ARTICLE:

ELECTRONIC SIGNATURES: VALUE IN LAW AND PROBATIVE EFFECTIVENESS IN GREECE

WRITTEN BY:
DR. KOMNINOS KOMNIOS

This article focuses on the law on electronic signatures in Greece and outlines how electronic signatures are evaluated in court. Consideration will be given to the implementation of the EU Electronic Signature Directive into national legislation. The result is that the EU Directive was transposed correctly in general terms. However, regarding the details, some provisions are open to criticism. Relevant case law is considered throughout the article.

The Background

The European Directive on Electronic Signatures[1] binds the Greek legislator. Thus, the requirements for electronic signatures laid down in this Directive apply to the Greek legislation on electronic signatures. It may be stressed that Greece was among the first countries in the European Union that issued a law concerning electronic, respectively digital, signatures prior to the EU Electronic Signature Directive. Article 14 of Law 2672/1998 on "the exchange of documents by electronic means (telefax/e-mail) between the public administration services or between public administration services and citizen" regulates the electronic exchange of documents within the Greek public sector. Article 14.2 lit. e) of the Law 2672/1998 is, however, restricted to a simple definition of digital signature. This regulation does not provide for electronic signatures in general, but only for the use of digital signatures in the public sector.

The Greek Civil Code does not require that private law conventions should adopt a specific form in order to be legally valid (Art. 158 Greek Civil Code). This means, as a general matter, legal acts must be executed in certain form only when the law so requires (Art. 158 Greek Civil Code) or the parties have so provided (Art. 159 Greek Civil Code). The types of form known to Greek law are: the 'written form', i.e. an instrument under a handwritten signature, a notarial act, and various kinds of affidavits before public authorities. Legal acts do not require any of these forms unless the law or the parties have so provided. To sum up, under Greek law there are no formal requirements for a contract to be valid, unless explicitly provided for by law or the parties. However, the provisions of various items of Greek legislation mandate the use of written form (i.e. an instrument under a handwritten signature) for the passing of certain acts.[2] For example, Art. 849 of the Greek Civil Code provides that a surety bond requires a handwritten signature in order to warn the surety. The handwritten signature is the only constituent fact of the written form under Greek Law.[3] Where written form is required by statute, the document has to be signed by hand (Art. 160.1 Greek Civil Code). The failure to satisfy a signature requirement provided for by statute renders a transaction void in principle, nor may the parties derogate from the legal rules concerning statutory form. Signatures by stamp, by telegram or facsimile are not considered to be 'handwritten' in this context. The rationale for such statutory signature requirements is related to the functions of written form.[4] When no statutory signature requirements are applicable, but the parties have agreed to apply them anyway, the statutory provisions concerning signature requirements are

[1] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 19.1.2000 L13/12).*

[2] *On the meaning of such formal legal acts, see Konstandinos Kerameus and Phaedon Kozyris (eds.), Introduction to Greek law, (2nd revised edition, 1993 Kluwer/Sakkoulas), 64.*

[3] *See Stelios Koussoulis, Contemporary forms of written transactions (in Greek), (1992 Ant. N. Sakkoulas Publishers), 82; see also Dimitrios Maniotis, The electronic formation of contracts and the liability of third parties responsible for the authentication of the electronic document (in Greek), (2003 Ant. N. Sakkoulas Publishers), 23.*

[4] *On this issue see Apostolos Georgiades, General Principles of Civil Law (in Greek), (3rd edition, 2002 Ant. N. Sakkoulas Publishers), 382.*

applied unless the parties have agreed otherwise (Art. 160.1 Greek Civil Code).

Private documents with a handwritten signature enjoy enhanced evidentiary status under the Civil Procedure Code. They are regarded as genuine when they have been actually made by the party who appears to have signed them and when they have not been subsequently altered.[5] The prerequisite for the probative effect of a private document is the recognition of its authenticity or the proof of its authenticity by the party adducing the instrument.[6] In principle, it is sufficient that a private writing bears the signature of the person who appears to have signed it.[7] Insofar as the authenticity has been accepted through recognition or has been proven, private documents that are duly signed, are conclusive evidence that the statements that they contain have been made by the person who appears to have signed them (Art. 445 Code of Civil Procedure).[8] The prevailing opinion in Greek Law also accepts that they provide full evidence for the declarations that are contained in them, but only as against the person who signed them.[9] This probative effect can be overcome by any means of counterproof except testimony (Art. 393.2 Code of Civil Procedure).

