, A can be sure that only B-or persons authorised by B to know and use his private key will read his message, (iv) the plaintext message is run through the same algorithm (hash function) and a message digest is produced, (v) B compares the message digest of the sent and the recieved messages; if they differ, even in one bit, the sent message has been altered in transit 61. If they are the same, A's signature is validated and the integrity of the plaintext is guaranteed.

B. European and greek legal definition

a. The European approach

Regarding signing as a common phenomenon among the centuries, it seems futile trying to find a definition in European legal texts; the national laws of the Member States are a better object of examination. However, the concept of electronic signatures, due to its rather complicated and technical character in comparison to handwritten signing and to its significance for the augmentation of e-commerce, has become of great interest to the european legislative world.

The European Directive 1999/93 on Electronic Signatures defines an electronic signature as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication" [art.2 (1)] 62. This quite broad definition is justified by recital 8 of the Directive, which says that due to the speedy progress of technology and the worldwide nature of the Internet, every legislative approach on electronic signatures has to be 'open to various technologies and services capable of authenticating data electronically", i.e. technologically neutral 63. The technological neutrality principle is also met in art.2 (4) and art.2 (7) of the Directive, where, although public or private key cryptography are recognised as methods of creating and verifying an electronic signature, the use of

"such as" indicates the European Union's desire to leave the doors open for innovation, research and development.

The novel notion that the Directive embraces is the two-tier approach 64 it adopts in relation to the legal recognition of electronic signatures. In particular, it provides for two types of electronic signatures, namely the "simple" and the "advanced" electronic signature. The first is defined in art.2 (1), the latter is an advanced version of the first and is defined in art.2 (2) as "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" 65.

b. The greek approach

The greek contract law does not give any definition of the term "signature" 66. Nonetheless, art.160 para 1 of the Civil Code states that, in the case that a document is required by the law 67 or agreed by the parties to be in written form, this document will be regarded as valid only if it carries the handwritten signatures of the parties 68. Inspite of being necessary for reasons of contracts' security and confidentiality, the above provision proves to be strictly formalistic as it calls for signature written in hand 69, even though greek case law has broadened the horizon of hand-writting by recognising as legal valid signtures put by foot or mouth or signatures created by technical means such as fax or telex. In addition, it is indirectly incosistent with art.444 (3) of the Civil Procedure Code, as the latter, in the course of the evidential procedure, defines "document" as "any mechanical pictuation" and allows, in that way, techniques such as video or tape recordings or-in a further extent, electronic mails- to be legally accepted. The gap that appears in the case e.g. of an e-mail contract is noticeable, as signing the e-mail cannot be made by hand but only by using electronic means, which, in turn, must be recognisable by law (broader interpretation of art.160 para 1 of the Civil Code) in order for the e-mail document to be accepted as evidence and legally binding the parties. The only solution that prima facie seems feasible is the consideration of the several manners of e-signing as equal in nature to the legally admissible traditional hand-signing ways, fro reasons of development of e-commerce and support of the technological growth 70.

With reference to electronic signatures, the Ministerial Decree 150/2001 which has adopted the European Directive 1999/93 gives exactly the same definition of art.2 (1) and art.2 (2) of the Directive for the electronic signature and the advanced electronic signature respectively in its art.2 (1) and 2 (2). The same technology neutral spirit also appears in art.2 (4) and 2(7) 71. It is evident that the greek legislator wishes to avoid any deviation from the european letter and spirit of the law so as to contribute in the harmonisation process and the expansion of e-commerce in Europe by adopting in the larger extent the European Commission's policy dicta. It is also beneficial for Greece to bring its legislation on e-commerce into line with the european standards from an early point in order to avoid s "follow-up" tactic later that could harm its national status 72. Furthermore, the creation of a secure regime for on-line trading could make Greece a crucial player in Balkan's economic life.

As a consequence, two parameters have to be kept in mind; firstly, the construction of a double-typed model for electronic signatures by the European Directive and its adoption by the Greek law. Secondly, the European Commission's willingness to support the appearance of new technologies on e-signing by defining electronic signatures in such a broad way 73; provided that the safety requirement is satisfied and improved by pioneering methods which suit to the Directive's security

standards 74. The examination of the handwrittem and on-line signatures' tasks as well as a comparison between those two categories will take place below.

2. Signatures' mission

The comprehension of a signature's purpose is the starting point for the understanding of its legal meaning and the realisation of the problems its use may cause in the electronic environment. Invented to satisfy the security and reliability requirements for safe transacting, a signature fulfills four tasks 75.

A. Authentication

By signing at the last page of a paper-based contract or by applying the essential mathematical procedures to decrypt an electronic message, the signatory not only indicates his intention to identify himself as the originator of the text but also sugnifies his purpose to be legally bound by the content of that text. Thus, the primary role of a signature is to identify "who participated in the transaction" 76. The authenticity of the signature is the result of a successfull decryption procedure as discussed above which, apart from the case where the signatory has lost control of his key by accident or purposively 77, provides the verifying party with the information that the party that signed the message electronically is the same person who possesses the public key which the verifying party used to decrypt the message.

The authentication part of e-signatures is regarded as an element of their definition by Directive 1999/93, as in art.2 (1) e-signatures are defined as "data...which serve as a method of authentication" 78. The Greek Ministerial Decree 150/2001 fully accepts the importance of the authentication aspect by implementing in art.2 (1) the Directive's art.2 (1) word for word.

B. Data integrity

What follows the question on the identity of the signatory is the matter of the veracity of the message's terms 79. It is of great importance for the receiver of a data message 80 (e.g. en e-mail taken as an offer for contracting) to be reassured that what he reads after having decoded the message digest is what the signatory intented to communicate to him without the data having been modified, demolished or accessed by any unauthorised person. The integrity of the data contained in the electronic message is being proven at the same time with the authenticity of the electronic signature 81, namely after the realisation of the fact that the message digest of the sent and the received message is the same. The issue of integrity is critical not only for the consumers (B2C commerce) as, for example, consumer protection concerns are born by the alteration of on-line contractual terms and conditions without the authorisation of the on-line company (e.g. by a hacker of an antagonistic company) and the consumer's prior notification, but also for the business (B2B commerce) as, for instance, orders between companies that occur daily on-line could be declared void in the absence of consistency between the sent and the received offer. Subsequently, the whole structure of on-line trading would be collapsing if not based on a method of e-signing that would promote security and safety, i.e. PKI encryption.

The European Commission, acknowledging these perils, although, as mentioned above 82, it does not establish PKI as the exclusively superior technology, it refers in the Directive to "signature-creation data" (e.g. codes or cryptographic keys) "used by the signatory to create an electronic signature" 83 implemented by "signature creation device" ("configured software or hardware") 84 or "secure-signature-creation-device" 85 and to "signature-verification-data" 86 (e.g. codes or public cryptographic keys) used to verify an electronic signature which are implemented by "signature-verification device" ("configured software or hardware") 87. It becomes plain that the regulation of such a technical matter like e-signing in a pan-European level, in combination with the imperative need for a comprehensible

legal text which will guarantee stability and progress in the European Single Market, has to take into serious consideration the technological background as well as the new electronic signature products 88. The greek Ministerial Decree 150/2001 entirely implements the above provisions in its art.2 (4)-(8).

C. Confidentiality

The concept of confidentiality is based on the idea that any commercial transaction (e.g. commercial negotiations on the formation of a contract, offers and acceptances e.t.c.) carried out through the Web should be readable only by the contracting parties. This can be achieved only if each of the parties has complete control over his private key; it can be strengthened if the signatory encrypts his message not only with his private key, but also with the receiver's public key, so that only the receiver can read the message by decrypting it using his private key. Regarding the encryption algorithm as the lock of a safe and the private key as the combination to open that lock, we can understand that, as a multi-numbered combination makes the lock less vulnerable to theft, in the same way a lengthy private key protects the algorithm against attacks and, thus, the messaga against unauthorised access 89. A technical example is this of the pay-TV services, to which only users under a contract have access; this is being achieved by the provision to the user of the necessary equipment (hardware, software, interfaces) so as to be able to decrypt the programme that is being broadcast with the use of his set-top box 90.

Confidentiality comes as a physical consequence of the confirmation of the fact thqt the signatories are the ones that they claim to be (authentication) and that the content of the data message has not been altered (data integrity). Directive 1999/93 does not refer explicitly to the notion of confidentiality, probably because the satisfaction of the authentication need through the use of advanced technology is regarded as automatically covering the requirement of secrecy. However, recital 6 inserts a problematic perception when it says that "This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security". It is obvious that the European Commission not only is unwilling to take a position towards the key-escrow issue 91, but also creates, with such a neutral approach, the potential for the governmental intelligence agencies to abuse any individual's privacy while he is contracting on-line for reasons of national security or public policy/safety. Art.8 of the Directive comes as a panacea, as it imposes on the Certification Authorities the obligation to comply with the Data Protection Directive 2002/58/EC 92. In addition, the recital 18 of the Directive says that "the storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures". However, the Directive seems to leave the possession or controlling of private keys directly from the government unregulated. The greek approach is identical, i.e. confidentiality is taken as self-evident when authentication is fulfilled; art.7 (1) and (2) of the Ministerial Decree deals with data protection matters by putting Certification Authorities umder the "sword of Damocles" of greek laws number 2472/1997 and 2774/1999 on the protection of individuals from processing of personal data.

D. Non-repudiation

The fourth mission of a signature is to prevent the signatory from denying that he made and signed a particular statement 93. Non-repudiation follows the previous principles of authentication, data integrity and confidentiality. As long as the identity of the parties, the truth of the message's content and the secrecy of it have been verified, none of the signatories could refuse to be legally bound by the terms of the message/contract 94. Non-repudiation can be divided into "non-repudiation of origin"

which prevents the creator of the messaage from claiming that he did not send it, and "non-repudiation of delivery" which prevents the message's receiver from denying having received it. Additionally, a distinction between "non-repudiation of enforceability" and "non-repudiation of authentication" has to be made 95: the first refers to situations such as when signing was "procured by duress or fraud, if it was based on a material mistake of fact" e.t.c.; in such cases, no matter how reliable is the signature-creation and verification device, the hypothetical contract lacks of enforceability due to circumstances that have taken place outside the verification technique's detectability. The second refers purely to the technical procedure of authenticating a signature and the data integrity of a message; in that case, the signatories are bound by the on-line contracting game they themselves have chosen to play and, as a result, no denial of the validity terms is acceptable by the court.

It becomes obvious that non-repudiation is a matter that arises in the case of a dispute over the validity of a signature and the acceptance of the terms of a contract. Yet, Directive 1999/93 takes a controversial position on the matter: although it declares in recital 17 and in art.1 that "it does not cover aspects related to the conclusion and validity of contracts or other legal obligations...nor does it affect rules and limits...governing the use of documents" 96, it provides for advanced electronic signatures to be "admissible as evidence in legal proceedings" 97. The hypothetical example of an on-line contract, whose validity, although it has been signed with the advanced electronic signatures of both parties, is being challenged by one of them on the basis of threat, raises the dilemma: "is the judge obliged to rely on the 100% assurance about the authenticity of he electronic signature whcih the verification procedure guarantees or does he have to apply the traditional rules of contract law on fraud or duress while contracting"?

