"Digital Signature Legality in Different Jurisdictions: Legally Binding Issues"

Nikolaos A. Karanikolas

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES

A thesis submitted for the degree of

Master of Laws (LLM) in Transnational and European Commercial Law, Mediation, Arbitration and Energy Law

February 2019

Thessaloniki – Greece

Student Name: Nikolaos Karanikolas

SID: 1104160017

Supervisor: Prof. Komninos Komnios

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

February 2019

Thessaloniki - Greece

Abstract

Digital signature is a legally valid way to sign documents in the digital environment. In Europe, the need to establish a secure electronic communications framework has been repeatedly demonstrated. It was in 2014 that Parliament and the European Council approved the new rules on national electronic identification systems (eIDAS), which allow access to public services available in other EU countries. To achieve European coherence, it will undoubtedly have to go through the establishment of a European policy of harmonious control with other economic powers such as the USA. Also, there are some privacy and security concerns associated with the wide spread adoption of digital signature evolving towards the use of biometric identification method at advanced level. They need attention in creation of certification body for future technologies. A single Certification Body of universal scope is not viable, therefore there must be one or several networks of national or sectorial authorities, interrelated and that in turn provide service to the users of their respective fields. This research work has tried to give an idea of the important changes that the firm has experienced from its origins to our days and how they should try to adapt these changes to the social reality and leave the door open to other future changes and new technologies that will undoubtedly come.

Keywords: Digital Signature, Digital Certificate, eIDAS Regulation, Trusted Third Party, Biometric Signature

Student Name: Nikolaos A. Karanikolas

Date: 10/2/2019

Preface

The selection of the theme of "Digital Signature" was held for two main reasons. First of all, my personal engagement and involvement in eGovernment issues, in my 20-year term of office in the civil service (and for the longest time as Head of Departments), has enabled me to observe closely the repeated attempts to implement the measure of Digital Signature, by acquiring personal recruits for the administrative, technological and legal implications of this innovation. In addition, my recent engagement at the key position of the “City of Athens” Data Protection Officer (DPO) led me to the intensive study of literature related to "Legal Informatics", a relevant new branch of law and administrative science, in the field of which the concept and the function of digital signatures is quite much related. The criterion for selecting the individual thematic units to be analyzed in this paper was the need to highlight the points for which the legal scientist is required to have an understanding of technological developments without however the development of such capacities being linked to cumulation but with a deeper understanding of technological innovations and applications that affect either the legal science itself or our perception of law in general.

Acknowledgement

Foremost, I would like to express my sincere gratitude to my supervisor, Prof. Komnino Komnio, a regular professor of the School of Economics, Business Administration & Legal Studies of the International Hellenic University, for his academic support and guidance, and immense knowledge, but also for his spiritual inspiration and motivation. His contribution has been catalytic, and I feel really honored that he accepted to supervise my work. I could not have a better mentor.

Besides my supervisor, I would like to extent my gratitude to the other two members of my dissertation committee, Prof. Ioanni Inglezaki from Aristotle University of Thessaloniki and Prof. Riga Giovannopoulo from Aristotle University of Thessaloniki, for providing me feedback with very helpful and valuable comments and suggestions.

My sincere thanks also go to Rafaella D. Tsertsides, scientific assistant at the International Hellenic University, for her encouragement and insightful comments, throughout my LLM studies at IHU.

Contents

Summary

There are 3 types of signatures that can be established such as simple/ basic, advanced/electronic and qualified or recognized electronic signatures. From contracts to e-mails, everything that is electronically signed with this certificate becomes legal. This allows for sales contracts to be closed in minutes or in hours, as there is no longer any need to move further. In Europe, the need to establish a secure electronic communications framework has been repeatedly demonstrated. The encryption methods and certificates used for the electronic signature are not valid for eternity. On the other hand, the period expires at some point, within which the certificates can be checked, confirming the affiliation of a signature to a person. US regulations recognize two types of digital signature, and the difference between them does not lie in the technological, but, rather, in the legal terms. The digital signature, defined as the result of applying a mathematical procedure to a digital document, requires information of the signer's exclusive knowledge, and is under his absolute control. The features: electronic signature, digital signature, electronic certificate and digital signature share are security, convenience and ease to carry out transactions, transactions and transactions online without costs and quickly and easily. Electronic documents are pure information, converted from an analogue source or even created directly into electronic media, that is, they are mathematically encoded and decoded by computer equipment. Both can be written to a data storage medium and exist temporarily in a processing and transmission media. In United Kingdom, there is a lively debate on the possible regulation of Trusted Third Parties. There is a bill on digital signature and Trusted Third Parties for all the major countries. What the European Commission intends is to find a common legal recognition in Europe of the digital signature, in order to harmonize the different legislations. Although at first glance the biometric signature and the digital signature seem similar concepts and are considered by many to be synonymous, the truth is that they are totally different concepts and that it is very important to differentiate. The main concern of users who use biometrics is the security with which that information is stored, because there will have to be a database with the digitized information, in this way the system will be able to compare it every time. There are some privacy and security concerns associated with the wide

spread adoption of digital signature evolving towards the use of biometric identification method at advanced level. They need attention in creation of certification body for future technologies.

Introduction

Digital signature is a legally valid way to sign documents in the digital environment. From a digital certificate, which proves the authorship of the signature and the identity of the signatory, it is possible to validate any document, such as the authentication done in a notary. The mechanism uses encryption, creating a unique fingerprint for each signer. In this way, the digital signature confers security to the documents that process in the virtual environment, guaranteeing the authenticity, the integrity and the non-repudiation - negative of the authorship. This powerful tool has streamlined the routine of companies and offices that handle document management, reducing costs and time of operation. Proposals, contracts, power of attorney and invoices can be signed at any time and from anywhere. Provided there is access to the internet and an electronic device, such as a computer, tablet or cell phone. In general, the certificate is the identity of a person in the digital environment. It must be purchased from a certifying authority from where, a person can sign documents without being physically present, eliminating time, displacement and bureaucracy.

Digital signatures are legally binding for almost every business or personal transaction across the globe. This dissertation aims at exploring the idea of digital signature and studying dynamics associated with it. Furthermore, legal implications associated with the adoption of digital signature at global scale in terms of legislations passed across the world are subjected to evaluation.

The concept of the “signature” into a legal context

In the European Union, in 1999 it was established, through Directive 1999/93 / EC[1], the legal framework for the use and development of the electronic signature. Directive 1999/93 / EC of the European Parliament and of the Council of 13 December

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093 is no longer in force, Date of end of validity: 30/06/2016.

1999 establishing a common framework for electronic signatures defines new concepts: the electronic signature, the data in electronic form attached to other electronic data or associated in a logical way with them, used as a means of authentication[2].

Legal effects of the electronic signature

There are 3 types of signature that can be established such as simple/ basic, advanced electronic and qualified or recognized electronic signature[3].

- *Simple or basic electronic signature*: Data that can be used to identify the signer (authenticity). "The data in electronic form attached to other electronic data or associated in a logical manner with them, used as a means of authentication".

- *Advanced electronic signature*: the one that
  a) is linked to the signer in a unique way,
  b) allows the identification of the signer,
  (c) is created using means that the signer can keep under his control, and
  d) is linked to the data that is refers so that any subsequent change in them is detectable.