Because of the requirement of a handwritten signature,[10] it is generally held that an electronic document cannot be a private document,[11] meaning that it cannot enjoy the probative effect described above. However, Art. 444 Nr. 3 of the Civil Procedure Code defines that photographs, films, recording tapes and all other kinds of mechanical reproductions are to be considered as private documents with evidential effect.[12] Pursuant to Art. 457.4 of the Civil Procedure Code, the authenticity of such mechanical portrayals can be disputed before a court of law. In this regard, Greek legal theory[13] and jurisprudence[14] accords evidential weight to both signed and unsigned electronic documents, which are deemed as mechanical reproductions according to Art. 444 Nr. 3 of the Civil Procedure Code.[15]

The Greek e-signature legislation

The EU Electronic Signature Directive was implemented into Greek law by the Presidential Decree 150/2001 *Implementation of Directive 99/93/EC of the European Parliament and Council on a community framework for electronic signatures*. It came into force on 25 June 2001. The Presidential Decree contains the common and abstract rules for electronic signatures and is supplemented by signature Regulation No 248/71 of the Hellenic Telecommunications and Post Commission - EETT (Regulation 248/71) "on the provision of certification services for electronic signatures" which deals with technical details. The Presidential Decree is structured in the same way as the EU Electronic Signature Directive and consists of 10 articles, the most important of which are: Art. 1, which defines the scope and coverage, Art. 2 contains the definitions of article 2 of the Directive, Art. 4 deals with the market access and the Internal market principles, Art. 5 regulates international aspects, Art. 6 adjusts the liability of certification-service-providers, Art. 7 lists requirements for the data protection, Art. 8 adjusts the notification of the Commission according to article 11 of the Directive, and Art. 9 literally transposes the Annexes of the Directive.

Definitions

The Presidential Decree provides a definition of electronic signature and one of advanced electronic signature. Both the Presidential Decree (Art. 2.1) and the EU Electronic Signature Directive similarly define the 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. The term electronic signature is very broad: it would

[5] *Pelayia Yessiou-Faltsi, in International Encyclopaedia of Laws, Civil Procedure - Suppl. 28 (Hellas), General Editor: Prof. Dr. R. Blanpain, (2004 Kluwer Law International), § 394.*

[6] *Art. 445 Code of Civil Procedure.*

[7] *Pelayia Yessiou-Faltsi, Civil Procedure in Hellas, (1995 Kluwer/Sakkoulas), 349.*

[8] *Pelayia Yessiou-Faltsi, in International Encyclopaedia of Laws, Civil Procedure - Suppl. 28 (Hellas), note 5, § 400.*

[9] *For details Kostas Beys, Commentary on the Code of Civil Procedure IIb (Art. 335-465) (in Greek), (1975 Sakkoulas), Commentary on Article 445, 1750-1751; Ioannis Tentes in Konstandinos Kerameus, Dionysios Kondylis and Nikolaos Nikas, Commentary on the Code of Civil Procedure (in Greek), (2000 Sakkoulas), Article 445 no. 4-6; Pelayia Yessiou-Faltsi, Law of Evidence, (in Greek), (3rd edition, 1986 Sakkoulas), nr. 266, 289. See, however, Paris Arvanitakis, Questions concerning documentary evidence (in Greek), (1992 Sakkoulas), 115.*

[10] *Art. 443 Code of Civil Procedure.*

[11] *See Stelios Koussoulis, Contemporary forms of written transactions, 142; Dimitrios Maniotis, The digital signature as a Means for the ascertainment of authentic documents in civil procedural law (in Greek), (1998 Ant. N. Sakkoulas Publishers), 65. Concerning the distinction between public and private documents under Greek law, see Pelayia Yessiou-Faltsi, supra note 7, p. 344.*