In my opinion, by making advanced electronic signatures equivalent to handwritten signatures when it comes to evidential matters, the Directive does not (or should not) support the idea that a verified advanced e-signature can guarantee both for the technical genuineness of the message's content and the authenticity of the signatory's will. As long as on-line trading is being operated between human beings through pc's and not merely between pc's, the human factor has to be taken into account when validity of will is disputed. Thus, the judge in the above example will just consider the advanced signature as valid 98; it is a matter of proof if finally a threat is proved to have taken place and a matter for greek contract law or law or evidence to set a special rule which will provide for a combining solution. In addition, recital 21 of the Directive says that "...this Directive...does not affect national rules regarding the unfettered judicial consideration of evidence.

E. Concluding notes

What becomes clear from the above analysis is the quadraple mission of traditional and, more importantly, electronic signatures. The identification of the contracting parties 99, the integrity of the data content of the message 100, the guarantee that the encrypted message has not been accessed, altered or devastated 101 ("time-stamping services" and "computing services" are encouraged by the Directive in recital 9) and the prevention of the signatory from denying "having performed a particular action related to data" 102, i.e. from disclaiming that he meant to sign and send the message to the receiver, shape the meaning of e-signatures' existence. The European Union concedes that, in order to construct a stable and progressive e-commerce regime, it has to apply the new technologies to its legislation if high levels of security are guaranteed. For that reason, terms such as "signature-verification-data" or "secure-signature-creation-device" appear on the Directive without being furtherly specified as long as they comply with a basic level of ability to provide security. The

greek law loyally implements the Directive's provisions trying to act in accordance with the European policy on law harmonisation and financial unification.

3. Handwritten v. electronic signatures: a real wrestle?

After having mentioned not only the several ways of signing in a manuscript or an electronic manner but also the purposes a signature serves in the off-line and on-line trade world, we can compare those two signing categories.

Manuscript and electronic signatures are aiming at fulfilling the same tasks. Firstly, they indicate the signatory's intention to be regarded as the author of the document and as the person that deliberately incorporated his ideas in that document in order to be legally bound by its content. Secondly, they guarantee the integrity of the terms included in the document; this is the reasoning of the obligation according to which the signatory of a contract has to sign in every single page of his will. In electronic documents, this is pledged by the application of public key encryption. Thirdly, the secrecy of the information contained in the document and the non-repudiatibility of its content come as a normal result of its previously verified authenticity.

However, there are differences in some aspects. For instance, a handwritten signature is "in the flesh" connected with a carrier[103], i.e. the paper page, a fact that makes it automatically readable and tangible and, thus, more detectable about its authenticity. On the other hand, due to the metaphysical nature of the electronic document[104] (though visible, it is not touchable, and what we see is just Os and 1s on the screen of our pc), any a1teration on it is hardly measurable and, thus, advanced technology such as biometrics, time-stamping or watermarking is needed to increase security. In addition, an individual's manuscript signature is unique due to every person's inimitable handwriting[lO5] and thus difficult to be completely copied, and when this happens, graphology specialists often uncover the forgery. In contrast, because of the fact that an electronic signature is based on the concept of the possession of a private key that has to be kept secret[106], it is extremely easy for any person that may attain access to the private key 107 to represent himself as the signatory and transact on the latter' s behalf without his knowledge and consent.

Judging by the similarities and differences between handwitten and electronic signatures, and despite the fact that the technological nature of the latters makes them seem so complex and diverse from the firsts, we should not focus on trying to find out which of these triumphs over the other. Rather, we should examine how they can function in combination for the development of e-commerce.[108] This is the approach that the European Union, and consequently Greece, has taken. In particular, art.5 (1) (a) of the Directive 1999/93 equalises the legaJ effectiveness of an electronic signature[lO9] to this of a handwritten signature; obviously, the Directive attempts to treat advanced security signatures in the same maηner with the handwritten ones, indicating in this way two ideas, i.e. that it is unwilling to establish a completely new and exclusive regime for electronic signatures 110 and that it acknowledges the quantitative and historical prevalence of traditional signing over on-line signing (for reasons of consumer confidence[111]). Based on the priciple of functional equivalence which represents the idea that legal admissibility shou1d be given to electronic signatures if the way of their creation provides the same degree of security and authenticity as the handwritten signing, art.5 of the Directive "reconciliates" the two signing categories.

The Ministerial Decree 150/2001 fully adopts the above approach; from a case law point of view, Decision *1327/2001* of the One-Member Magistrate Court of Athens 112 reaches to some interesting conclusions. In particular, in the text of the decision it is said that a1though the electronic document, due to the lack of its stability and

lifetime durability when being incorporated in a hard disc, can not be regarded as much alike to the traditional document, it can be considered as legally equal to the latter. The Decision goes on to say that an e-mail address, due to its uniqueness and creation by the e-mail sender by himself, "has the character of a handwritten signature, independently of its position on the electronic document" and is admissible as evidence in legal proceedings. The judge bases the legal effect of the e-mail as a handwritten signature on the fact that, due to common experience, the creation of the e-mail presupposes a server connected on the Internet through a software installed in the owner's pc and a special code through which the owner of the e-mail is being uniquilly recognised as the sender or the receiver of electronic data. The abovementioned code is created originally by the owner and consists of characters (numbers, symbols, letters e.t.c.) selected by him which, connected with the symbol @ and characters set by the server, form the e-mail. In that sense, the greek judge concluded that the authentication and the non-repudiation of the e-mail signature was undoubted. The eagerness of the Greek judge to validate electronic contracts and, thus, create a friendly environment for the growth of e-commerce is obvious. However, from an electronic signatures' authentication point of view, the judge has misunderstood two aspects: firstly, that the security provided by the method of creating an e-mail address does not meet the standards imposed by the Directive 1999/93 [advanced electronic signature created by a secure-signature-creation device, art.5 (1)] 113; secondly, that the existence or not of a qualified certificate that would guarantee the true connection between the owner of the e-mail address and the sender of the e-mail document and would make the e-mail address equal to a handwitten one according to art.5 (1) of the Directive was not examined. 114 Taking into account that the concluded via e-mail contract was worth approximately f25.000-a relatively large amount of money- and that most of the Certification Authorities (CAs) classify the signature certificates they provide in accordance with each transaction's value[115], the acceptance of the effectiveness of the e-mail address as an electronic signature equal to manuscript signature seems overenthusiastic if compared to the security requirements for on-line dealing.

In Decision 3279/2004 of the Council of State, the greek judges had to deal with a slightly different situation: the chinese company that submitted its offer to the Ministry of Public Constructions did not meet the requirements of the greek Ministerial Decree for public contracts. More specifically, the company's papers had only the company's electronic seal and not the handwritten signature of its legal representative as the greek law for public contracts demanded for reasons of public order and safety. This fact created serious doubts to the judges on the authentication of the electronic seal and the true will of the company to be bound by the contract in case that someone else had become in possession of the seal. In other words, the Decision used the aspect of public order and common good which the Ministerial Decree had set as a legal prerequisite for the legal recognition of any type of signature on electronic papers and put a limit on the general acceptance of unclassified signatures, though without examining the field of signature's digital formation and its legal aspects.

In Decision 25208/2009 of the One-Member Magistrate Court of Thessaloniki, the judge faced another common problem: considering the e-mail address of a woman as her electronic signature, he concluded that the "breaking" of its password by a third person and the sending of e-mails to other people without her consent was, apart from an offence to her personality, a forgery of her "electronic signature" as well.

Therefore, handwritten and electronic signatures can go hand-by-hand,

provided that full respect is being attributed to the risks resulting from the false application of novel technologies while, at the same time, the structure of the existing legal system (contract law, law of evidence) is accepted as the basis for every legislative work on e-signing.

4. The Trusted Third Party's concept

A. The necessity for Certification Service Providers (CSPs):"On the Internet, nobody knows you're a dog,,!116

Due to the dematerialisation of transactions on the Web world[J17], physical contact between the agreeing parties has been flattened. Thus, while in traditional trade it is usual that the signatories of a contract know each other, either personally or through their lawyers, in on-line contracting the parties often transact for the first (and last) time. The issue of knowing who really the other party with which we deal electronically is, is fundamental for the establishment of trust in e-commerce. The procedure of the verification of the authenticity of an electronic signature based on P**KI** encryption solely assures the recipient of the electronic message that the person who theoritically possesses a public key is the one that sent the message[118]; however, it does not answer to the following questions:

a) is the possessor of the public key the person that he claims to be, i.e. is there a real connection between phenomenical and actual identity of the signatory?

b) regardless of answering positively to the above question, was the signatory in real possession of his private key or this had been lost or stolen at the time of the transaction?

From a personalisation point of view, the problem is that the private and public keys form a pair of numbers that has no relationship with the actual identity of a person[119] as it does not attibute to him some special characteristics (e.g. height, date of birth etc) which his identity card contains. Therefore, it is possible and trouble-free for a third party to create a pair of keys, place the public key in an on-line directory under somebody else's name and begin signing electronic messages in this else's name[120]. As a consequence, what the transacting parties struggle for is the affirmation that each others' public keys tru1y belong to whom it is claimed. 1t has to be mentioned that the identity problem refers to transactions in open networks like the Internet where the parties have not established a previous commercial relationship 121 and the demand for trustworthiness is imperative.The notion of Certification Authorities (CAs) or Trusted Third Parties (TTP) or Certification Service Providers (CSPs) appears in order to serve the above purpose, namely to warranty the relationship between the identity of the signatory and his public key.

B. CSPs' mission

Having understood the underlying reasoning for the existence of CSPs, it is unadorned to define their mission. A CSP declares to ascertain the identity of a signing party and certifies that this party's public key in fact belongs to him.[122] Thus, the linkage of signature verification data (e.g. codes or public keys) to a person and the confirmation of that person's identity 123 is the motivation of the CSP's function with the eventual purpose of intensifying confidence in the e-commerce scenery.

C. Designation of CSPs

By its definition, a CA plays the role of an entity that acts as an intermediary 124 between the contracting parties as it satisfies the request of the one (receiver of the signed electronic document) to know the identity of the other (sender of the message). In other words,a CA aims at being trusted by the receiver in relation to the accuracy and completeness of information it provides him about its customer (the

sender). To achieve this reliability in the receiver's mind, the CA must be designated as an independent unit.

Directive 1999/93 defines broadly a CSP as "an entity or a legal or natural person" [art.2 (1)]; the Ministerial Decree 150/2001 defines a CSP in exactly the same way [art.2 {11}]. The Directive leaves the structure of the CSPs (and the services they may provide) to the legislators of the Member States according to recital 12 and art.4 (1), with the sole restriction of art.3 (1) 125. The Ministerial Decree declares that the provision of certification services in Greece by a CSP that is established in the Greek territory is ruled by the existing Greek legislation [art.5 (1)]. In relation to the above restriction, the Decree states in art.4 (4) that, apart from art.4 (5) (provision of voluntary accreditation by the EETT 126-or private or public bodies authorised by EETT-after the submission of a written application of the interested party) which complies with art.3 (2) of the Directive, the provision of any form of certification services in Greece is not dependent on a license given to the CSP.