- *Qualified or recognized electronic signature*: that "advanced electronic signature" that is based on a qualified certificate and that has been created by a "Secure signature creation device" as defined by the directive. This last type of signature satisfies the legal requirement of signatures in relation to data in electronic form in the same way that a handwritten signature satisfies these requirements in relation

[2] See also Abbott, K. W., Keohane, R. O., Moravcsik, A., Slaughter, A. M., & Snidal, D. (2000). The concept of legalization. International organization, 54(3), (pp. 401-419),
and Chen, J. J. C., & Chia, L. (2014). Authentication of unknown parties in secure computer communications , U.S. Patent No. 8,667,154. Washington, DC: U.S. Patent and Trademark Office.
[3] See Chernyi, S. G., Ali, A. A., Veselkov, V. V., Titov, I. L., & Budnik, V. Y. (2018, January). Security of electronic digital signature in maritime industry. In Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018 IEEE Conference of Russian (pp. 29-32). IEEE.

to paper data. In addition, an electronic signature cannot be rejected by the mere fact that: it is presented electronically; do not rely on a recognized certificate; do not rely on a certificate issued by an accredited certification service provider; is not created by a secure signature creation device[4].

Current initiatives with respect to digital signature

The digital signature is a technological tool that guarantees the authorship, integrity and non-repudiation of digital documents. These files are thus given three fundamental characteristics that until now only paper documents have enjoyed.

The digital signature is not only technology, although it plays a fundamental role in this system. It is technology and law, because in this mechanism technical elements and normative elements are interwoven. It has been said that the digital signature is an instrument with technical and training characteristics, which means that there are technical procedures that allow the creation and verification of digital signatures, and there are normative documents that support the legal value that these signatures have legal value and the importance of the normative elements is highlighted in the types of digital signature recognized by different company laws[5].

US regulations recognize two types of digital signature, and the difference between them does not lie in the technological, but, rather, in the legal:

- The digital signature, defined as the result of applying a mathematical procedure to a digital document, requires information of the signer's exclusive knowledge, and is under his absolute control. But, since the same law stipulates that in order to ensure that the signer is the only one who knows and controls the mathematical

[4] See Chen, J. J. C., & Chia, L. (2014). Authentication of unknown parties in secure computer communications ,U.S. Patent No. 8,667,154. Washington, DC: U.S. Patent and Trademark Office, (pp 5-8).
[5] See Saxena, N., Kumar, D., & Pandey, A. K. (2018). Electronic signature framework with enhanced security, U.S. Patent No. 9,935,777. Washington, DC: U.S. Patent and Trademark Office.

procedure, a series of legal precautions must be complied with; the digital signature can be characterized by means of the following formula:

Digital Signature = digital document + mathematical procedure + legal requirements[6].

- The electronic signature, on the other hand, is defined in negative terms as the set of integrated electronic data, linked or associated in a logical manner to other electronic data, used by the signatory as its means of identification, lacking any of the legal requirements to be considered a digital signature. The formula, in this case, is the following:

  Electronic Signature = digital signature - legal requirements[7].

This difference in terms of requirements influences the effects assigned to each digital signature. They may be equivalent to the handwritten signature or it is presumed that the signature belongs to the holder of the digital certificate, or it is presumed that the document has not been modified after the signature. In case of being unknown, it is the person who invokes it to prove validity of Electronic signature. The range of application possibilities of the digital signature is very varied, as varied as the application of the handwritten signature[8].

[6] See Smejkal, V., Kodl, J., Novák, D., & Schneider, J. (2015). Strong Identification and Authentication Using Dynamic Biometric Signature. In Computer Science and its Applications, Springer, Berlin, Heidelberg, (pp.1-10).
[7] Ibid (pp 1-5)
[8] See Peterson, D. G., Rybacki, D. P., & Wald, D. E. (2018). System and method for rules-based control of custody of electronic signature transactions, U.S. Patent No. 9,893,895. Washington, DC: U.S. Patent and Trademark Office, (p.3).

Chapter 1 – "Legal Recognition of Digital Signature"

The digital signature as an alternative for the handwritten signature

From the technical point of view, electronic and / or digital signatures are offered as an alternative to the handwritten signature on paper. In electronic commerce, the classic paper document is replaced by the new electronic document. Correlatively, the traditional handwritten signatures disappear, which can be replaced using a variety of methods that are included in the broad concept of electronic signature, within which the digital signature has a place as a particular category.

Digital signatures based on asymmetric cryptography can be framed in a more general concept of electronic signature, which does not necessarily presuppose the use of asymmetric encryption technologies. Although, several authors speak indistinctly of electronic signature or digital signature, it has the same tasks as the handwritten signature, but expresses, in addition to identity and authorship, authentication, integrity, date, time and reception, using asymmetric public key cryptographic methods electronic sealing techniques and hash functions, which means that the signature is based on the document that is subscribed (it is not constant), but which makes it absolutely inimitable as it does not have the private key with which it is encrypted, true attribution of identity and authorship.[9]

For Poullet (2018), the electronic signature supposes a series of characteristics added at the end of a document. It is elaborated according to cryptographic procedures, and it carries an encoded summary of the message, and of the identity of the sender and receiver[10].

[9] See Zank, A. E., & Stevens, D. R. (2001). Electronic signature management system, U.S. Patent No. 6,307,955. Washington, DC: U.S. Patent and Trademark Office, (pp. 5-10)
and Handley, M. (2018). Schnorr's Digital Signature and its Applications. Review of Computational Science and Engineering, 4(1), 47, (pp. 1-8).

[10] See Poullet, Y. (2018). Law Facing Information and Communication Technology (ICT)—Conflict or Alliance? In Progress in Science, Progress in Society, Springer, Cham, (pp. 91-108).

For some authors, it is a digital signal represented by a string of bits that is characterized by being secret, easy to reproduce and recognize. It is easy to reproduce and recognize, difficult to falsify and changing depending on the message and depending on time, whose use requires the appearance of what it calls electronic or telematic notary that will be able to verify the authenticity of documents circulating through of communication lines, having not only computer training, but also legal training[11].

The article 2.1 of the proposed Digital Signature Directive, defines the electronic signature as that signature in digital form placed on some data, or added or logically associated to them, and used by the signatory to indicate the approval by the signatory of the content of these data and fulfilling certain requirements[12].

Overview of concepts and terminology

Digital signature is a technology that enables the matching of digital documents with paper documents and, therefore, the realization, via digital, of fully valid legal acts[13]. Basically, the digital signature fulfills three functions:

- *Authentication*: guarantees the identity of the signer of the document, that is, that the document has been signed by the person who claims to have signed it.
- *Integrity*: ensures the integrity of the message, that is, that the information contained in the digital document has not been modified after its signature.
- *Non-repudiation*: guarantees that the signer cannot deny the content of the document or the veracity of the signature.

It is very important to bear in mind that this type of signature does not imply endorsement of the confidentiality of the message. The information contained in the

[11] See Peterson et al (2018).
[12] See Poullet, Y., & Rouvroy, A. (2007). General introductory report, in *Ethical Aspects on the Information Society,* Conference organized Jointly By UNESCO and Council of Europe, Strasburg, (text available on the UNESCO website).
[13] Handley, M. (2018). Schnorr's Digital Signature and its Applications. Review of Computational Science and Engineering, 4(1), (p. 47).

document thus signed can only be read by certain persons. In this way, a digitally signed digital document can be viewed by third parties. There are other cryptographic tools through which you can ensure the confidentiality of messages sent digitally, but this is not the case of the digital signature.

Digital signatures must allow the identification of the signatory. People enter into the concept of "electronic authorship" as the way to determine that a person is who they say they are. It can only be generated by the issuer of the document, unforgeable and inimitable. The information generated from the electronic signature must be sufficient to validate it, but insufficient to falsify it. The possible intervention of the Electronic Notary improves the security of the system. The opposition of a signature must be significant and is linked indissociably to the document to which it refers. There should be no delay of time or place between acceptance by the signatory and the opposition of the signature. Article 2.1 of the proposed Electronic Signature Directive, in addition to defining the concept of electronic signature, indicates that the following requirements must be met: is linked only to the signatory, is able to identify the signer and is created in a way or using a medium that is solely under the control of the signer. It is linked to the data to which it refers in such a way that if the data is altered the electronic signature is invalidated[14].