[12] *Pelayia Yessiou-Faltsi, Civil Procedure in Hellas, 350-351.*

[13] *See Stelios Koussoulis, Contemporary forms of written transactions, 142; Dimitrios Maniotis, The electronic formation of contracts and the liability of third parties responsible for the authentication of the electronic document, 34; Ioannis Pitsirikos, New ways of Communication (telefax, telex, electronic document) for the constitution of formal legal acts as subject of the Relationship of written form and legal act (in Greek), (2002 Ant. N. Sakkoulas Publishers), 389. See also Kostas Beys (in Greek), Dike 2001, 466; Ioannis Igglezakis, RHDI 2002, 536; Argiro Karanassiou (in Greek), Dike 2002, 565.*

[14] *Athens Single-Member Court of First Instance 1963/2004, published in Dike 2005, 586; Athens Single-Member Court of First Instance 1327/2001, published in Dike 2001, 457. For a case note in English, see Georgia Skouma, Case Note, e-Signature Law Journal, Volume 1, Number 2 (2004), 95 - 98; see also Ioannis Igglezakis, RHDI 2002, 531; For an English translation by Michael G. Rachavelias, see Digital Evidence Journal, 2006, Volume 3 Number 1, 57 – 60.*

[15] *Article 448.2 of the Civil Procedure Code: "mechanical reproductions consist a full proof for the facts or things which are stated upon them; however, counterproof is permitted".*

A qualified certificate is a certificate which is compliant with the format described in Annex I of the Presidential Decree and which has been issued by a provider who meets the requirements of Annex II.

even encompass a scanned image of a handwritten signature in a word processed document. The present wide diffusion of the digital signature, absolutely prevalent with respect to other technologies, has deeply conditioned the Greek legislator, by constituting an explicit reference model: "advanced electronic signature" or "digital signature" means 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.

A closer look reveals, however, that the Presidential Decree envisages three different kinds of electronic signature:[16] a simple electronic signature, an advanced electronic signature and an advanced electronic signature based on a qualified certificate and created by a secure-signature-creation device. Unfortunately, the Presidential Decree did not clarify this by expressly naming signatures that fulfil the above mentioned requirements. For the sake of distinguishing between such a signature and other forms of signature, which do not meet the same level of functional security, the term "qualified" electronic signature will be used. A qualified certificate is a certificate which is compliant with the format described in Annex I of the Presidential Decree and which has been issued by a provider who meets the requirements of Annex II. A secure signature-creation device is a device that fulfils the security requirements of Annex III of the Presidential Decree. The provisions of Annexes I, II and III of the Presidential Decree are the equivalent of the provisions of the EU Electronic Signature Directive.

The term "signatory" is defined under the Presidential Decree as a natural or legal person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. Regulation 248/71 (Art. 4.1), however, considers only contractually capable natural persons as beneficiaries of qualified certificates. Hence, only a natural person can be the signatory of a "qualified" electronic signature, since this form of electronic signature is based on a qualified certificate.

Legal effects of "qualified" electronic signatures

The Presidential Decree defines the organizational framework of electronic signatures and sets the requirements for their legal recognition. As to the legal effect of the "qualified" electronic signature (those regulated by article 5.1 of the EU Electronic Signature Directive) the Greek legislator decided to explicitly recognise the equivalence between the handwritten and a specific type of signature by imposing the same conditions as those stipulated in article 5.1 of the EU Electronic Signature Directive. Art. 5.1 (a) and (b) of the EU Electronic Signature Directive is implemented by article 3.1 of the Presidential Decree, stipulating that the advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device is legally equivalent to a handwritten signature both in substantial law and procedure. In addition, the legal effectiveness and admissibility as evidence in legal proceedings of all electronic signatures is not denied solely on the grounds that it is not a "qualified" electronic signature.