Among the different forms of structure, such as a state-controlled entity 127, a mainly owned by the government private legal person 128 or an entirely independent corporation, the Greek practice has selected the third model to incorporate the idea of CSPs. Thus, at the moment, nine CSPs are active in Greece according to the data archive of EETT[129]: two of them are bank entities, another one is "an obligatory, autonomous and independent association of natural and legal persons, conducting commercial activity in a given region, and operates under the constraining administrative supervision of the Minister (with respect to the legality of its activities within the context of its statutory autonomy)" 130 and the other four are governmental organisations or private entities. Only three of them (www.ase.gr, www.ypesdda.gov.gr and www.adacom.com) provide their customers with a certificate that complies with the Directive's definition of a"qualifiedcertificate".131

In a further extent, and in order to fill in the potential gaps regarding the designation of CSPs, the European Commission has adopted Decision 2000/709/EC[132] "on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3 (4) of the Directive 1999/93/EC ... ". Art.3 (4) of the Directive refers to public or private bodies designated by the Member States and having the responsibi1ity to determine "the conformity of secure signature-creation devices with the requirements laid down in Annex III". The purpose of Decision 2000/709 is to establish the legal framework *on* the requirements such a body should fulfil in order to be designated as responsible for the above task. Thus, the independence aspect of that body will be covered if its stuff is not engaged in designing, manufacturing, supplying or installing of secure-signature-creation-devices or in providing CSPs services and if the body is financially independent (art.3). The body' s personnel must carry out its task with "sufficient technical competence" (art.4) gained by "sound technical and vocational training" [art.7 (1)] and "satisfactory knowledge and ... adequate experience" [art.7 (2)]. The impartiality of the staff (art.8) as well as the adequacy of the financial sources of the body "to cover liabilities arising from its activities" and the sufficiency of ways "to ensure the confidentiality of the information obtained in carrying out its tasks" (art.l0) are also of great importance.

The Greek response to this Decision is incorporated in the Ministerial Decree's provisions. In particular, EETT-"an independent self-funding decision-making body"- has the responsibility: (a) to examine the compliance of any secure-signature-creation device with the provisions of Annex III of the Directive and the

Decree [art.4 (2)), (b) to provide voluntary accreditation to any interested party that complies with specific security standards, (c) to supervise all the CSPs that are established in Greece and (d) to inform the European Commission about the names and the addresses of all the accredited CSPs in Greece. In addition, EETT has already come up with "the criteria for the selection of Designated Bodies (in either the public or private sector) for ascertaining compliance with secure-signature--creation devices" .133 This statement could be interpreted as an attempt of the EETT to decentra1ize the task of confirming the compliance of CSPs with specific security standards preventing in that sense the monopolisation of such a responsibility by one authority and reinforcing competition (i) between the potential confirming bodies, by giving them motivation to operate in the most appropriate way and (ii) between the latent CSPs by demanding the best functioning that wil1 satisfy the same minimum but different additional criteria sett1ed by the various confirming bodies; the final purpose remains the benefit of the consumers and businesses dealing in a secure weboutlook.

C. Functioning of CSPs

1. Issuance of certificates and other services

The satisfaction of the requirement for trust is met not only by the proper designation of the CSP as an independent body but also by its appropriate functioning. The European Commission adopts that notion in two ways. Firstly, by defining the issuance of certificates or the provision of "other services related to electronic signatures" 134 as *the* main duty of a CSP, in combination with recital 9 (definition of products and services related to electronic signatures not limited to "the issuance and management of certificates" but also encompassing "any other service and product ... such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures"),the Directive al1ows a CSP to function in a variety of technical applications. Thus, for instance, it can generate the private and public key of its customer, register the identity and examine the official documents of him, revoke public key certificates, provide time stamps on certificates or govern directories of public key holders.[135] The aim of the European Union is palpable, namely to hearten the creation of advanced and multiple technologies and to ensure safety and security in on-line transactions.

2. Provision of (simple) and "qualifιed" certificates

In a second aspect, the Directive provides for two sorts of electronic signatures' certificates, that is to say the (simple) certificate ["an electronic attestation which links signature-verification data to a person and confirms the identity of that person", art.2 (9)] and the "qualified certificate" ["a certificate which meets the requirements 1aid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II", art.2 (10)]. This categorisation, though *primα fαcie* theoritical, has practical consequences because art. 5 (1) depends the legal effectiveness of an advanced electronic signature on it is being based on a qualified certificate. Thus, the admissibility of an advanced e-signature as evidence in legal proceedings and its equality with the handwritten one highly depends on the fact that it can be verified through a qualified certificate; it is clear that the whole tendency of recognising electronic signatures as equal to manusript relies on the satisfaction of the requirements of Annexes I and II of the Directive and of the Ministerial Decree.

Annex I asserts a compulsory list (ten requlrements) of the content of a qualified certificate. The name of the signatory or his pseudonym (req.c), the indication of the beginning and end of the period of validity of the certificate (req.f), the advanced electronic signature of the certification-service-provider issuing it (req.h) and any limitations on the scope of use (req.i) or the va1ue of transactions for which the certificate can be used (req.j) are some of the elements that must be contained in a qualified certificate. Annex I of the MinisteήaI Decree implements the above list literally.

Annex II contains a list of twelve prerequisites which must be fulfilled by a CSP when he issues qualified certificates. The operation of a "prompt and secure directory and ... revocation service" (req.b), the ensurance that "the date and time when a certificate is issued or revoked can be determined precisely" (req.c), the verification of the identity and of any "specific attributes of the person to which a qua1ified certificate is issued" (req.d), the employment of experienced personnel (req.e), the adoption of reliable measures against forgery (req.g) and the non-storage of signature-creation data (private keys) of the person to whom the CSP provided key management services (req.j) are some of the mandatory rules a CSP issuing qualified certificates must obey. Again, the Decree entirely adopts the above provisions in its Annex Π.

The above brief reference to Annexes I and II signifies the intention of the Directive to construct a technologically welcoming field for e-commerce based on trust. To achieve this, it has to accept models of electronic signatures that are simple and certificates that guarantee for these signatures that are simple too. It also has to encourage the adoption of advanced e-signatures and qualified certificates. This two-stage process is not only unavoidable but also necessary in this early period of e-signing. By showing its preference to advanced signatuers and qualified certificates, the European Union indirectly declares to the Member States and to any CSP willing to provide products and services that, although in theory even an e-mail address can serve as electronic signature, practical1y in the near future what wil1 be safer and convenient for the on-line consumers and businesses for the sake of trust is the sophisticated technology and its applications such as the advanced electronic signature and the quaIified certificate. Thus, it succeeds in not discouraging the average consumer from doing business on-1ine while, at the same time, it encourages the operation of safer e-commerce. A practical example of this attempt is art.5 (2) of the Directive, which imposes on Member States the obligation to ensure that solely being in electronic form or not being advanced or not being quaranteed by a qualified certificate issued by an accredited certification-service-provider does not suffice foτ an electronic signature to be "denied legal effectiveness and admissibility as evidence in legal proceedings". There must exist other reasons, based on legal defects (e.g. proof of use of threat during the transaction) or factuaI deficiencies (e.g. proof of existence of non-reliable personell of the CSP) that will permit the judge not to admit the electronic signature as evidence.

3. V oluntary accreditation of CSPs

As noted above [chapter 4 *(C)]*, for reasons of enrichment of the electronic signature products and services' market, *for* a CSP to provide certification services it is not necessary to gain prior authorisation 136 from a govemmental organisation, a public authority, a private legal person or a natural person. However, the European Union is aware of the dangers a totally !awless market access regime can enfold. Therefore, recital **11** of the Directive states that the purpose of voluntary accreditation schemes is the stipulation of an "enhanced Ievel of service-provision [by the CSPs]"

and the "development of best practice among certification-service-providers" by offering them "the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market". The national law of each Member State shal1 additionally ensure the freedom of the CSPs to operate outside or inside voluntary accreditation schemes (recital 12), to remain and to make profit from such schemes (recital 11). Moreover, no discrimination (e.g. by the courts or the public administrative authorities) between accredited and non-accredited CSPs shou1d exist, as this could be injurious for the level of competition between them (recital 12).

For those CSPs that have chosen to be accredited, art.3 (2) provides that the preconditions for a successfu! accreditation shou1d be "Objective, transparent, proportionate and non-discriminatory"; additionally, there is no *numerus clause,* i.e. 1imited number of CSPs that are aIlowed to be accredited, provided that their functioning falls within the scope of the Directive. The idea from which the voluntary accreditation notion originates is that the participating CSPs in such a scheme will compete with each other, firstly so as to comply with the requirements of the scheme, and secondly to gain the largest share in the market of certification services provision. The subsequent benefit for the net-consumers wil1 be manifest as they will enjoy high quality technological services[137]. It is also suggested that the voluntary nature of the scheme makes it more flexible than a mandatory model because the participating CSPs' welfare wiIl attract those operating outside to invest and innovate and finally enter the scheme for the benefit of trust. 138

The operation of voluntary accreditation schemes has been spread throughout Europe. For example, tScheme in the UK is an "independent, non-profit making industry led body" estab1ished to guarantee that CSPs' services are provided "honestly and expertly" and ensure confidence between CSPs and consumers. By providing the CSP' s web page with a "web seal" which acts as a trust mark, tScheme reassures the consumer of a CSP that the latter has been independently examined by experts and meets high level security standards, that it complies with a specific "code of conduct" and that it wil1 "act promptly and fairly to remedy faults"139 In Greece, aJthough art.4 (5) of the Ministerial Decree provides for the institution of voluntary accreditation schemes, EETT has not yet formed a specific scheme[140]. Finally, what has to be clarified is that the participation in such a scheme is not obligatory for the provision of any certification services ('simple' or 'qualified' certificates); the purpose which such an option serves is the organisation of CSPs in a group that will provide high quality services for the benefit of consumers. However, it is likely in the near future that the partaking in such schemes wil1 be the only alternative for a CSP that will aim at gaining a considerable market share in CSPs services' field.

E. Supervision of CSPs

Art.3 (3) of the Directive obliges each Member State to establish an appropriate system for the supervision of CSPs located on its territory and providing qualified certificates to the public. Apart from the fact that this paragraph refers exclusively to the CSPs that issue qualified certificates and leaves, in that sense, the activity of the rest unregulated, what is more important is its contradiction with art.3 (1) which prohibits the prior authorisation (or "any other measures having the same effect", recital 10) as a prerequisite for the provision of certification services. And if we consider the importance of a qualified certificate for the legal status and admissibility of an advanced electronic signature [art.5 (1)], the proper supervision of

the provider of such a certificate is of crucial significance for the whole functioning of e-commerce.