The electronic or digital signatures basically consist of the application of encryption algorithms to the data, in this way, they will only be recognizable by the addressee, who will also be able to verify the identity of the sender, the integrity of the document, the authorship and authentication, preserving at the same time confidentiality. The security of the algorithm is directly related to its type, size, encryption time and non-violation of the secret[15].

The cryptosystems of public key, are the most suitable as a digital signature, are based on the use of a pair of associated keys: a private key, which is kept secret, and a public key, freely accessible by anyone. This pair of keys is mathematically related in

[14] See Skiles, D. (2012). Digital Signature Technology. Technology Tools for Today's High-Margin Practice: How Client-Centered Financial Advisors Can Cut Paperwork, Overhead, and Wasted Hours, (pp. 6-9).
[15] See Pilkington, M. (2016). 11 Blockchain technology: principles and applications. Research handbook on digital transformations, 225.

such a way that only the public key corresponding to the private key used to sign can verify the signed message; also, technically they are very resistant, it is calculated in thousands of centuries the average duration that it would take the most powerful computer to be able to break the key. Its security mechanism is based above all on the absolute secrecy of private keys, both when generated and when saving and in the certification of the public key by the certifying authority. Among the objectives of the electronic signature is to achieve a universalization of an electronic signature standard.[16]

Electronic signature versus digital signature

Although it is likely that you have used them as synonyms or believe that their meanings and utilities are identical, we review the differences between the digital signature and the electronic signature. If previously, all bureaucratic and administrative processes were done on paper, nowadays the digital universe offers us alternatives to present all kinds of documentation, prepare our invoices in electronic format or render accounts with the Treasury without the need to print a single sheet[17].

With the appearance of new modalities to certify our identity in the network, new terms arise that we tend to confuse, such as those of electronic certificate, electronic signature and digital signature. These are often used as synonyms and interchangeably, although their uses are different. Therefore, we need to define these concepts and to unfold their main applications and utilities[18].

The feature Electronic signature, digital signature, electronic certificate and digital signature share is security, convenience and ease to carry out transactions online without costs, quickly and easily.

[16] See Kim et al, (2015:10)
[17] McCabe, A. D., & Gosner, T. H. (2014). Systems and methods for distributed electronic signature documents, U.S. Patent No. 8,655,961. Washington, DC: U.S. Patent and Trademark Office, (p.5).
[18] See Beenau, B. W., Bonalle, D. S., Fields, S. W., Gray, W. J., Larkin, C., Montgomery, J. L., & Saunders, P. D. (2008). Method and system for proffering multiple biometrics for use with an FOB, U.S. Patent No. 7,360,689. Washington, DC: U.S. Patent and Trademark Office.

Electronic signature: This is the "set of data in electronic form, consigned together with others or associated with them, which can be used as means of identification of the signer", according to Law. This is therefore a legal concept and an identification method, equivalent or analogous to the handwritten signature, which uses different electronic media, such as an electronic pen or a digital signature. Making an electronic signature means that a natural person verifies an action or procedure through an electronic means, leaving a record of the date and time of the same. This concept is more generic, broad and undefined from the electronic point of view than the digital signature[19].

Digital signature: The set of characters that are added to the end of a document or body of a message to inform, attest or show validity and security. The digital signature serves to identify the person issuing the message and to certify the veracity that the document has not been modified with respect to the original. One cannot deny having signed it, since this signature implies the existence of an official certificate issued by an organization or institution that validates the signature and identity of the person who performs it. The digital signature is based on public key cryptography (PKI) systems that meet the requirements of advanced electronic signature definition[20].

Electronic or digital certificate: This document or computer file is the one that a natural or legal person uses to identify itself in the network, authenticated by a third party or certifying authority and the automatic application of a mathematical algorithm that associates the identity to the message or document[21].

Digitized signature: Although many people confuse it with the digital signature, it has nothing to do with it. This term refers to the simple graphic representation of the handwritten signature obtained through a scanner, which can be inserted into any document, such as an email and that was popularized by marketing experts. For example,

[19] See Bresciani, P., Donzelli, P., & Forte, A. (2003, May). Requirements engineering for knowledge management in eGovernment. In IFIP International Working Conference on Knowledge Management in Electronic Government, Springer, Berlin, Heidelberg, (pp. 48-59).
[20] Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In Post-quantum cryptography, Springer, Berlin, Heidelberg. (pp. 1-14).
[21] Ginter, K. L., Shear, V. H., Spahn, F. J., Van Wie, D. M., & Weber, R. P. (2006). Digital certificate support system, methods and techniques for secure electronic commerce transaction and rights management, U.S. Patent No. 7,133,846. Washington, DC: U.S. Patent and Trademark Office, (p. 6)

the Facebook Messenger bot allows you to have a professional signature. However, for practical purposes, the signature that we use mostly for the completion of numerous procedures both before the Tax Agencies and before other Public Administration Services. is the digital signature, also used internally by companies and in the electronic mail insurance[22].

The answer to whether electronic signature is the same as the digital signature lies in consonance with the definitions provided, is no. While the electronic signature is a generic and much broader expression of electronic data, it does not necessarily have legal validity. An example is the creation of a PDF signed by its author, which identifies it but without legal validity or authentication security. On the other hand, the digital signature is the certified electronic signature based on the aforementioned public key-based cryptography (PKI), thus complying with the rules of advanced electronic signature. In this way, the digital signature is the one that has validity legal, avoids identity theft and allows authentication and identification in all kinds of administrative, bureaucratic or fiscal processes, among others[23].

Main practical usages of digital signature

Digital certificates start to be an extended tool in the business world. Almost all companies have digital certificates, although the majority of owners are not aware of their potential use. Without going into the technical details, a digital certificate is a software component that contains information that identifies us. Submitting a digital certificate in a remote digital transaction is like presenting your ID at a counter. The question is, why should the other party trust that these data are real? This is where trust in the issuer of the certificate comes into play. Therefore, to obtain our digital certificate, we have had to

[22] Mukherjee, D., Godara, S., Das, A. K., Dey, S., Kumar, S., Islam, R., ... & Mukherjee, C. (2017, October). Unique digitized activity signature for human authentication. In Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2017 8th IEEE Annual (pp. 714-720). IEEE.

[23] See Martinez-Diaz, M., Fierrez, J., & Ortega-Garcia, J. (2009). Dynamic signature verification using portable devices, Spied Newsroom. 10.1117/2.1200905.1600.

move to a registration office, and present the documents that accredit our identity and powers. This registry office is managed by the issuer of the certificate (it is known as a Certification Services Provider), which must be an entity recognized by the public administration authorities[24].

The digital signature, uses and possibilities

It has been more than twenty years since the State of Utah in the United States was the first place in the world to recognize the legal validity of the digital signature. In Spain, following a decree law of September 1999, this technology has progressively become known and there were a number of companies that offered related products and services. Throughout these years the digital signature has had an impact on society, but what has changed and what will be its evolution?

Unlike other technologies, which eventually are limited to specific sectors of society, the digital signature is of general interest by definition, since it is quite possible that within the next years, we all have a digital ID or e-DNI. For this reason, the most popular media have published news and articles on the subject in recent years. Therefore, it is not necessary to go deeper into the general data of this technology, as they are undoubtedly well known. Although it may be of great interest to take stock of the impact of the digital signature on our society to date, in search of the keys that reveal the role that can play in the near future, which can be advanced and will be very important[25].