Therefore in Greece, the general rule is that documents may be used in electronic form. If there is no form requirement, electronic documents can be used without an additional electronic signature, which means that the sender of an e-mail does not need to type their name into an e-mail for it to be valid. However, if there is the requirement of statutory written form, electronic documents can only be used if they are signed with a "qualified" electronic signature, which is considered the electronic equivalent of the handwritten signature. "Non-qualified" electronic signatures do not satisfy the

[16] *Komninos Komnios, The electronic signature under German and Greek law (in German), (Peter Lang Verlag 2007), 258.*

requirement of statutory written form. This rule is applicable to all general and specific laws in the private sector, as for instance the other provisions of the Greek Civil Code or the Greek Commercial Code. Art. 8.2 of the Presidential Decree 131/2003 "Implementation of Directive 2000/31/EC of the European Parliament and Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)"[17] recognizes three exceptions concerning contracts which, according to Greek law, may not be valid if conducted by electronic means.[18]

Since the "qualified" electronic signature is considered by law as equivalent to the manuscript signature, an electronic document constitutes an evidentiary private document according to Art. 443 of Civil Procedure Code, as long as it is signed with a "qualified" electronic signature. The provisions about private documents are directly applicable in the same way.[19] Thus, if the opposing party disputes authenticity, the party adducing the electronic document must prove the document's authenticity (Art. 457.1 of the Civil Procedure Code). The provisions of Art. 457.3 of the Civil Procedure Code makes things somewhat easier, in that the content of the document above the signature will be assumed to be authentic where the authenticity of the signature has been established. Therefore, the dispute will centre upon the authenticity of the "qualified" electronic signature. However, the Greek legislator did not include a legal presumption concerning the authenticity of private deeds signed with a "qualified" electronic signature. It is not necessary that this should be regulated by a statutory rule of evidence.[20] The Greek law of evidence is flexible, and is, moreover, technology-neutral and hence open to future developments. Although some judges may not be familiar with electronic signatures, this must change, because they are used every day. Users of "qualified" electronic signatures which conform to the Presidential Decree will normally have good evidence that the signature was used. Given that "qualified signed" electronic documents have to comply with the extremely high standards set by the Presidential Decree, it is anticipated that judges will accept that a "qualified" electronic signature, if checked according to the Presidential Decree, will constitute prima facie evidence in regard to the identity of the owner of the signing device and the integrity of the message. Such evidence is not based upon a principal derived from experience, but upon the requirements that ensure that a high degree of security exists for this signature scheme.

To sum up, where an electronic document bears a checked "qualified" electronic signature, the court, by way of prima facie evidence, is expected to assume that it is genuine, i.e. that it originates from the beneficiary of the particular qualified certificate concerned. This prima facie evidence can be upset by simple counter-evidence if it is proven that there is a serious possibility of an occurrence other than the one derived from prima facie evidence, e.g. by facts that give rise to serious doubts that the declaration was made by the signatory. As a result, the roles of parties in proceedings are expected to shift in favour of the one with whom the burden of proof of electronic conclusion of a contract lies. Where an electronically signed document is submitted in evidence and the authenticity of the "qualified" signature is contested, the full onus of proof does not lie with the party adducing that evidence, as in the case of a written document, and since it is up to the party contesting the evidence to challenge that evidence, the burden of proof must, generally speaking, turn out to be to the disadvantage of the actual or alleged signatory. If, for example, person Y obtains a "qualified" signed document from person X, the document is treated as authentic because of the prima facie evidence. If person X denies this, then they need to prove that they did not sign the document (reasons include the private key and PIN were stolen, or someone forged identity papers and acquired a false private key, for instance). This interpretation enables "qualified" electronic signatures for the use in court as evidence of signature. It remains to be seen how the courts will deal with this new proposed form of prima facie evidence.