Art.3 (3) leaves it to the national laws of the Member States to find the best formula for striking a fair balance between the need of the consumers for trustwortiness and the craving of CSPs for freedom of electronic signatures' services flow. Trying to avoid the notion of prior authorisation, some Member States have come up with the idea of giving "notification to the appropriate public authority before starting the provision of services".141 However, notification can be regarded as a measure having very similar effect with prior authorisation and it will remain to the national and European courts to judge on the correct implementation of art.3 (3) by the Member States in the case of a dispute.

In Greece, the provision of e-signatures' certificates, either qua1ified or not, is regulated by Decision 248/71 of EETT[142]. EETT is recognised as the supervisory authority for the CSPs which are located in Greece (art.9). Art.10 (2) states that "With the beginning of his activity, every CSP located in Greece shall notify in written form to EETT ... " information such as its name, address, phone number, legal status and services provided; for" the CSPs which issue qualified certificates to the public, apart from the notification a number of documents have to be submitted, namely: (a) statement of the CSP that he complies with the requirements set out in Annexes I and II of the MinisteriaI Decree and the Directive 1999/93, (b) Certification Practice Statement (CPS) of the CSP , which is a document that describes in detail the practice foIlowed by the CSP for the issuance of certificates and/or the provision of other certification services (art.2), (c) documents proving the CSP's financial abi1ity to cover any damage caused by its profession and (d) documents edited by the competent public or judiciary authorities proving that the CSP is not being under bancruptcy proceedings or mandatory management audit. 143 The Decision contains some other important provisions, such as (a) that the CSP of qualified certificates is obliged to provide its customers with a 24 hour basis certification revocation service [art.5 (5)], (b) that the same CSP must provide for a continuously updated directory of the valid and the revoked certificates [art.5 (8)], (c) that the above CSP must maintain a 7-days-a-week revocation list service [art.5 (9)], (d) that the same CSP must keep in written or electronic form a database including information (date of issuance, revocation, modification etc) about the qualified certificates it has issued [art.7 (1)] and a database of all the qua1ified certificates it has issued for 30 years from the date of their expiration or revocation [art.7 (2»), (e) that every CSP is obliged to notify EETT, its customers and all the other CSPs with which 1t has done business that he intends to stop operating at least three months before doing so [art.6 (a)], (f) that the CSP which issues qualified certificates iB obHged ω infoI1l1 its potential custorner at least for the latter's responsibilities flowing from the certficate' s use, for the code of conduct and the CPS of the *CSP* as wel1 as for the conditions and the procedure of revocation (art.8) and (g) that EETT has the right to check the comp1iance of the CSPs' functioning with the Ministerial Decree's provisions byinspections in the latters' place of business and imposition of the proper penalties (art.12).

F. Liability of CSPs

Considering the fact that CSPs act in a course of trade, fau1ts on the provision of certification services may take place in various ways. Thus, for example, the CSP may not take proper evidence of its customer' s identity-either because of its neg1igence or due to misrepresentation on behalf of the customer-

144; also, the CSP may not use security reliable technology, may not maintain a 24-hour-basis revocation list service or may employ dishonest or unskilled staff, reducing, as a consequence, its trustworthiness status.[145]

Liability issues cou1d arise towards the CSP's custorner-holder of a digital signature as wel1 as towards the third party which transacts with the CSP' s customer and relies on the latter's identification as this is verified by the CSP's certificate. Directive *1999/93* acknowledges the above risks and provides for a minimum framework of liabi1ity ru1es. What has to be clarified is that the provisions of art.6 of the Directive regulate the liabi1ity of CSPs issuing (or guaranteeing) a qualified certificate to the public and, thus, leave not only the functioning of CSPs in closed networks to be regulated by liability rules according to the contractual relationships between the members of those networks 146, but also the liabi1ity of CSPs that do not issue qualified certificates to be ruled wholly by national (contract) law.

Art. 6 refers to the liability of a CSP that issues a qualified certificate to the public "for damage caused to any entity or legal or natural person who reasonab!y relies on that certificate" [art.6 (1)]. Thus, what is basical1y regulated by the Directive is the CSP' s liabi!ity towards the recipient of the electronically signed and certified message, namely the re!ying party. The CSP's liability towards its customer (the holder of the certificate) is, *prinzα facie,* !eft solely on the contractual relationship between CSP and customer[147]; however, it is suggested 148 that art.6 could also be regarded as a minimum liability aspect that provides extra protection to the customer in addition to the contractual terms binding him. The notion of "reasonable re1iance" of the third party on the qualified certificate is also crucial for the maintenance of trust between CSPs and the public. Apart from situations where the third party is technically expertised, it is logical to intrepret the reasonability or this party' s reliance with a minimalistic approach, i.e. to exclude CSP’s 1iabi1ity only when the third party was extremely careless (did not check at all the compliance of the certificate with Annex **I** of the Directlve).149 On the other hand, the basis of liabi1ity for the CSP is negligence and not strict liability; the reasoning for that is that the CSP has the technical background to inspect in more depth any deficiencies related to its services and, thus, bears the burden of prooving that he did not act negligently when, for example, he collected the personal identification details of his customer.[150]

More specifically, art.6 (1) refers to the obligation of a CSP to compensate the relying party ("entity, legal or natural person") for any damage caused as regards to:
(a) the accuracy, at the time of issuance, of the information included in the qualified certificate and the existence of all the prerequisites prescribed (in Annex I) for a qualified certificate [art.6 (1) (a)]
(b) the assurance that the identity of the holder of the certificate corresponds to the signatory of the electronic document whose signature is guaranteed by the certificate [art.6 (1) (b)]
(c) the assurance that, in cases where the CSP produces both private and public keys, these products can be used in a complementary way [art.6 (1) (c)].

In addition, art.6 (2) makes the CSP liable if he neg1igently failed to register revocation of a qualified certificate. Furthermore, a CSP is al1owed by art.6 (3) to set a limit of liability according to the use of the qualified certificate-and, thus, not be liable for damage caused by further use- provided that this 1imitation is communicated to third parties. Additionally, the CSP is permitted by art.6 (4) to set a limit on the value of the transactions for which the qualified certificate can be used-and, thus, be excluded from liability generating from damage caused after the exceeding of this limit-, given that this 1imitation is recognisable to third parties.

All the above provisions provide a minimum "advisory" but "binding" set of rules for each Member State's regulator when he intends to rule on CSPs' liabi1ity; this means that stricter rules may apply in order to enhance security, a1though extra care should be taken so as not to create barriers to entry in the CSPs' market by making the provision of such services financially inattractive and, as a result, eliminate competition. In Greece, the liabi!ity issue is not ruled by the Ministerial Decree 150/2001. Decision 248/71 does not contain any special provision; however, according to Annex I of the Decision, the Certification Practice Statement (CPS) of the CSP shou!d contain, *inter αlία*, an analysis of the responsibi1ities and the liability of the CSP towards its customers (para 3) and the re!ying third parties (para 8). The absence of such details gives EETT the right to impose appropriate penalties after inspection (probably to declare the functioning of the CSP invalid and stop its business), although no measure is being specified in the Decision.

G. Cross-certiflcation within and outside the Community

Taking into consideration the universa! nature of e-commerce operated through open networks !ike the Web, and also the need of the European Union for harmonised rules on certification services so as to achieve a competitive level on that market, Directive 1999/93 provides for two aspects of e-signatures' services trade, i.e. intra and outside Community trade.

Art. 4 (1) mentions that "Member States may not restrict the provision of certification services originating in another Member State in the fie!ds covered by this Directive". It also states that a CSP estab1ished in a Member State will be governed by the rules of that Member State. Thus, a CSP estab1ished, for instance, in Greece which provides certification services not only in Greece but also in France will be supervised and, if necessary, penalised by the Greek authority (namely EETT) and the French authority may not confine the CSP’s activity. A problematic situation arises when the CSP is established in different Member States; which law will prevail is sti11 a question that could be possibly dealt with if an intra-Community voluntary accreditation scheme-perhaps not quite demanding in relation to high technologies at the beginning- started operating so as to harmonise the different national laws applying in each case.Art.4 (2) of the Directive provides for the free circulation of e-signatures' products in the internal market provided that they cornply with the standards set out in the Directive. Thus, codes, private and public keys as well as advanced methods of e-signing (steganography, biometrics etc.) are free to flow through the Community with the intention to enhance security and promote e-commerce.[151]

With reference to the international aspects of providing certification services and selling e-signatures' products, art.7 of the Directive intends to set up a friendly regime for CSPs established outside the Community. Thus, qualified certificates issued to the public by CSPs established in third countries must be recognised by national laws of the Member States as "legally equivalent" to those issued by intra-Comrnunity CSPs provided that: (i) the CSP established outside the Comrnunity complies with the provisions of the Directive and participates in a voluntary accreditation scherne of a Mernber State or, (ii) a CSP established in the Community guarantees the outsider CSP's certificate or, (íií) the outsider CSP's certificate is recognised under a bilateral or multilateral agreement between the Community and third countries. Three comments worth to be made here; firstly, that the Directive indirectly encourages the idea of CSPs being organised in voluntary accreditation schemes so as to facilitate the procedure of harmonisation of e-signatures' standards

and the free transborder flow of e-products and services. Secondly, that by referring only to CSPs issuing qualified certificates, the Directive leaves the ruling of those CSPs issuing 'sirnple' certificates to the national regulators, although the danger of discrimination and eradication of competition is perceptible. Thirdly, that in order to increase the level of competition and the investment in the European market, the Directive encourages the signing of bilateral or multilateral agreements between Member States and third countries. The same position is adopted by the Ministerial Decree *15012001* in its art.5.

5. PK1'B efficiency, key escrowing and key recovery

Although public key encryption has been widely recognised as the most effective and financially suitable way of signing electronical1y, its compliance with increased levels of security has been doubted. Starting from the fact that a trusted third party is needed to guarantee extra security, because the pair of private and public keys is just a pair of numbers that does not guarantee the identity of its holder, the regulation of the activity of that party is regarded by many experts as troublesome and problematic. Moreover, even if the problem of identification is being solved by the provision of advanced certification services, 152 the CSP is not able to ful1y verify that the holder of the key pair was actual1y in possession of his private key during the disputed transaction, as factual circumstances like loss, threat or fraud are always likely to take place. 153 Deficiencies in the maintenance of revocation lists or false calculation of a private key's Iifetime are also some parameters which have to be taken into consideration by the CSPs when reassuring their customers for the quality of their services. And if we consider that Directive *1999/93* regu1ates in an appreciable extent only the issuance of qualified certificates, the question of how the 'simple' certificates are going to be treated arises automatica1ly.

In addition, much debate has arisen on the issue of key esrcowing. Key escrowing is a system under which the holder of a private key deposits a copy of it with an escrow agent or, altematively, splits the key into several parts and deposits them with different agents (dispersion). 154 The idea behind that is that a superior authority wiIl be able to have access to the private key without having to gain that access directly from the holder. After having obtained a warrant by the courts, intelligence and law enforcement agencies will have access to any private key in order to fight terrorism or international crime.