The first wish of many citizens who have heard of the digital signature is to have one. There are numerous websites that offer them for free or for a small fee in Kriptochip card format, such as a Credit or a Debit Card. The question is where to use it, how and for what purpose. Probably there is no other example of application of the digital signature in which the advantages and the method are as clear as that of the realization of the

[24] See Mana, A., & Matamoros, S. (2002, September). Practical Mobile Digital Signatures. In International Conference on Electronic Commerce and Web Technologies, Springer, Berlin, Heidelberg. (pp. 224-233).
[25] Abidi, A., Bouallegue, B., &Kahri, F. (2014, June). Implementation of elliptic curve digital signature algorithm (ECDSA). In Computer & Information Technology (GSCIT), 2014 Global Summit on IEEE. (pp. 2-5).

declaration of income over the Internet. In this case, the taxpayer sees the need to obtain a digital certificate to make his declaration online and, in return, obtains the advantage of being able to enjoy, if applicable, the rapid return of the tax documents[26].

In other applications of the digital signature it is not so easy to find the advantages for the user, so it is difficult to instruct him to use it. This is the case of the SET payment system promoted by VISA, which facilitates the non-contact identification of the consumer with a digital certificate. It can hardly be accepted by him while he can access without any disadvantage other simpler payment options, which are perfectly valid and of extended use, such as virtual purchase with a credit or debit card. In comparison with the previous case of online income, it is as if the Tax Authorities did not reward who bothers to obtain a certificate and enter all the data of the declaration on the Web, returning their money in the same period as whoever the made-on paper. One of the most widespread myths is that the digital signature is safer to make on-line payments, which is true for the selling party that can thus perfectly identify the buyer. However, the latter does not obtain any direct benefit, while using the classic on-line card saves the procedures for issuing the digital certificate. In addition, in any case, you always have the option to cancel those charges against your account that are fraudulent[27].

In this way, it is concluded that, in general, consumers are not the main beneficiaries in the digital signature applications, so researchers will have to find a way to share this benefit or suppress other options, such as the case of the eID[28] or the digital medical prescription, which in the future promotes the Public Administration. Companies can have it a little more difficult if they do not make a common front to encourage the use

[26] See Pilkington, M. (2016). 11 Blockchain technology: principles and applications, in "Research handbook on digital transformations", edited by F. Xavier Olleros and Majlinda Zhegu, Associate Professors of Innovation Management, École des Sciences de la Gestion, Université du Québec à Montréal, Canada, (p. 225).
[27] See Wu, C. C., Hsu, C. W., & Cheng, R. S. (2018, April). The digital signature technology for access control system of mobile. In 2018 IEEE International Conference on Applied System Invention (ICASI) (pp. 896-898). IEEE.
[28] The CEF eID building block is a set of services (including software, documentation, training and support) provided by the European Commission and endorsed by the Member States, which helps public administrations and private service providers to extend the use of their online services to citizens from other European countries. This is realized through the mutual recognition of national electronic identification (eID) schemes (including smartcards, mobile and log-in), allowing citizens of one European country to use their national eIDAS to securely access online services provided in other European countries. See https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+eID

of payment systems based on electronic certificates. In most cases, the digital certificates of companies are used to identify themselves in front of web applications, and mainly in procedures and queries in a tax agency website, or the notification mailbox. However, a digital certificate also has other applications.

Technical Issues

If digital signatures are to replace the signature by hand everywhere, they must also meet the requirements of a proof. Digital signatures are not built for eternity. Qualified signatures are available and testable at non-accredited certification service providers for just five years, and accredited ones are at least 30 years old. However, documents relating to a person's legal status may have to be kept for a lifetime - rights to a property or building, or even more than a century. Doctors and hospitals as well as lawyers have a documentation obligation. In case of dispute, they therefore have the burden of proof.[29]

In general, there are three problems with long-term archiving: On the one hand, the document owner must keep track of the security suitability of the digital signature. As the computer technology progresses, the cryptographic techniques underlying the signature lose security. The signatures must therefore be repeatedly "sealed" with better algorithms[30].

The encryption methods and certificates used for the electronic signature are not valid for eternity. On the other hand, the period expires at some point, within which the certificates can be checked, confirming the affiliation of a signature to a person. Therefore, in order to verify the authenticity of the document, the owner must obtain the verification data from the respective certification bodies in good time before the expiration of these deadlines in order to check the validity of the certificate data from the root, issuer and user certificate. If it is foreseeable that its validity period is about to expire, the owner

[29] See Chamberlin, C. R., & Reck, B. A. (2016). Apparatus and methods for the secure transfer of electronic data, U.S. Patent No. 9,252,955. Washington, DC: U.S. Patent and Trademark Office. (pp. 2-9)
[30] ibid

of the documents must also re-sign them. Finally, he has yet to prove that the document has never been protected by an inappropriate crypto procedure, so it is guaranteed to have been preserved unchanged. For individuals with few documents such an effort is still manageable by hand. In contrast, professional institutions would hardly be able to cope without an automated procedure[31].

The need for a secure information transmission framework

The need for a secure framework for the transmission of information was first revealed in the USA, specifically in UTAH in 1996. The success of this initiative led to its incorporation into the US Commercial Code (Uniform Commercial Code), which established the foundations so that commercial relations could be developed in this framework. In 1997, on the initiative of UNCITRAL, the Model Law on Electronic Commerce was approved, which has served as the basis for regulatory development in this area [32].

In Europe, the need to establish a secure electronic communications framework has been repeatedly demonstrated. The Lisbon Summit of Heads of State and Government of March 2002, considered that the harmonization of the regulatory legal framework of electronic commerce and security in it, was a fundamental pillar for the construction of the economy of the European Union. The process begins in a stable manner with the approval of Directive 1999/93 of the European Parliament and of the Council, which establishes a Community legal framework for electronic signature.

Before analyzing the most technical aspects of the operation of the electronic signature, it is convenient to clarify some basic points of what is meant by security in telematic communications. There are four main normative blocks:

[31] See Bisbee, S. F., Carpolette, B. K., & Moskowitz, J. J. (2010). "System and method for electronic transmission, storage, retrieval and remote signing of authenticated electronic original documents", U.S. Patent No. 8,924,302. Washington, DC: U.S. Patent and Trademark Office.

[32] See Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), (pp. 638-646).

- *Technical Security*, that allows to obtain private, authentic and complete Inter-parties communications and that guarantees that the sites are safe from hackers.
- *Legal Security*, understood as such, a regulatory legal framework for possible responsibilities that may arise from unlawful conduct or acts through the network.
- *Commercial or economic security* can be the application of the previous concept to ensure a secure framework for financial transactions through the network.
- *Security for consumers*, avoiding the abuse of large companies in their dominant position and the use of abusive clauses.

The operation of the electronic/ digital signature

The fundamental problem posed by transactions through the Internet, from a legal point of view can be summarized in four major points, which have been highlighted by numerous experts in the field: *authenticity; integrity; confidentiality and non-repudiation*.

Integrity refers to the fact that the information cannot be manipulated in the sending process. The authenticity means that the information is sent by who appears as issuer and received by the one to whom it is addressed, confidentiality ensures the secrecy of the communications contained in the messages. Finally, the non-repudiation (do not reject), comes to ensure that the authorship of the message sent cannot be denied[33].