As far as the treatment of electronic documents signed with a "non-qualified" electronic signature is concerned, it is difficult to agree with the prevailing opinion, which deems them to mechanical reproductions – and thus deeds - according to Art. 444 Nr. 3 of the Civil Procedure Code. Given that both legal doctrine[21] and jurisprudence[22] classify traditional paper

[17] *See Elisa Alexandridou, E-Commerce Law (in Greek), (2004 Sakkoulas), 40; Ioannis Igglezakis, The Legal Framework of E-Commerce (in Greek), (2003 Sakkoulas), 147; Komninos Komnios (in German), ZfRV 2005, 63.*

[18] *(a) contracts that create or transfer rights in real estate, except for rental rights; (b) contracts requiring by law the involvement of courts, public authorities or professions exercising public authority; and (d) contracts governed by family law or by the law of succession. The use of electronic signatures is also excluded in relation to the establishment of a handwritten will, since the law requires that both text and signature must be handwritten (Art. 1721 Greek Civil Code).*

[19] *Komninos Komnios, The electronic signature under German and Greek law, 372.*

[20] *Komninos Komnios, The electronic signature under German and Greek law, 348. See, however, Dimitrios Maniotis, The electronic formation of contracts and the liability of third parties responsible for the authentication of the electronic document, 31.*

documents which are not signed with a handwritten signature as evidence, which do not conform with the statutory requirements, and since only the "qualified" signature is the electronic equivalent to the handwritten signature, it follows that electronic documents which are not signed with a qualified signature should be categorised as evidence, which do not conform with the statutory requirements with free appraisal of evidence.[23]

Accreditation and Supervision

The Hellenic Telecommunications and Post Commission (EETT), is the authority responsible for the control and supervision of certification-service providers for electronic signatures that are established in Greece, as well as for ascertaining compliance with secure-signature-creation devices. In parallel, EETT is responsible for the designation and supervision of private or public sector bodies for the accreditation of certification providers (CSPs), as well as for ascertaining compliance with secure-signature-creation devices.

It must be noted that, according to Art. 4.8 of the Presidential Decree and Art. 9 of Regulation 248/71, EETT supervises and inspects all CSPs established in Greece, regardless of whether they issue qualified certificates or not. The Greek legislator has, therefore, introduced a broader supervision scheme than the EU Electronic Signature Directive requires. The prior authorisation of certification services is prohibited by law (Art. 4.4 Presidential Decree). However, the Regulation generally requires all CSPs to notify their services to EETT. The notification is supposed to occur upon commencement of their operations; the CSP has to submit the following information to the authority: relevant co-ordinates (name, address, website, etc.), company's legal form and authorized representatives, the taxpayer's Identity Number of the Provider, and a description of services provided. CSPs issuing qualified certificates should submit several documents in addition. The submission of the information by the CSPs is sufficient to start the services, so that notification does not introduce prior or hidden authorisation. The EETT holds a registry in electronic or paper form of the data of all the CSPs established in Greece. The registry is also required to mention those CSPs who, according to their declaration, issue qualified certificates. All CSPs are required to inform EETT of any subsequent amendments to the information held on the registry within seven days of the changes if they cease their activities, and must submit to the authority annual reports describing their activities. The EETT, may either on his own initiative or following a complaint, examine the CSPs' compliance with the provisions of the Presidential Decree and Regulation 248/71. To this end, EETT itself or other bodies designated by it may proceed to audit controls at the location in which CSP is formally established or from which it operates its business (Art. 12 of the Regulation).

CSPs aiming for a higher level of trust and quality may apply for a voluntary accreditation. The accreditation is an option, not an obligation for CSPs (Art. 4.5 Presidential Decree). The criteria, prerequisites, procedure, and standards of the voluntary accreditation scheme are established in Regulation No. 295/65 "on the Voluntary Accreditation of Certification Service Providers".[24] The Greek system does not encourage accreditation, since it does not grant privileges to the certificates of accredited CSPs. The consequences of the electronic signature legislation regarding supervision, formal requirements and liability do not depend on accreditation but on the existence of "qualified" electronic signatures.