Furthermore, key recovery is another similar alternative, based on the idea that the govemment or an organisation could set up a "key recovery centre" 155 where every interested key holder could send, through a message, a copy of his private key, so as, in cases of loss or dispute over it, the repository service could affirm its holder. However, it is being argued that by operating under a key escrow system, a private key is more vulnerable to on-line attackers as the security of the repository service can be harmed. 1η addition, it is suggested that the key holder loses the perfect control of his key as he further trusts its secrecy in another entity.156 Key recovery has also been criticised not only on the fact that it violates the right to privacy and that it is an ineffective measure for the prevention of crime (criminals are likely to use "multilayered encryption"), but a1so on the costly infrastructure needed for its designation in a global level and on the danger of being attacked by information invaders.[157]

Directive 1999/93 states in Annex **II** (para j) that a CSP which issues qua1ified certificates must not "store or copy signature-creation data of the person to

whom the certification-service-provider provided key management services". The same policy is followed by the Ministerial Decree (Annex **II** para j). It remains to the future to see if any dispute will arise over abuse of information stored in a govemmental repository; though, it is very likely that such interferences with citizens' private 1ife will take place under the alibi of national security, prevention of crime or maintenance of public order.

III. Conclusion-final remarks

Having attempted to assess the issue of electronic signatures from a technical and legaI perspective, we have completed thoroughly a challenging study. Several aspects of the above analysis are crucial for the understanding of the e-signing's idea and function and, therefore, should be taken into account.

Firstly, it became plain that the geographical horizon within which the electronic signatures are operating is completely different from the "hand-shaking" scope where the.handwritten signatures work; the traditional bazaar has been substituted by the virtual marketplace and on-line commerce has no frontiers. Thus, electronic signatures apply intemationally and their operation must be facilitated by the establishment of globally recognised technical standards which wi1l ensure security on the Net.

Secondly, what was rea1ised is that the existence of electronic signatures dependds, from a legal point of view, on the rules regulating the formation of contracts and their transforrnation in the Web world; the validity and admissibility of electronic contracts as evidence in legal proceedings go hand-by-hand with the legal recognition of e-signatures. AIthough paperless, the evolving on-line commercial practice still has as its cornerstone the notion of a contract which, in order to be binding for the parties, must be signed electronically in an impenetrable and bilaterally accepted way.

From a technical standpoint, the dissimilarity between the conventional methods of hand-signing and the modern techniques of e-signing is noticeable; from rubber stamps and seals we have moved to iris/handlvoice identification processes (biometrics) and elite technological solutions like steganography or quanturn cryptography. Public key encryption is the most widespread, easily performed, financially convenient and safe way of signing by electronic means, although many concerns on its efficiency in relation to faultless authentication and reliable certification have already arisen. Taking into consideration the tendency of Directive 1999/93 to encourage the one-sided development and "legalisation" of advanced electronic signatures, and bearing in mind the need for elevated criteria of trust which the market by itself irnposes on its players, we can predict that in the ernergent B2C and B2B as well as A2B and B2A markets novel forms of e-signing are likely to appear.

However, from a legal angle, handwritten and electronic signatures not only operate in the contract context but also serve the same purposes. In particular, they are used to identify the author of a document, to confirm his relationship with the written text and to reassure the reader that the signatory intented to be legally bound by the content of the scriptum; moreover, they guarantee for the integrity of the data content and prevent the signatory from repudiating in any sense (except if based on factual evidence) the va1idity of his signature. Electronic signatures additionally ensure the secrecy of the information exchanged via the electronic docurnent.

Therefore, manuscript and digital signatures should not be regarded as opponents but as contributors in the growth of e-commerce. By applying the idea of

functional equivalence, the national legislators of the Mernber States shall try to harmonise the customary and the contemporary ways of signing by recognising to the latters the right to be treated as equal to the firsts and to be legally admissible in legal proceedings as evidence. Directive 1999/93 has taken the initiative, and the greek Ministerial Decree has followed; though, the categorisation of electronic signatures into “simple/non qualified” and “advanced” blurs the field. It remains to the case law of each Member State to clarify the circumstances under which a “simple” e-signature can be faced as equal to an “advanced”, elucidating in that sense the consumers when choosing the safest way of transacting on the Internet.

After having implemented the concept of electronic signatures, the European Commission has moved cautiously to the next stage, namely the establishrnent of an open rnarket for e-signatures' products and services. By not recognising any e-signing practice as the ultimate method, Directive 1999/93 approaches cryptography and other techniques with a technologically neutral manner so as to hearten the entrance of new players into the market, reinforce competition within and outside the Community and build a safe environment for on-line commerce. Products other than codes and keys are quite likely to come into view in the e-commerce panorama. In the services' area, by putting into operation the practice of voluntary accreditation of Certification Service Providers (CSPs), Directive 1999/93 has moved one step further; the participation of CSPs in such schemes where the compliance with high-tech standards is compulsory, not only toughens competition and promotes technology through research and innovation but also, and more significantly, builds up a 'firewal1' of security on the Web. Recently, the European Commission has demonstrated its agony for the establishment of a safer digital signature marketplace and the opening of the european market to third countries with its **Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions “Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market”[COM(2008) 798]** 158

Furthermore, for the effective function of public key encryption, the existence of a Trusted Third Party is necessary. The connection between the actual identity of the signatory with his public key is of fundamental importance and the CSPs provide an alternative for the "physical presence" model which applies in the traditional trade.

Not surprisingly, the vital role which the CSPs play is accompanied by a number of legal issues. For instance, Directive 1999/93 (and the Greek Ministeria! Decree 150/2001) states that only the "qualified" certificates a CSP issues can give automatically !egal validity to an electronic signature. In addition, the designation, supervision, liability and cross-certification of CSPs issuing 'simple' certificates is left to the discretionary power of the national legislator, while for the CSPs that provide qualified certificates the same issues are dealt with in accordance to a minimum legal framework provided by the Directive itself. This "two-tier" approach, though inevitable for this embryonic phase of the e-signatures’ market where the priority seems to be the involvement of as many CSPs as possible, is probable to cause uncertainty in the consumers’ and businesses’ field. Voluntary accreditation schemes in national as well as in European level would be a way out; in a more mature stage of the market, a slight moving away from the technological neutrality principle by replacing voluntary with mandatory accreditation could give a better solution, provided that foreclosure of the relevant markets is avoided.

Focusing on CSPs that issue qualified certificates to the public, their

designation, functioning, supervision, liability and cross-certification throughout the Community is regulated by national laws that have to comply with the provisions of Directive 1999/93. Thus, for instance EETT is the Greek authority which sets out the insitutional precondition for the designation of a CSP, the technical standards which have to be followed, the ways and consequences of the supervision as well as the liability rules applying to each case and the cross-certification modus operandi. It is obvious that the better a national law adopts the Directive's provisions (from matters such as the compliance of the CSPs; technology with European and international standards to issues such as the ensurance of the reliability and state-of-the-art knowledge of the CSPs' staff), the more stable the structure of e-commerce becomes.

From a consumer protection viewpoint, the on-line customer not only is not deprived of the protection of national and international legislation on consumer protection, but also is placed in an advantageous position when dealing with a negligent CSP's mediation; the latter (CSP) has the burden of proving that it did not act negligently during the provision of certification services like time-stamping, public key registration and directory or revocation listing. The net-ignorance of the consumer is compensated by firm obligations imposed on the CSPs.

Moreover, from a data protection position, it became clear that the provision of key escrow and key recovery services has to be srutinized before implemented; the dangers it encloses for the privacy and the self-determination of the individual in the information society should be fairly balanced with the actual need for maintenance of public safety and national security.

Finally, it was comprehended that the motivation of any legislative attempt on electronic signatures does not rely solely on the grounds of technical applications but is rather a subsequence of public measures; thus, the European Union, by adopting Directive 1999/93, apart from harmonised standardisation and financial integration, has aimed at fortifying the e-commerce practice in the Community and toughening the levels of competition with the US market. In a microscopic level, similar should be the purpose of the Greek legislator in relation to the presence and the potential leading position of Greece in the Balkan territory's on-line commercial regime.

In a nutshell, behind the idea of electronic signatures there is the need for trust in an electronic environment characterised by anonymity and unlimited manipulation. The challenges which the traditional rules on forgery or fraud face are multiple as advanced technology becomes a dangerous weapon in the hands of competent but malicious netizens. While establishing a primary field of e-signing, policy-makers should place great emphasis on Intemet security.The future will show if "a technology born of distrust can become a guarantor of trust in the online world". 159

IV. Bibliography

a. Books

1. Arno R. Lodder and Henrik W.κ. Kaspersen, "eDirectives: Guide to European Union Law on E-Commerce", Kluwer Law Intemational 2002
2.Christopher Reed, "Intemet Law: Texts and Matelials", Butterworths 2000 3. D. Maniotis, "The digital signature as a means of confirming the va1idity of documents in CiviIlProcedure" (in Greek), Ant.N.Sakkoulas 1998
3. Ian J.Lloyd, "Information Technology Law", Butterworths 2000, 3rd edition
5. Konstantinos N. Christodoulou, ΄EIectronic Documents and Electronic Contract" (in Greek), Ant.N.Sakkou1as 2001
6. Li1ian Edwards & Charlotte Waelde, "Law & the Intemet: a framewor kfor electronic commerce", Hart Publishing 2000
7. Roland de Bruin, "Consumer Trust in Electronic Commerce: Time for Best Practice", Kluwer Law Intemational 2002
8. Stewart A. Baker and Pau1 R. Hurst, "The Limits of Trust: Cryptography, Govemments and Electronic Commerce", Kluwer Law Internationa11998

b. Articles

1. Adian McCul1agh, William Caelli and Peter Little, "Signature Stripping: A Digital Dilemma", *http://elj.warwick.ac.ukljiltlO1-1/mccu1lagh.html*, visited *27/05/2003*
2. Anastasia Papathoma-Betge, ΄EIectronic commerce: Legal issues on the transactions on the Intemet" (in Greek), Dikaio EPiheiήseon kai Etairion (Year 5), p.1237
3. Carl ElIison and Bruce Schneier, "Ten Risks of PKI: WI1at You9re not Being To}d about Public Key Infrastructure", Computer Security Joumal VoJ.XVI, Number 1, 2000