To ensure compliance with these four requirements, two major alternatives were proposed:

- Data Encryption Standard (DES) a technique that was developed by IBM, but which failed due to its insecurity regarding secrecy and confidentiality of said key. However, this system has been the most historically used.
- Asymmetric cryptography system, which requires the interlocutors to use the same key to encrypt and decrypt the message. Practical experience has been

[33] Ford, W., & Baum, M. S. (2000). Secure electronic commerce: building the infrastructure for digital signatures and encryption. Prentice Hall PTR, (p.5).

responsible for highlighting the shortcomings of these systems for the transmission of high security information[34].

Legal Issues

During the evolution of societies, law appears as a set of rules for the purpose of establishing methods for the resolution of conflicts of interests, as well as disciplining the execution of common interests. And as new technologies are developed and adopted, the ways of contracting are modified as well, and therefore a method is required which allows to certify the validity of the contract and legislation regulating this method. As a partial example of this evolution we have verbal contracts, written contracts, contracts by telegraphs, by the post office, by telephone and, finally, digital contracts[35].

They change the ways of hiring, they change the means to protect the interests and to give security to these legal businesses. Consequently, the importance of protecting contracted obligations increases, since the more developed a society, in terms of technology and organization, the more interdependent the individuals become.

As an explanatory introduction, the term "digital signature" is mistaken, since a signature is the individual written mark of its author; however, the so-called digital signature is a sequence of digits produced by an automated computer system in order to make it possible to verify origin and not to alter, by third parties or even subscribers, the electronic document produced previously. The correct terminology for the so-called "digital signature" would then be an element of the "digital certification" process. However, both types of signatures exist as evidence for the agreement of what was written,

[34] See Boutant, Y., Labelle, D., & Seux, H. (2015). Use of a digital signature obtained from at least one structural characteristic of a material element to protect the direct reading of sensitive data and method for reading this protected data, U.S. Patent No. 8,943,325. Washington, DC: U.S. Patent and Trademark Office.
[35] See Ben-Assuli, O. (2015). Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments. Health Policy, 119(3), (pp. 287-297).

physically or digitally electronically, by virtue of the current legal system, explicitly or by authorization of the judge to use the free convincing when judging evidence[36].

Concept of document

The origin of the word "document" is "documentum", Latin word derived from "docere", whose meaning is "to teach, to demonstrate". Thus, the meaning of document can be understood as "structured register of information for human consumption". In technical-legal language, a document is evidence of a fact and can be demonstrated to the judge, since the fact itself cannot be used. A document may then contain the record of a will agreement and be referred to as a "contractual document", that is, the registration of a will agreement between two or more persons for the purpose of regulating the particular interests which are protected legislation[37].

Traditional document concept

Traditional physical documents can be defined as an outward representation of the fact that one wants to prove. They are recorded on a physical substrate and in an analogical way, that is, they are continuous signals, without abrupt changes (when the signals are amplified, even the apparently discontinuous changes are smooth), they have imperfect reproduction to noise present in the signal) and there is some degree of difficulty to change them without being noticeable, after a more detailed analysis (technical expertise) of the material in which they were produced. Although it is more related to the written and signed document of its own hand, modern legal doctrine accepts that "(...)

[36] Bisbee et al, 2018:2-9

[37] Abu-Hakima, S. (2004), "Concept identification system and method for use in reducing and/or representing text content of an electronic document", U.S. Patent No. 6,823,331. Washington, DC: U.S. Patent and Trademark Office.

holography, the transmission of data (via the internet) are also useful documents to demonstrate the occurrence of facts relevant to the process "[38].

Concept of electronic document

Electronic documents are pure information, converted from an analogue source or even created directly into electronic media, that is, they are mathematically encoded and decoded by computer equipment, and both can be written to a data storage medium and exist temporarily in a processing and transmission media. In short, they are "representations of reality, devoid of physical support, produced and / or stored in electronic equipment" and which need to be converted into physical format compatible with the human senses.

Because they are essentially a numerical sequence, represented electronically by discrete states of information, their most striking characteristics are reproduction and lossless transmission, volatility (since their existence does not depend on a specific physical substrate, but on anything with the capacity to contain numbers) as well as the need to use a properly configured computer for the translation of these electronic signals into signals which may be perceived by humans. These qualities all stand in opposition to the physical existence of a traditional document, facts that cause problems to verify if the electronic document has changed[39].

The Computer as A Place for Formerly Existing Wills Agreement

In this situation, even if each party uses its own computers to transmit their wishes, they will be registered and improved in a system unrelated to both, programmed by a third party, subject to hiring, according to objective criteria that guarantee an equal

[38] Bouchard, T., & Benson, G. (2006), "Electronically verified digital signature and document delivery system and method", U.S. Patent No. 7,082,538. Washington, DC: U.S. Patent and Trademark Office.
[39] Abu-Hakima, (2004:2-9).

protection of the interests counterpoints of the contracting parties, that is, someone not especially interested in the contractual objects which will be made through their equipment. As an example, we have the electronic forums and portals on the Internet for the purchase and sale of fixed price or auctioned goods and services, in which users register and register the goods or services to be provided to others they may be interested in, and in such cases, it is possible to apply the same rules for traditional auctions, together with the rules for distance contracts. One problem that arises from this lack of a direct link between the participants in the contractual relationship is the identification of the persons involved, since the most widely used method, which is the recording of important personal data, is relatively easy to circumvent[40].

It is sufficient for a person with access to a customer registry to use it to impersonate another person, and that some objective criteria for assigning trust (such as the score received from other registered users, which may also have been created with the objective of attacking the system), causing disruptions to those who, in this instance, were victims of identity theft and / or social engineering. Victims in this example include both the person whose data were improperly used and those who were harmed by the ideological falsehood created. Already a system that uses digital certification would not have this evident fragility, as well as safer methods for identifying the person who will be using the digital authentication service, such as the prior and actual verification of their documents and the legitimacy for the use by the bearer, specific security algorithms for the marking of electronic documents, suitable for avoiding the breach of security, would be used by third parties or even by the subscriber himself, after the application of the certificate[41].

[40] Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016, May). Blockchain-the Gateway to Trust-Free Cryptographic Transactions. In ECIS (pp.2-9).
[41] ibid

Chapter 2 – "Country Overview of digital signature law"

European Union

The eIDAs regulation, approved by the European Parliament in 2014, finally entered into force in 2016, thus establishing new laws on electronic signatures, seals and certificates. The rules that form part of EU Regulation No. 910/2014 are valid in the internal electronic interactions of all (still) 28 Member States of the European Union, but also in all transactions of the kind carried out across borders and between countries of the group. Official information provided by the European Commission states that under these new laws "citizens, companies and public entities of the Union can now conduct electronic transactions with each other in a convenient, legal and secure manner". For example, any electronic signature based on such services that are certified will have the same legal and administrative validity as a conventional "left" signature on physical documents. Moreover, this is in transactions internally and between countries, in a common perspective and in a Digital Single Market environment. These Trust Services, based on electronic and digital media, cover signatures, date and time records, stamps, delivery records, certifications and authentication of documents and websites[42].

Confirming the "rule" that technology is always at the forefront, there are plenty of companies ready to offer electronic certification services based on the new regulations. The Qualified Electronic Seal Certificate, for example, works in a manner analogous to the stamp currently used in companies and the blue stamp used in public administration authorities to ensure the integrity of official and binding documents[43].

So, it was in 2014 that Parliament and the European Council approved the new rules on national electronic identification systems (eIDAS), which allow access to public services available in other EU countries. The aim is "to ensure that any Trust Service has

[42] See Nguyen, K. (2018). Certification of eIDAS trust services and new global transparency trends. Datenschutz und Datensicherheit-DuD, 42(7), (pp.424-428).
[43] See Lodder, A. R., & Murray, A. D. (2017). The European Union and e-commerce. In A. R. Lodder, & A. D. Murray (Eds.), EU Regulation of E-commerce: A Commentary (pp. 1-14). Edward Elgar

the same legal validity in the community space as any paper certification[44]". It should be noted that the regulations in question were approved on September 17, but that only on July 1 they legally cover these electronic interactions[45].