Liability provisions

Liability issues are stated in Art. 6 Presidential Decree, which is related to a "reserved burden of proof" to the detriment of negligent CSPs: a CSP, accredited or not, issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public, is liable for damage caused in specified circumstances to any entity or legal or natural person who reasonably relies on that certificate unless the provider proves that they have not acted negligently. The liability causes of Art. 6.1 of the EU Electronic Signature Directive are literally copied in a respective Art. 6.1 Presidential Decree.[25] The same liability applies where the CSP fails to register revocation of the certificate. The liability of the signatory and that of the party relying on the signature is not regulated in the

[21] *Kalliope Makridou in Konstandinos Kerameus, Dionysios Kondylis and Nikolaos Nikas, Commentary on the Code of Civil Procedure (in Greek), (2000 Sakkoulas), Article 270 no. 6.*

[22] *Areios Pagos (plenary session) 15/2003, Helliniki Dikaiosini 2003, 937; See also Areios Pagos 1628/2003, Helliniki Dikaiosini 2004, 724, concerning the probative effect of an e-mail.*

[23] *Article 340 of the Civil Procedure Code provides as follows: "Unless otherwise explicitly provided, the judge evaluates the means of proof freely and decides in accordance with his inner conviction whether the factual allegations are true. The judgment must include the reasons which led the judge to the formation of his conviction".*

[24] *EETT also decided the adoption and implementation of the Electronically Signed List solution for supporting the National Voluntary Accreditation scheme.*

[25] *The Presidential Decree specifies that a certification service provider is liable for damage caused to any person who reasonably relies on the certificate data, unless he proves that he has not acted negligently. The service provider is liable for the accuracy of all information in the qualified certificate at the time of issuance, for assurance that at the time of issuance of the certificate, the person identified in the qualified certificate held the signature creation data corresponding to the signature verification data given or identified in the certificate and that these two data function correctly together.*

Presidential Decree. In addition, this liability does not depend on accreditation and is not extended to all electronic signatures. The applicability of Art. 6 Presidential Decree is restricted to a CSP issuing or guaranteeing qualified certificates to the public. The liability for "non-qualified" certificates is also left to the existing national law. What is decisive, is the designation of the certificate as "qualified" by the CSP itself. Whether the defective certificate is actually qualified or unqualified is irrelevant. It is also noteworthy that if a CSP issuing qualified certificates proceeds to assign part of the certificate issuing procedure to a third party, it shall remain exclusively liable for actions or omissions on the part of the above contractor.[26]

Any party having reasonably relied on a certificate issued by a negligent CSP may benefit from the provisions of Art. 6 Presidential Decree. However, it is not clear from the wording of the Article if the signatory is a relying party in the meaning of this provision.[27] The prevailing opinion in Greek legal theory considers a signatory can also benefit from this provision. Since the signatory enters into a contract with the CSP regarding the issuance of a certificate, it could be argued that the liability of the CSP to the signatory is governed by the terms of the contact between the CSP and the person obtaining a signature, and that the liability provisions of the Presidential Decree do not apply to the signatory. In any case, it is not easily conceivable that the signatory would rely on a certificate issued for the purpose of identifying them, and even if a person does so, it will be more than questionable, if the signatory can be said to have reasonably relied on the respective certificate.

The Greek electronic signature legislation appears to adopt an inconsistent approach regarding the regulation of liability. The provisions of Regulation 248/71 demands the CSP to meet numerous requirements, but infringement of many of those requirements is not stipulated in Art. 6 of the Presidential Decree as liability cause. Given that broadening the list of the grounds for liability is authorised by the EU Electronic Signature Directive, the scope of the provisions relating to liability should, perhaps, have been extended to cover cases of infringement of the requirements as set out in the Presidential Decree and Regulation 248/71, and any failure of the products used by the CSPs for qualified electronic signatures or other technical security facilities. In order to deal with this problem, and taking into account the provisions of Art. 6.6 of the Presidential Decree explicitly states that Law 2251/1994 on consumer protection also applies to electronic signatures, the liability of the CSPs could be broadened by classifying them as service providers according to Law 2251/1994. With specific regard to consumers, Art. 8 of Law 2251/1994 stipulates that the service provider shall be liable for any damage caused by its fault (any damage resulting from wilful misconduct or negligence), in the course of the provision of services. Limitation or exoneration clauses are invalid. The law includes a broad definition of the term consumer.