4. Chris Reed, "What is a Signature?", *http://elj.warwick.ac.uklii1t/OO-3/reed.html*, visited 27/05/2003

5. Chryssoula Michaelidou, "The electronic signature's problem" (in Greek), Dike Intemational 31 (2000) ρ.1188
6. Chήstína SpyreI1i, "Electronic Signatures: A Transantlantic Bridge? An Eυ and US LegaI Approach Towards Electronic Authentication", http://eli/warwick.ac.uk/iilt/02-2/spyrelIi.htmI, visited *27/05/2003*
7. Caro!ine Cope!and, "Digita! Signatures: Throw Away Your Pens", ENTLREV 2000, 11 (5)
8. ElIí Phi1ipopoulou, "The !ega! framework of e!ectronic commerce", Dikaio Epiheiriseon kai Etairion (Y ear 6) ρ.1086
9. Ioannis D. Igglesakis, "The legal provisions on digital signatures: Directive 1999/93 and nationallaws" (in Greek), Episkopisi Emporikou Dikaiou *C12000*, ρ.619 10. Jamie Munay, "Public Key Infrastructure, Digital Signatures and Systematic Risk", http://eli.warwick.ac.ukliilt/03-1/murray.html, visited 29/07/2003
11. James Backhouse, "Assessing Certification Authorities: Guarding the Guardians of Secure E-commerce?", Journal of Financial Crime Vol.9 No 3, 2002, pp.217-226 12. Jeremy Newton, "The European Directive on Electronic Signatures", EBL, March 2002, ρ.5
13. John Angel, "Why use Digital Signatures for Electronic Commerce?", http://eli.warwick.ac.uk/iilt/99-2/angel.html, visited 27/05/2003
14. Kamini Bharvada, ΄EIectronic Signatures, Biometrics and PKI in the UK", International Review ofLaw, Computers & Technology Vol.16, No 3, pp.265-275, 2002
15. Konstantinos N. Christodoulou, "Order of payment based on electronic document" (in Greek), Dike International 32(2001), ρ.457
16. Konstantinos N. Christodoulou, "Three new issues on the law of electroni documents after the draft on electronic signatures" (in Greek), Dike International 31(2000), ρ.1006
17. Lorna Brazel1, ΄Electroηíc Security: Encryption íη the Real World", EIPR 1999, 21

(1), 17-27
18. Nancy Muenchinger and Adam Mekaoui, "Regulation Aspects of Electronic Signatures", Computer Law & Security Report Vo1.l8 vol. 2002
19. Nicholas Bohm, Ian Brown & BRIAN Gladman, ΄EIectroηίc Commerce: Who Cames the Risk of Fraud?", http://eli.watwick.ac.ukliilt/00-3/bohm.html, visited *28/0$12003*
20. Nikos K. Rokas, "Modern Technology and Commercial Law" (ín Greek), Epiotheorisi Emporikou Dikaiou 98
21. Richard Hamson, "Public Key Infrastructure: The Risks of Being Trusted", C&L, August/September 2000
22. Sarah Andrews, "Who HoJds the Key?-A Comparative Study of US and European Encryption Policies", *http://eli.warwick.ac.ukliilt/00-2/andrews.htrnl*, visited *27/05/2003*
23. Steffen Hindelang, "No Remedy for Disappointed Trust- The LiabiIity Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in England and Germany Compared", *httP:lle1iIwarwick.ac.uklíilt/02-1/híndeIang.htmI*, visited 27/05/2003
24. Stephen Mason, "The Evidential Issues Relating to Electronic Signatures-Part Γ, Amicus Curiae Issue 45 JanuarylFebruary 2003
25. Vassilis S. Karagiannis, "The legal protection of electronic data exchange", Dikaio Epiheiriseon kai Etairion (in Greek) (Year 6), ρ.19
26. Vincenzo Sinisi, Sinisi Ceschini Mancini & Partners, Rome, "Digital Signature Legislation in Europe", Butterworths Joumal of IntemationaI Banking and Financial Law, January 2001

c. On-line references and links (due to date visited)

1. http://www.eett.gr. visited *27/05/2003*
2. Rosa-Julia Barcelo, "The German LegaI Situation after the Digital Signature Law", *http://www.droit.fundp.ac.be/tex* tesl addendum. pdf, visited *26/08/2003*
3. NigeI Hawkes, "Machines wiII pay up in blink of an eye", *http://www.cI.cam.ac.uklusers/igdl1000latm.ipg.* visited *27/08/2003*
4. http://www .pscom.co.uklproducts/signaturel, visited *27/0812003*
5. Declan McCuJlagh, "Bίη Laden: Steganography Master?", http://www.wiIed.com/news/poli tics/O,1283 ,41658,00.html, visited *30/05/2005* 6. MukuJ Pareek, "Cryptography-a primer", http://www.financeoutlook.comlcryptography.htm. visited *27/0812003*
7. http://www.apogeegraphology.com/lectures.html. visited *28/08/2003*
8. Kevin Scott Boomsma, "The Key Escrow Debate", http://ΓaPhael.math.uíc.edu/#ieɪemY/CIYPt/contríb/boomsma2.html, visited *29/0812003* 9. James M. Galvin, "Authentication, Non-Repudiation and Secure Electronic Signatures", http://lists.commerce.net/archi ves/ts-portfolio/ 199709/msgOOOO 1.html, visited *29/0812003*
10. httP://www.fΓeeniχ.fr/netjZen/chjffΓe/ecrYPto1.html. visited *29/08/2003*
11. http://www.ficoIa.fi/englantiltietoturva/suoiausm.htm. visited *10/03/2004*
12. http://www . archi ves. gov /records rnanagernent/pol icy and gui dance/electΓOni c signa ture technoJogy.htrnl, visited 29/08/2003
13. http://www.ternple.edu./pharrnacy QARN8, visited 29/08/2003
14.http://www.wayrnaker.se/bitonline/2003/05/20030523BIT00310/05230031.htm. visited 30/08/2003
15. http://www . irc/cec.eu.int/downloadlpress/newsletters/letter200005-en. pdf, visited 30/08/2003
16. http://www.dsanet.gr:83 80/W ebtop/ws/alis9i/www/case/Record ?set=6&m= 17 &sid=2 Q., visited 30/08/2003
17. http://www.cartoonbank.comlproduct details.asp ?/mscssid=DA 1DH4 UJDG459HA V C4PMEVB218TG24TB&sitetype=1&did, visited *30108/2003*
18. http://www .ac.uk.pgp.net/pgpnet/seqemail/q4/node8.htmI. visited 30/08/2003
19. http://www.pki.gov.ar. visited 31/08/2003

20. http://www.eurobank.gr, http://www.space.gr, http://www.adacom.com, htιp.://www.asyk.ase.gr, httP://www.acci.gΓ, http://www.deltasinguJar.gr, visited *30/5/2003*
21. http://www.eema.org/SProiects/esigqa.asp, visited 01/09/2003
22.http://www.tscheme.org, visited 01/09/2003 23.
http://www.ecp.nJ, visited 02/09/2003
24. http://www .elIΓOpa.eu.int/information society/eeuΓOpe/action pJan/safe/esi gnaturesin dex en.htm, visited 02/09/2003
25. http://www.opta.nl/index. asp ?urI=recentinfoπnati *onl* document.asp&i d= 1 063&thema id=0&pervurI=%2Findex&2Easp, visited 02/09/2003
26. MichaeI FΓOomkin, "The EssentiaI Role of Trusted Third Parties in Electronic Commerce", http://www.law.miami.edu/-froomkin/articles/trusted1.htm. visited 02/09/2003

d. Legislation

1. American Bar Association Digital Signature Guidelines 1996, http://www .abanet.org/scitech/ec/isc/dsg-tutori al.html, visited *26/08/2003*
2. Commission Decision 2000/7091EC "on the minimum criteria to be taken into account by Member States when designating bodies in accordance with art.3 (4) of the Directive 1999/93IEC", OJ L 289, 16/11/2000, ρ.42
3. Decision *132712001* of the One-Member Magistrate Court of Athens (case law reference),
http://www.dsanet.gr: 83 *801W* ebtop/ws/alis9i/www/case/Record ?/set::::6&m:::: 17 &sid:::: 26, visited *30/0812003* (in Greek)
4. Decision 248/71 of EETT "on the provision of electronic signatures' certification services" (FEK Issue *603/B/16-05-2002)* (in Greek)
5. Directive 97/7/EC "on the protection of consumers in respect of distance contracts", OJ L 144/19,4/6/1997
6. Directive 1999/931EC of the European Parliament and of the CounciJ of 13 December 1999 on a Community framework for electronic signatures, OJ L13/12, *19/1/2000*
7. Directive *2000/31IEC* "on certain legal aspects of information society services, in particular electronic commerce, in the IntemaI Market, OJ L 178, *17/712000*
8. Directive 2002/58/EC on privacy and electronic communications, OJ L 201/37, 31/7/2002

9. European Commission, "Communication to the European Parliament, the Council, the Economic and Social Committee of the Regions: A European Initiative in Electronic Commerce" COM 97 (157), 15/04/97
10. European Convention on Human Rights, http://www.echr.coe.intlEng/BasicTexts.htm. visited 25/08/2003
11. Greek Law No 2472/1997 "ση the protection of individuals with regard to the processing of personal data", http://www.dpa.gr/Documents/Eng2472engJ1.doc. visit~d 25/08/2003
12. Greek Ministerial Decree 150/2001 (FEKJIssue *125/Al25-6-200l),* http://www.gspa.gr/INETDHES/diadp/b-2-1-5.htm. *visited 26/08/2003 (iη Greek)*
13. Intemational Covenant oη Civil and PoJitical Rights, httP:l/www.unhchI'Och/htmI/menu3/b/aCCPr.htm. visited 25/0812003
14. Rome Convention oη the Law Applicable to Contractual Obligations *(801934/EEC), OI* L266, 09/10/1980
15. United Nations Commission oη Intemational Trade Law (UNCITRAL) Model Law oη Electronic Signatures 2001,
http://www . uncitral.orgl engli sh/texts/electcomlmJ-elecsi g -e. pdf, visi ted *26/08/2003* 15. Treaty estab1ishing the European Community (consolidated text) O] C 325, 24/12/2002, httP:lleuropa.eu.ınt/eur-teχ/eη/searchtΓeaties.htm, visited *24/08/2003*

V. Footnotes

1.Ian J. Lloyd, "Information Technology Law" 3fd edition, Butterworths 2000, p.p..29-31

2 see also recita114 of Directive 1999/93 on Electronic Signatures

3 Treaty establishing the European Community (consolidated text) O] C *325,24/1212002*, art.3 (1) (c),

23 and 24, http://europa.eu.int!eur-lex/enlsearch/searchtreaties.html, visited 24/08/2003

4 Their use is also apparent in the public administration system, in goveΓnmentaI organisations, in intelligent agencies (where the further issue of key-escrowing arises) etc.

5 European Commission, "Communication to the Euι-opean ParJiament, the Council, the Economic and Social Committee and the Committee of the Regions: A European Initiative in EJectronic Commerce", COM (97) 157, BrusseJs, 15/04/97, ρ.2.

6 ibid. ρ.2

7 Arno R. Lodder and Henrik W.K Kaspersen, "eDirectives: Guide to European Union Law on ECommerce-Commentary on the Directives on Distance SelJing, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection", Kluwer Law International 2001, ρ.3

8 Ronald de Bruin, "Consumer Trust in Electronic Commerce: Time for Best Practice", Kluwer Law International 2002, ρ.6

9 Directive *9717fEC* on the protection of consumers in respect of distance contracts, OI L 144/19, 4.6.1997

10 Directive 2000/31/EC on certain !ega! aspects of information society services, in particular electronic commerce, in the Interna! Market, OJ L 178, 17.7.2000

ll. footnote [7], ρ.3

12 Lilian Edwards and Charlotte Waelde, "Law & the Internet: a framework for e!ectronic commerce", Hart PubIishing 2000, p.18

13 ibid ρ.20

14 see ElOίη Philipopoulou, "The lega! framework of electronic commerce", Dikaio Epjheirjseon aki Etairion (Year 6) (in Greek), p.1087

15 ibid ρ.22

16 ibid ρ.22, where the postal rule is refeπed as an exemption to the general rule that a contract is concluded once the acceptance is sent and received by the offeror as it sets out that if the acceptance is sent by post (and not, for instance, by telephone OY telefax), it becomes effective "once posted, rather than when it is received".