Starting, July 1, 2016, the European Union started to implement new rules to regulate electronic commerce between people, businesses and public administrations of all member countries. This new version of the European regulation is called to update the current rules, dating from 1999, to improve and enhance e-commerce throughout the EU. With the new electronic signature rules, the European Union intends to make electronic transactions between its member countries easier, safer and of course, completely legal regardless of the specific territory where the contracts or concrete agreements are signed, in a further step towards a unique digital market[46].

The new EIDAS regulation replaces the old electronic signature directive, introduced in 1999 but which had not achieved a full and effective implementation of the electronic signature in all the countries of the European Union, due mainly to the different interpretations of the laws in each state, and the lack of the necessary technical structure. These new laws, in accordance with the communiqué of the European Commission, affect equally the 28-member countries of the Union, so that an electronic signature of a country will be recognized in any other EU country without exceptions, and will also have the same value as a written signature. The electronic signature itself is not the only thing controlled by the EIDAS regulations. Other elements related to electronic commerce will also be regulated by this regulation, in order to ensure that they work equally in all countries, and that they can be admitted in legal proceedings.

We are talking about things like the timestamp that proves the existence of a document at a certain time and that has not changed since then; the electronic seal, equivalent to a stamp that proves the authenticity of a document; the digital delivery

[44] See "Trust Services and Electronic identification (eID)", available at : https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

[45] See Attström, K., Ludden, V., Lessmann, F., Weström, P., Conrads, J., Carrapico, H. F., ... de la Maza, C. (2017). Study on the Evaluation of the European Union Agency for Network and Information Security. Luxemborg: Publications Office of the European Union, (p.5-10).

[46] ibid

record, which would be like the electronic version of a certified letter; the authentication of the website, a certificate that proves the authenticity of a website and its content; and the possibility of using all these documents with full legal validity. In the words of the European Union, this regulation will help all these services gain in security, integrity and legal value, which will encourage European citizens to participate more in electronic commerce. In addition to the regulation of economic transactions across the EU, the EIDAS regulation will also open an Observatory where individual citizens, businesses and public administrations with links to electronic commerce can exchange views and opinions, as well as suggest new ideas and best practices[47].

In this way, as has happened with other regulations that regulate some aspects of the digital world, such as the Privacy Directive or the e-commerce Directive, Directive 1999/93 / EC was also outdated. That is why the new Regulation (EU) No. 910/2014 has emerged and entered into force on July 1, 2016 throughout the European Union. The eIDAs Regulation regulates electronic identification and establishes guidelines for trust services related to electronic transactions that are common to all EU countries[48].

The new European Regulation on electronic identification and trust services, defines a new legal framework for electronic signatures in the European Union. But not only for the electronic signature, but also for the following services, which are also trusted services, as well as the electronic signature: establishment of stamps and time stamps, electronic documents and registered electronic delivery services or certified email, as well as certificate services for website authentication. It should be noted that the new Regulation - not Directive, which means that it does not need transposition in the Member States and therefore, is applied directly - extends the provisions of the previous 1999 Directive, regulating the establishment of a common basis for interaction secure electronics among citizens, businesses and European public authorities[49].

[47] Ibid

[48] See Nguyen, K. (2018). Certification of eIDAS trust services and new global transparency trends. Datenschutz und Datensicherheit-DuD, 42(7), 424-428.

[49] See Hučková, R., Sokol, P., &Rózenfeldová, L. (2018). 4th Industrial Revolution and Challenges for European Law (with Special Attention to the Concept of Digital Single Market). EU AND COMPARATIVE LAW ISSUES AND CHALLENGES SERIES, 201, (pp.2-9).

The intention of this expansion is to increase the efficiency of public and private online services, to enhance electronic commerce in the European territory and to make individuals trust more in electronic transactions. That is, in short, it is about eliminating the barrier between member countries, having citizen identification systems and the validity of their electronic signatures that allow them to operate with greater agility, lower cost and be more efficient at a European level[50]. The European Commission is committed to harmonizing the Cryptography regulations of all its member states. So far, the majority of the European countries have laws on digital signature and / or encryption:

Greece

One would expect that, prior to Directive 1999/93, any regulation of the digital signatures issue would be non-existent in Greece. The national legislature, however, in Article 14 of Law 2672/98 introduced the legal concept of "digital signature" quite early, but with limited scope. Article 14 of Law 2672/98 is entitled "Document Handling by Electronic means" (fax) and expresses the intention of the national legislator to allow the circulation of electronic documents:

- Between Public Services and OTA or
- Among these are the interested natural and legal persons by fax and e-mail.

Article 14 (2) (e) gives the first definition of digital signatures in Greece, according to which: "As a digital signature (defined), the electronic type of signature formatted in data or logically related to it, used by the signatory as an indication of acceptance of the content of such data, provided that such signature:

- it is uniquely linked to the signatory
- it identifies the signatory
- it shall be created by means which the undersigned may retain under his control

[50] Nguyen (2018)

- it is linked to the data to which it relates in such a way that any subsequent alteration of that data may be disclosed.

This definition is quite similar to the definition of advanced electronic signature (or digital signature) of Directive 1999/93. As regards the legal effects of the digital signature, Article 14 § 22 of Law 2672/98 introduces the concept of assimilation, providing that the digital signature produces the same results as the handwritten signature under the current legislation[51].

The eIDAs Regulation, greatly changes the previous legal framework of digital signatures in Greece, which came into force with the Presidential Executive Order 150/2001. As it has already been mentioned, the regulation aims to boost confidence in digital transactions within the union, by ensuring a common basis for secure electronic transactions between citizens, businesses and public bodies. It promotes and extends a transnational integrated framework for the development of secure, reliable and easy-to-use electronic transactions by establishing a Digital Single Market[52]. Greece, under this regulation, is legally obliged to recognize national eID (electronic identity) systems and accordingly their digital signatures from other EU countries which have already incorporated and complied with the eIDAs regulation. The Regulation specifies the security requirements and the providers' supervision framework according to whether or not they are qualified or non-qualified, whether or not they have approved trust services.

It should be noted that certification service providers which can issue approved certificates under EC Directive 1999/93 / EC, are required to submit an assessment report on their compliance to the supervisory authority. If the provider fails to submit a timely report, he cannot be considered an approved trust service provider. The supervisory authority in Greece is EETT[53], which maintains a register of Certification Service Providers established in Greece

[51] See Κόμνιος Κ., 2003, «Η ηλεκτρονική διακυβέρνηση (E-Government) και οι ηλεκτρονικές υπογραφές στη δημόσια διοίκηση», Περιοδικό Δίκη Τόμος 2003

[52] See "Digital single market consultations", available at : https://ec.europa.eu/commission/priorities/digital-single-market_el

[53] HELLENIC TELECOMMUNICATIONS & POST COMMISSION, https://www.eett.gr/opencms/opencms/EETT_EN/index.html

Germany

The digital signature law regulates the certificates of the keys and the certifying authority. It allows the pseudonym but provides for its real identification by court order. The electronic signature is defined as a digital seal, with a private key associated with the public key certified by a certifier. The Law of September 19, 1996 is the first digital signature bill in Europe.