International aspects

Art. 5 of the Presidential Decree provides for the recognition of foreign qualified certificates and products for electronic signatures. According to Art. 5.2 of the Presidential Decree, certification services by a CSP established in an EU member state are recognised as legally equivalent to the corresponding certification services provided by a CSP established in Greece. This means that electronic signatures that are based on qualified certificates of member states of the EU that comply with the provisions of Art. 5.1 of the EU Electronic Signature Directive are recognized as legally equivalent with "qualified" electronic signatures in the sense of the Presidential Decree. It is noteworthy that the Presidential Decree regulates the recognition of certification services in general, and not only the recognition of the legal equivalence of qualified certificates. An interpretation of Article 5.2 of the Presidential Decree that extends the certification services by including registration services, time-stamping services, directory services and such like seems reasonable and in line with the principle already expressed by the European legislator in Recital 9 of the EU Electronic Signature Directive, which reads:

(9) Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time stamping services, directory services, computing services or consultancy

[26] *Art. 11.5 of the Regulation.*

[27] *See Konstandinos Christodoulou, Electronic documents and electronic contracts (in Greek), (2001 Ant. N. Sakkoulas Publishers), 150; Dimitrios Maniotis, The electronic formation of contracts and the liability of third parties responsible for the authentication of the electronic document, 75.*

services related to electronic signatures.

In addition, products for electronic signatures that comply with the provisions of the EU Electronic Signature Directive are equivalent to those originating in Greece in terms of their legal effects. Once the conformity of secure signature-creation-devices with the requirements set out in the EU Electronic Signature Directive are recognised by a public or private body entrusted with this role according to the legislation of an EU member state, this recognition has direct legal effects in Greece (Art. 5.3 Presidential Decree).

Qualified certificates issued to the public by a CSP established in a third country outside the EU are deemed to be legally equivalent to those offered by a CSP established in the EU under the following conditions: (a) the CSP fulfils the requirements laid down in the Presidential Decree and has been accredited under a voluntary accreditation scheme established in a Member State; (b) a CSP established within the Community which fulfils the requirements laid down in the Presidential Decree guarantees the certificate; (c) the certificate or the CSP is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations. Although the EU Electronic Signature Directive requires that one of these three conditions be met, it is not clear in the Presidential Decree if these conditions have to be met cumulatively or alternatively.

Concluding remarks

Since the Presidential Decree literally copies most of the provisions set out in the EU Electronic Signature Directive, the Greek e-signature law is in conformity with the essential requirements of the Directive. The European framework has assisted the Greek legislator in regulating the key issues of concern, however many challenges have not been taken into consideration. For example, although the provision of time-stamping falls under the general category of the provision of certification services as specified in the EU Electronic Signature Directive, there are no statutory requirements with regard to time stamping in the Greek legislation. As far as the liability system is concerned, Art. 6 of the EU Electronic Signature Directive begins with setting out the minimum standard of liability that Member States have to comply with when implementing the Directive. This means that the Greek legislator had the opportunity to build a broader national liability system on the basis given by the EU Electronic Signature Directive. However, the legislator decided not to introduce a higher standard than suggested by the Directive, probably because it would put CSPs situated in Greece at a competitive disadvantage.

The use of qualified electronic signatures is not currently common, although the legislative framework is in place. There are five registered CSPs in Greece and only two of them have indicated that they issue qualified certificates. None of the CSPs have been accredited yet. The reason why the wide-spread adoption of "qualified" electronic signatures remains limited is because there is no real need for them in the national market. Given the small number of the formal legal acts in the Greek law and the fact that both jurisprudence and legal doctrine regrettably regard non-qualified signed e-mails as equal to private documents shifting additionally the burden of proof of the authenticity to the sender-defendant, many people obviously do not see the need to invest in the unnecessary costs and complexity of "qualified" electronic signatures.

Dr. Komninos Komnios, LL.M is a lawyer and mediator in Greece. He received his doctorate on the Law of electronic Signatures at the Institute of Law and Informatics in Saarbrücken, Germany as a scholarship-holder of the German Academic Exchange Service (DAAD) and of the "Alexandros S. Onassis" Foundation. He specialises in Civil law, Civil Procedural law and IT law.

k.komnios@mail.jura.uni-sb.de