17 ibid ρ.25

18 ibid ρ.25, where a click wrap contracting procedure is considered as different to e-mail contracting in two ways, name!y because during the first the communication between offeror and offeree is instantaneous and also because the practice of traditional negotiation of the terms of the contract that can take place through e-mails is replaced by the "1 accept" or "Yes" technique that applies to click wrap agreements.

19 ibid ρ.29; EC Directive on E-commerce art.lO (1)

20 ibid ρ.31; EC Directive on E-commerce art.lO (1),(2)

21 as set oυt in the Rome Convention on the Law Applicable to ContractuaI Obligations *(8OI934IEEC)* , OJ L 266, *09/10/1980*, arto3

22 Rome Convention, art.5 (1); EC Directive on E-commerce, art.2 (e)

23 ibid art.5 (2)

24 Directive 1999/93/EC of the European Parliament and of the Counci! of 13 December 1999 on a Community framework for e1ectronic signatures, *OI* L 13/12,19.1.2000, art.5 (1)

25 Internationa! Covenant on Civi! and Politica! Rights art.l7, which dec!ares that "no one shall be subjected to arbitrary or un!awfu1 interference with his privacy ... "; genera! comment 16 states"The gathering and ho1ding ofpersona! information on computers, data banks and other devices, whether by pub!ic authorities or private iηdividua1s or bodies, must be regu!ated by Jaw", http://www.unhchr.ch/htm!/menu3/b/accpr.htm. visited 25/08/2003

26 Eυτopean Convention on Human Rights art.8 (respect for private life with the exemption of interference permitted due to, *iηter αlia*, nationa! security and pub!ic safety reasons) http://www.echΓ.coe.jnUEng/BasicTexts.htm, visited *25/08/2003;* Directive *2002158/EC* on privacy and eIectronic communications O] L 201/37,31.7.2002

27 Greek Law No 2472/1997 on the protection of individuaJs with Γegard in the processing of personal data http://www.dpa.gr/DocumentsIEng2472engl1.doc. visited *25/08/2003*

28. United Nations Commission on InternationaJ Trade Law (UNCITRAL) Model Law

on E!ectronic Signatures 2001 http://www . llncitra!.org/engJish/texts/eIectcom/inl-elecsi g -e.pdf, visited *26/08/2003*

29 American Bar Association Digita! Signature Guide!ines 1996, http://w\VW .abanet.org/sci tech/ ec/i sc/ ds g -tutoria1.htmI, vi si ted 26/08/2003

30 Rosa-Julia Barcelo, "The German LegaJ Situation after the 'Digital Signature Law'", *http://www.droit.fundp.ac.be/textes/addendum.* pdf, visited *26/08/2003*

31 FEK Issue *125/* A/25-6-200l, *http://www.gspa.gI-ιINETDHES/diadp/b-2-1-S.htm.* (in greek), visited *26/0812003*

32 Konstantinos N. Christodoulou, "Electronic Documents and Electronic Contract (in Greek)", Ant N. Sakkoulas 2001, ρ. 174, where the author supports the view that, for reasons of technologicaI neutrality and improvement of e-commerce policy, the European Union has plIrposively left the field of electronic signatures that can be admitted as valid open to adjustments according to technology r:rogress.

33 Although the location of the signature shouJd not be a precondition of its vaJidity except if such a requirement is imposed by law,as it happens in the wilIs where each page mlIst be signed by the testator and the witnesses,Adrian McCullagh, "Signature Stripping: A Digital Dilemma", *http://eJi.warwick.ac.uk!iiltJO* l-l/mcculIagh.htmJ, visited *27/05/2003,* ρ.4

34 Chris Reed, "What is a Signature?", *http://eIi.warwick.ac.uk!iiJtJOO-3/reed.html*, visited *27/05/2003,* p.1

35 Karmini Bharvada, "Electronic Signatures, Biometrics and KI in the UK", Internationa\ Review of Law, Computers & Techno\ogy, vo!ume 16, Nα 3, 2002, ρ.266

36 footnote [34], ρ.2

37 footnote [35], ρ.267

38 ibid ρ.267

39 footnote [32], ρ.B

40 Nicho!as Bohm, Ian Brown & Brian G!adman, ΄EIectronic Commerce: Who Caπries the Risk of Fraud?", http://e!i.warwick.ac.uk/iiJtlOO-3/bohm.htmJ, visjted 28/05/2003, ρ.8

41 footnote [7], ρ.42, where it is he!d that this would be admitted as e-signing only if based on ar1.5 (2) of Directive 1999/93.

42 footnote [35], ρ.269

43 ibid ρ.270

44 ibid ρ.270; a!so, Nige! Hawkes, "Machines wiIl pay up in blink of an eye", http://www.c!.cam.ac.uk/users/igdl000/atm.ipg. visited 27/08/2003; aIso,http://members.fortunecity.comlpawanjanbandhu/biometrjc_signatures.htmI, visi ted 27/08/2003, where it is held that, aIthough advanced, the iris technique has a sIight possjbjJity of mistake every time due to factors such as "reflections from eyeg!asses, motion blur, noise in the camera etc".

45 footnote (35], ρ.270

46 footnote [34], ρ.I3; also, http://WWw,Dscom.co.uk./products/signature/, visited *27/0812003,* where it is said that pressure, rhythm, ink flow, timing and speed are the criteria of the examination of the authenticity of a digitised pad's signature.

47 footnote [35], ρ.27I

48 ibid ρ.27I

49 Declan McCullagh, "Bίη Laden: Steganography Master?", httP://www.wired.cσm/news/PωJιtιcs/O.I283.41658.00.html. visited 27/08/2003 50 footnote [33], ρ.272

51 http://www.cs.dartmouth.edul-/ford/crypto.html. visited *27/08/2003*

52 Sarah Andrews, "Who Holds the Key?-A Comparative Study of US and European Encryption Policies", http://eli.warwick.ac.ukliiItlOO-2/andrews.html, visited *27/0512003,* ρ.2

53 footnote [8], ρ.52

54 Lorna BrazeIl, ΄EIectronic Security:Eηcryption in the Rea! World", EIPR 1999,21 (1), pp.18-19

55 footnote [8], ρ.51

56Mukul Pareek, "Cryptography-a primer", http://www.financeoutJokk.comlcryptography.htm. visited 27/08/2003, where the 'computationaJ infeasibiJity' concept is regarded as a standard for KI encryption because:" 128-bit encryption has never beeη broken ... it wouId take a triJion-triIion years to crack

128-bit encryption using today's technoJogy".
57 JO,hn Angel, "Why use Digital Signatures for EIectronic Commerce?", http://eIi.warwick.ac.uk/iilt/99-2/angeI.html, visited 27/05/2003, *p.4*
58 Steffen HindeIang, "Nα Remedy for Disappointed Trust- The LiabiJity Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in EngJand and Germany Compared", httP://elj.warwick.ac.uk/iiItJ02-lIhindelanρ:.html, visited 27/05/2003, ρ.4
59 footnote [56], "a key, which is a user selected password, number OY 'passphrase', is used as a rιarameter in the encryption algorithm to convert the plaintext to encrypted text"
60 footnote [8], ρ.51 (footnote 70): "The digital signature itseJf consists of a signed message digest that often is attached to the message itself. Typically, the digital signature is sent a]ong with the message to the receiver".
61. footnote [8], p.51 (footnote 70): "The hash function has the property that, if the message is changed in any way, even by just one bit, an entirely different value will be produced by the hash function".
62. The influence of UNCITRAL Model Law on Electronic Signatures, http://www.uncitral.org/en-index.htm, vsited 25/05/2010, is obvious, as in art.2 (a) electronic signature is defined as "data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message".
63. see also Preamble of UNCITRAL Model Law, para 8
64. Crhistina Spyrelli, "Electronic Signatures: A Transantlantic Bridge? An EU and US Approach Towards Electronic Authentication", http://www.elj.warwick.ac.uk/jilt/02-2/spyrelli.html, visited 27/04/2003, p.4
65. From a greek point of view, this distinction is interpreted as if the "simple e-signature" can be used in any transaction where no formality is needed while the "advanced" e-signature can be used in all the other transactions that require formalities as equivalent to handwritten signatures, see John D. Igglesakis, "The legal provisions on Digital Signatures:Directive 1999/93 and National Laws", Episkopisi Emporikou Dikaiou C/2000 (in greek), p.633
66. An indirect reference is being made in art.1721 para 1 of the Civil Code that refers to the handwritten last will, where, apart from being written by the testator's hand itself, it must be written by his hand in whole, see Chryssoula Michaelidou, "The electronic signature's problem", Dike International 31 (2000) (in greek), p.1203
67. although in commercial transactions no formality is being required in greek practice, see N.K.Rokas, "Modern Technology and Commercial Law", Episkopisi Emporikou Dikaou 1998 (in greek), p.7. See also Anastasia Papathoma-Betge ,"Electronic commerce: Legal issues on the transactions on the Internet", Dikaio Epihiriseon kai Etairion (year 5, in greek), p.1240
68. D. Maniotis, "The digital signature as a means of confirming the validity of documents in civil procedure" (in greek), Ant.N.Sakkoulas publishing 1998, p.35
69. Still, case law has broadened the horizon of handwrtiting by recognising as legal valid signatures put by foot or mouth or signatures created by technical means such as fax or telex.
70.footnote [68], pp.83-87
71.Definitions of "signature-creation data" and "signature-verification data" respectively.
72. After being penalised, for example, by the European Commission, the European Court of First Instance or the European Court of Justice for not having implemented in a satisfactory degree the Directive's provision on data protection, consumer protection or Certification Authoritie's (CA's) designation etc.
73. this is also obvious by art.1 para 1 of the Directive, where the dual purpose of the Directive is "to facilitate the use of electronic signatures", and not to exhaustively rule it, and "to establish a legal framework fro electronic signatures and certain certification services in order to ensure the proper functioning of the internal market", and not to regulate in detail on their legal recognition. See also footnote [7], p.40. See also recital 4 of the Directive, where the framework provided by the Directive intends to "...strengthen confidence in, and general acceptance of, the new technologies"
74. as noted down in Annexes I, II, III, IV
75. see Vassilis Karagiannis, "The legal protection of electronic data exchange", Dikaio Epihiriseon kai Etairion (year 6, in greek), p.29
76. footnote [57], p.3