France

The new Telecommunications Law and provisions on the internal use of encryption

Italy

The Law of March 15, 1997 number 59, is the first law of the Italian legal system that includes the principle of full validity of computer documents. The regulation approved by the Council of Ministers on October 31, 1997, although for the effective recognition of the legal value of computer documentation and digital signatures, it will be necessary to wait for it to be operative by virtue of the emanation of the subsequent and indispensable technical regulations of action. The digital signature is defined as the result of the computer process (validation) based on a system of asymmetric or double keys, a public and a private one, which allows the subscriber to transmit the private key and the recipient to transmit the public key, respectively, to verify the origin and integrity of a computer document or a set of computer documents (article 1 paragraph b). In the regulation the

digital signature is based exclusively on the use of so-called asymmetric encryption systems[54].

The article 2 of the Italian Regulation establish that computer documents will be valid and effective for all legal purposes if they are in accordance with the requirements of the Regulation; in particular, art. 10.2 equates the digital signature on a computer document to the signature written on paper; and art. 11.1 establishes that contracts made by telematic or computer means through the use of the digital signature according to the provisions of the regulation will be valid and effective for all legal purposes; but bear in mind that article 8 states that anyone who intends to use asymmetric cryptography with the effects of art. 2 must obtain an appropriate pair of keys and make public one of them through the certification procedure carried out by a certifier. They regulate the Law and the Regulation among other things: The validity of the computer document; the computer document without digital signature; the computer document with digital signature; the certifiers; the certificates; authentication of the digital signature; the "cybernotary"; notarial public acts; the temporary validation; the expiration, revocation and suspension of the keys; the false digital signature; Duplicity, copy and extracts of the document; and the transmission document; and the transmission of the document. This regulation is based on foreign and supranational solutions[55].

Spain

The current legislation and jurisprudence in Spain are broad enough to receive under the concept of signature, the digital signature and any other type of signature. It is true that for reasons of security and to offer greater confidence in the users and judges who ultimately must judge the digital signature, a reform of the law whose objective was

[54] See Piva, A., Tinnirello, I., &Morosi, S. (Eds.). (2017). Digital Communication. Towards a Smart and Secure Future Internet: 28th International Tyrrhenian Workshop, TIWDC 2017, Palermo, Italy, September 18-20, 2017, Proceedings (Vol. 766). Springer.

[55] See Blythe, S. E. (2005). Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security. Richmond Journal of Law & Technology, 11(2), 6.

to equate the handwritten signature to any other means of signature that would fulfill the same purposes it would be a positive step[56].

Article 3 of the RD. 2402/1985, of December 18, when regulating the minimum requirements of invoices, does not require that they be signed. It is true that the Spanish Commercial Code does not require, as a general rule, for the effectiveness of the contract or the invoice, the signature or any other sign of validity, although many legal systems require that the documents must be signed in manuscript form.

The Circular of the Bank of Spain 8/88 of June 14 creating the regulation of the National System of electronic compensation, became a pioneer and marked a milestone for the protection and security necessary in the identification for access to information, indicating that the information will be encrypted, so that the entities introduce an authentication data with the information of each communication, to which this method is recognized the same value as the one that has a written document signed by people with enough power.

Article 45 of Law 30/1992 on the legal regime of Public Administration and the Common Administrative Procedure incorporated the use and application of electronic means in administrative action, in the face of citizens. For its regulation, Royal Decree 263/1996 of 16 February, indicates that technical measures must be adopted to guarantee the identification and authenticity of the declared will, but does not make any legal regulation of the "electronic signature"[57].

Other European countries

In the Netherlands an inter-ministerial body responsible for the study of the digital signature has been created. In Denmark, Switzerland and Belgium bills were prepared on digital signature. In the European Community Article 6 of the EDI Agreement of the

[56] Lodder, A. R., & Murray, A. D. (2017). The European Union and e-commerce. In A. R. Lodder, & A. D. Murray (Eds.), EU Regulation of E-commerce: A Commentary (pp. 1-14). Edward Elgar.
[57] ibid

Commission of the European Communities, determines the need for guarantee of origin of the electronic document, does not regulate the electronic signature.

The reliability of the electronic signature is superior to that of the handwritten signature. Equalization in the international commercial field of the electronic signature and the handwritten signature is considered. In the context of EDI transactions, it is usual to use the so-called "digital signature" that is based on "symmetric algorithms" in which both parties know the same key or in "asymmetric algorithms" in which, on the contrary, each contractor has a different password. In the same vein Isabel Hernando referring to the standard contracts in EDI indicates that if the EDI messages are transmitted through authentication procedures such as a digital signature, these messages will have the same probative value among the contracting parties as agreed to a signed written document. The European Commission has financed numerous projects (INFOSEC, SPRI, etc.) whose objective is the investigation of the technical, legal and economic aspects of the digital signature[58].

United Kingdom

In UK there is a lively debate on the possible regulation of Trusted Third Parties -TC. The legal framework for Digital Signatures in the UK is derived from the EU eIDAS Regulation. The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 implement the eIDAS Regulation in the UK, setting specific provisions on the effect, supervision, and enforcement of the regulation.

Struggle of finding common legal recognition

What the European Commission intends is to find a common legal recognition in Europe of the digital signature, in order to harmonize the different legislations before the

[58] See Buchanan, B., & Naqvi, N. (2018). Building the Future of EU: Moving forward with International Collaboration on Blockchain. The JBBA, 1(1), 3579.

year 2020, so that it has a legal nature before courts in criminal, civil and commercial matters, for the purposes of proof, warning and authenticity. Despite the security offered by the digital signature, any new legislative proposals will attempt to regulate the electronic signature in general, and not only the digital signature in particular, in an attempt to cover other electronic signatures, based on techniques other than asymmetric cryptography. This neutrality is surely convenient, to leave open the doors to future technological developments. But, on the other hand, taken to that end, leaves unresolved, because they are not even addressed, many of the problems currently posed by digital signatures, the only secure electronic signatures today[59].

To achieve European coherence, it will undoubtedly have to go through the establishment of a European policy of harmonious control with other economic powers such as the USA, Canada and Japan.

The status of the Digital Signature in Europe

Since the introduction of the European standard EU 910/2014, a real revolution is taking place given the repercussions that for the first time there will be a single digital market in Europe. Given the leading role played by the electronic signature in this framework, the role of the electronic signature is crucial for the proper development of e-Administration. In addition, thanks to funding programs that have been developed based on the Europe 2020 guidelines, companies specializing in ICTs can continue to advance in the development of projects to achieve the objectives set in Horizon 2020.

For example, it is intended that both natural and legal persons can use their electronic identification document (EIDs) in other countries of the European Union, to access telematic or online procedures of the different governments (e-government services).The latter would also allow, among other things, that the provision of cross-border healthcare would become a reality for Europeans through the use of such

[59] See Lodder& Murray, (2017:4-9).

electronic identification mechanisms; or that other administrative procedures between companies, individuals and governments of the European Union states could be done more efficiently[60].

United States

In the U.S., the legislation is commonly known as the ESIGN Act and UETA. Those acronyms stand for:

- The United States Electronic Signatures in Global and National Commerce Act and
- The Uniform Electronic Transactions Act

The ESIGN Act is a federal law, signed in 2000. It specifically identified the importance and legitimacy of electronic signatures and records, assuming contract participants agree to use electronic documents and e-Signing[61].

UETA was a forerunner of the ESIGN Act., introduced in 1999. The key provision of UETA is that when a law requires a document or a signature, an electronic record or an eSignature is valid when transacting parties agree to proceed electronically. At the end of the 1970s, the United States government published the Data Encryption Standard (DES) for its sensitive but unclassified data communications[62].