77. footnote [64], p.2
78. see also recital 8
79 Jamie Murray, "Public Key Infrastructure, Digita! Signatures and Systematic Risk", http://eli.warwick.ac.uk/iiltJ03-lImurray.html, visited *2910712003,* ρ.3
80 as weII as for, e.g., the reader of a last wiII on which some parts of the text have been scratched, rewritten or de!eted without having been signed, a!though there is a s!ight difference: any alterations on an electronic message are hardly detectable, while forgery on manuscripts is demonstrab!e with the helpof graphology (see, e.g., http://www.apogeegrapho!ogy.com/!ectures.html. visited 28/08/2003)
81 footnote [8], ρ.51 (footnote 70)
82 chapter 1 (B) (b)
83 art.2 (4)
84 art.2 (5)
85 art.2 (6) in combination with Annex ΠI, where the need for extra securjty appears through the use of phrases such as "the signature-creation-data used for signature generation can practicaIly occur only once" (para 1) (one-way function), "secrecy reasonabJy assured" (para 1), "the signature creation
data ... be reliably protected by the legitimate signatory against the use of others" (para 2) etc.
86 art.2 (7)
87 art.2 (8)
88 art.2 (12)
89 Stewart A. Baker & Paul R. Hurst, "The Limits of Trust:Cryptography, Governments and Electronic Commerce", Kluwer Law International1998, *p.4*
90 footnote [8], ρ.13
91. Kevin Scott Boomsma, "The Key Escrow Debate", http://raphaeI.math.uic.eduJ#ieremy/crypt/contrib/boomsma2.htmI, visited 29/08/2003
92 See aIso recitaI 18 :"The storage and copying of signature-creation data could cause a threat to the legaI validity of electronic signatures".
93 Stephen Mason, "The Evidential Issues Relating to Electronic Signatures-Part 1", Computer Law & Security Report Vol.18 no.3 2002, ρ.175
94 non-repudiation can be divided into "non-repudiation of origin" which prevents the creator of the message from claiming that he did not send it, and "non-repudiation of delivery" which prevents the message's recepient from denying having received it, footnote [8], ρ.14

95 James M. Galvin, "Authentication, Non-Repudiation and Secure Electronic Signatures", http://lists.commerce.net/archives/ts-portfoiio/199709/msgOOOOl.html, visited 29/08/2003
96 art.l para 2
97 art.5 (l) (b)
98 See also recitaJ 21:" ... this Directive ... does not affect national rules regarding the unfettered judicial consideration of evidence".
99 which, in closed networks where "contractual relationships and mutual trust already exist" between the users *(http://www.freenix.fr/netizen/chiffre/ecrypto1.html.* visited *29108/2003)*, is not as doubted as in semi-open networks like "the internal networks of companies" *(http://www.ficora.fi/englantıltietoturva/suoiausm.htm.* visited *29108/2003)* Oι' in open networks like the Internet.
100 the "structural integrity" of a record, i.e. the non-alteration of its structure (structure="jts physical andlogical format and the relationships between the data elements comprising the record"), is a special aspect of integrity,
http://www.archives.gov/records managementlpolicy and g:uidance/electΓOnic signature technology. html, visited *29108/2003*
101. the use of "secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify Oι' delete electronic records" (http://www.temple.edulphal'macv QARN8, visited *29108/2003)* is also encouraged by Directive *1999193* which, in recital 9 refers to "time-stamping services" 01' "computing services",
102. Adrian McCullagh & Wi11iam Caelli, "Non-Repudiation in the DigitaI Environment", *http://www.tirstmonday.dk/issues/issue5* 8/mccullaghl, visited *29108/2003*

103 footnote
[57], ρ.5

104 footnote [34], ρ.9

105 Vincenzo Sinisi, Sinisi Ceschini Mancini & Partners, Rome, "Digita! Signature Legislation in EUiΌpe", B utterworths Journal of Internationa! Banking and Financial La w, J anuary 200 I, ρ.I7

106 and the mathematical procedure that follows the application of that private key to the encryption a!gorithm

107 Considering that a signature can bc stored in a computer's hard disc, a floppy disc, a removab!e disc or a smart card (for smart cards see, e.g. http://www.\.Iayrnaker.se/bitonline/2003/05/23/20030523BIT0031O/0523003I.htm, visited 30/08/2003), it can be rea!ised how easily a private key could be attacked, !ost, sto!en or destroyed and, as a result, the risk of forgery and fraud the owner of that key runs. *http://www.ac*. uk. pgp.netlpgpnetlsecemai1lq4/node8.html. visi ted *301081200*

108 footnote [57J, ρ.6, where the autll0r says:"Instead of creating a cornplete new Iegal framework, existing achievements shouId be advised, as far as they are compatible with !T".

109. Provided that it is an advanced signature based on a qualified certificate and created by a securesignature-creation device [art.5 (1)].

110 Maybe because the other forms of e-signing (biometrics, steganography, quantum cryptography etc) apart from KI encryption have not developed enough so as to create the need for special and separated legislative treatment.

111.http:///www.irc.cec.eu.int/download/press/newsletters/letter200005-en.pdf, visited 30/08/2003, ρ.Z 1]2 Decision 1327/2001 of the One-Member Magistrate Court of Athens,

112. http://www .dsanet. ψ: 83 80/W ebtop/ws/alis9i/www/case/Record?set=6&m= 17 &sid=26, visited *30/08/2003* (in Greek).

113. It is common knowledge that a person can have more than one e-mail addresses, even by having provided false personal information to the ISP. "Eavesdropping" is another technique for diverting emails from the real owner and forging his e-signature, *http://www.ac*. uk. pgp.netlpgpnetlsecemai1lq4/node8.html. visi ted *3010812001*

114 see Konstantinos N. Christodoulou, "Order for payment based on electronic document" (in Greek), Dike International 32 (200l),pp.457-471

115 This is permitted by art.6 (4) ofthe Directive; see also, e.g., http://www.adacom.gr/engIish/frames.htm. visited 30/08/2003

116 Christopher Reed, "Internet La w: Texts and Materials", B utterworths, 2000, ρ.119 (The phrase originates from a cartoon, http://www.cartoonbank.com/product detai!s.asp ?mscssid=DA 1 DH4 UJDG459HA VC4PMEVB218TG 24TB&sitetype=1&did, visited 30/08/2003)

117 footnote [79], ρ.3

118 in contrast with biometrics, where the use of fingerprints or iris colour verify in an unmistakable way the identity of the person acting as advanced electronic IDs.

119 CaroIine Copeland, "DigitaI Signatures: Throw away your pens", Entertainment Law Review2000, 11 (5), ρ.112

120 footnote [57], ρ.4; in Greek law, this problem would be dea1t with by PenaI law (fraudu!ent use of signature) and Civil law (damage on the right of the person on his name).

121 in contrast with closed networks where the levels of trust are high!y based on personal relationships and voluntary agreements., see recital 16 of the Directive.

122 Stephen Mason, "The Evidentia! Issues Relating to Electronic Signatures-Part II", Computer Law & Security Report Vo1.l8 no 4 2002, ρ.244

129 namely: www.eurobank.gr, www.adacom.com, www.edps.gr, www.ase.gr/repository, www.ypesdda.gov.gr, www.geniki.gr, www.eap.gr, www.ktpae.gr and www.acci.gr,visited 30/05/2010

130 http://www.acci.gr/enindex2.htm. visited 30/05/2003

131 ar1.2 (10): "Qualified certificate means a certificate which meets the requirements laid down in Annex I and is provided by a certfication-service-provider who fulfills therequirements Iaid down in Annex Π".

132 OJ L 289, 16/11/2000 ρ.42

133 http://www.eett.gr/engpages/index2.htm. visited 27/05/2003 . See also Decision 248/71 (FEK Issue 603/B/16-05-2002), http://www.eett.gr/opencms/export/sites, visited 25/05/2010,

Regulation on the Provision of Electronic Signature Certification Services (FEK Issue 284/A/22-11-2002), Regulation 295/63 on the designation of bodies for the conformity assessment of secure-signature-creation devices and secure cruptographic modules and on the designation of bodies for the conformity assessment of certification service providers using the voluntary accreditation criteria, http:www.eett.gr/opencms/export/sites/deefault/EETT_EN?Electronic-Communications/DigitalSignatures/295-63.pdf, visited 25/05/2010, Regulation 295/64 on the conformity assessment of secure signature creation devices and secure cryptographic modules, Regulation 295/65 on the Voluntary accreditation of the certification service providers.

134 art.2 (11)

135 footnote (119], p.28

136 prior authorisation is defined in recita! 10 as " ... not only any permission whereby the certificaltion service provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect".

137 footnote [7], ρ.48

138 the market forces' concept drives the stucture of the e-signatures' market; see, e.g., "Questions and Answers from EEMA's European Electronic Signatures Directive Workshop, November 2001, Brusse!s, http://www.eema.org/SProiects/esigqa.asp, visited *01109/2003*, where it is said:"The value of a qualified eIectronic signature depends on market demand"

139 http://www.tscheme.org, visited 01/09/2003; see also, http://www.ecp.nl, visited 02/09/2003

140 see http://www.eett.gr/engpages/index2.htm. visited 27/05/2003

141 footnote [7], ρ.51; see, e.g., http:I/www.europa.eu.intlıformatíonsocıety/eeurope/actionplan/safe/esignaturesindex_en.htm , visited *02/0912003*, where we read that Germany, Austria and Denmark provide for mandatory notification, while in the Netherlands CSPs issuing qua!ified certificates have to register to OPTA which "does not conduct an assessment before registration"

(http://ww w. opta. nl/index.asp? /url=recentinformatio *ηl* document.asp&id= 1 063&themaid=O&prevurl= %2Findex&2Easp, visited 02/09/2003).

142 Decision on the provision of electronic signatures' certification services (FEK Issue 603/BIl6-052002)

143 see Konstantinos N. Christodoulou, "Three new issues on the electronic signatures' law after the Greek draft on electronic signatures", Dike Internationa! 31 (2000), ρ.1033.

144 Michael Froomkin, 'The Essentia! Role of Trusted Third Parties in Electronic Commerce", http://www/law/miami.edu/-froomkinlarticles/trustedl.htm. visited *02/09/2003*

145 footnote [57}, ρ.6

146 recitaI 16; see a1so, footnote [7J, ρ.58

147 and probably to the consumer protection Iaw applying to each contractuaI relationship 148 footnote [7], ρ.59

149 ibid ρ.60

150 ibid ρ.61; Directive art.6 (1) (c)

151 see Nancy Muenchinger and Adam Mekaoui, "Regulatory Aspects ofElectronic Signatures", Computer Law & Security Report Vol.I8, vol. 2002, ρ.29

152 though the possibility of misrepresentation of the holder is high, as the classification of certificates system does not require strong identity proof for all the categories when registering.

153 Carl Ellison&Bruce Schneier, "Ten Risks of PKI: What Y ou're not Being Told about PubIik Key Infrastructure", Computer Security Journal Vol.xVI, Number 1, 2000, ρ.6

154 footnote [54], ρ.20

155 ibid ρ.21 156 ibid ρ.20

157 footnote [52], pp.4-5

158.http:www.europa.eu./legislation_summaries/information_society/l24118_en.htm,25/5/10

159. footnote [89], p.5