On April 16, 1993, the US government announced a new cryptographic initiative aimed at providing civilians with a high level of security in communications: Clipper project. This initiative is based on two fundamental elements:

- An encryption chip to test any type of analysis or manipulation (the Clipper chip or EES (Escrowed Encryption Standard) and
- A system for sharing secret keys (KES -Key Escrow System) that, in certain circumstances, would grant access to the master key of each chip and that allows knowing the communications encrypted by him.

[60] Ibid
[61] Markos, E., Milne, G. R., & Peltier, J. W. (2018). Information sensitivity and willingness to provide continua: a comparative privacy study of the United States and Brazil. Journal of Public Policy & Marketing.
[62] ibid

In U.S.A, this is where the legislation on electronic signature is most advanced, even though the NIST standardization project (The National Institute of Science and Technology) does not succeed. The NIST has introduced within the Capstone project, the DSS (Digital Signature Standard) as a signature standard, although the American government has not yet assumed its use as a standard. The NIST has pronounced in favor of the matching of the handwritten and the digital signature. The law of reference of the digital signature, for the legislators of the United States, is the ABA (American Bar Association), Digital Signature Guidelines, of August 1, 1996. The probative value of the firm has already been admitted in Utah, the first state to acquire a digital signature law. The digital signature of Utah (Digital Signature Act Utah of February 27, 1995, modified in 1996) is based on an "Asymmetric Cryptosystem" defined as an algorithm that provides a secure key pair. Its objectives are to facilitate trade through reliable electronic messages, minimize the incidence of digital signature forgery and fraud in electronic commerce[63].

According to the above, the digital signature is a transformation of a message using an asymmetric cryptosystem, in such a way that a person who has the encrypted message and the public key of the person who signed it can accurately determine the message in clear and if it was encrypted using the private key which corresponds to the public of the signer[64].

This law establishes the presumption that a digital signature has the same legal effect as a handwritten signature if certain stocks are met; one of the requirements is for the digital signature to be verified by reference to a public key included in a valid certificate issued by a licensed certification authority[65].

[63] Ford, W., & Baum, M. S. (2000). Secure electronic commerce: building the infrastructure for digital signatures and encryption. Prentice Hall PTR, (pp.2-6).
[64] See Lloyd, I. (2017). Information technology law. Oxford University Press.
[65] See Blythe, S. E. (2005). Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security. Richmond Journal of Law & Technology, 11(2), 6.

The State of Utah has drafted a bill (The Act on Electronic Notarization) in 1997[66], while California[67] defines the digital signature as the creation by computer of an electronic identifier that includes all the characteristics of a valid, acceptable signature, such as: only able to be checked under a single control linking with the data in such a way that if the data is changed the signature is invalidated adopted at least as a standard by two of the following organizations:

- The International Telecommunication Union.
- The American National Standards Institute.
- The Internet Activities Board.
- The National Institute of Science and Technology.
- The International Standards Organization.

Other notable US legal initiatives could be the ABA Resolution concerning the Cyber Notary, which can be referred to as an International computer-transaction specialist[68]. The Electronic Signature Act Florida[69], of May of 1996 that recognizes the probative equivalence of the digital signature with the manual signature. In this law, the term "international notary" is used instead of the "cyber notary" used in other US laws. The Massachusetts Electronic Records and Signatures Act, of 1996, that welcomes all mechanism able to provide the functions of the handwritten signature without sticking to a specific type of technology[70].

[66] "Notarization and Authentication of Documents and Electronic Signatures" https://le.utah.gov/xcode/Title46/Chapter1/46-1-S16.html?v=C46-1-S16_1800010118000101

[67] Government Code section 16.5, available at : https://www.sos.ca.gov/administration/regulations/current-regulations/technology/digital-signatures/frequently-asked-questions/#definition

[68] See Del Duca Patrick, (2010), CHOOSING THE LANGUAGE OF TRANSNATIONAL DEALS: PRACTICALITIES, POLICY AND LAW REFORM, American Bar Association.

[69] Available at http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&URL=0600-0699/0668/0668.html

[70] See Hamel, L., (2004). Case & Statute Comments: The Massachusetts Uniform Electronic Transactions Act: Continuity and Change, Massachusetts Law Review, Issue v89 n1 January

International level

United Nations

The United Nations Commission for International Trade Law (UNCITRAL UNCITRAL) at its twenty-fourth session held in 1991 commissioned the Working Group on International Payments to study the legal problems of electronic data interchange (EDI: Electronic Data Interchange). The Working Group devoted its 24th session, held in Vienna from January 27 to February 7, 1992, to this topic and prepared a report that was submitted to the Commission. The definition of "signature" and other means of authentication that have been given in some international conventions were examined. The broad definition of "signature" contained in the United Nations Convention on International Letters of Exchange and International Promissory Notes was kept in mind, which reads: "The term signature designates the handwritten signature, its facsimile or an equivalent authentication made by others"[71].

On the contrary, the Model Law on International Credit Transfers uses the concept of "authentication" or "commercially reasonable authentication", dispensing with the notion of "signature", in order to avoid the difficulties that this may cause, both in the traditional meaning of this term as in its extended meaning. At its twenty-fifth session in 1992, the Commission reviewed the report of the Working Group and entrusted the preparation of the legal regulation of EDI to the Working Group, now referred to as Electronic Data Interchange[72].

[71] Castellani, L. G. (2016). The United Nations Convention on the Use of Electronic Communications in International Contracts at ten: practical relevance and lessons learned. Journal of Law, Society and Development, 3(1), 132-152.
[72] Mazzotta, F. G. (2006). Notes on the United Nations Convention on the Use of Electronic Communications in International Contracts and Its Effects on the United Nations Convention on Contracts for the International Sale of Goods. Rutgers Computer & Tech. LJ, 33, 251.

The Working Group on Electronic Data Interchange held its twenty-fifth session in New York from January 4 to 15, 1993, in which the authentication of EDI messages was attempted, with a view to establishing a functional equivalent to the "firm"[73]..

The Plenary of the United Nations Commission for International Trade Law (UNCITRAL), on June 14, 1996, at its 29th session held in New York, reviewed and approved the draft Model Law on legal aspects of EDI under the denomination of Model Law on electronic commerce (General Resolution of the Assembly 51/162 of December 16, 1996). Article 7 of the Model Law includes the concept of signature[74].

The Commission entrusted the Working Group, now called "on Electronic Commerce", and with the task of examining legal issues related to digital signatures and certification authorities. The Commission requested the Secretariat to prepare a background study on issues related to digital signatures. The study of the Secretariat was included in document A / CN.9 / WG. IV / WP.71 of December 31, 1996. The Working Group on Electronic Commerce held its 31st session in New York from February 18 to 28, 1997, which sought to establish guidelines on digital signatures published by the American Bar Association[75].

The Plenary of the United Nations Commission on International Trade Law, which held its thirtieth session in Vienna from 12 to 30 May 1997, reviewed the report of the Working Group, endorsed the conclusions and entrusted the preparation of a uniform regime on the legal issues of the digital signature and the certifying entities. Article 7 of the Model Law on Electronic Commerce regulates the functional equivalent of a signature, establishing the requirements for the admissibility of a signature produced by electronic means, which gives us a broad concept of electronic signature, stating "when the law requires the a person's signature, that requirement will be satisfied in relation to a data message: a) if a method is used to identify that person and to indicate that that person approves the information contained in the data message; and b) whether that method is

[73] Castellani, (2016:2-10).
[74] Mitchell, A. D., & Mishra, N. (2017). International trade law perspectives on paperless trade and inclusive digital trade (No. 170). ARTNeT Working Paper Series.
[75] Friedman, J. (2015). Signing Your Next Deal with Your Twitter@ Username: The Legal Uses of Identity-Based Cryptography. Canadian Journal of Law and Technology, 13(1).

as reliable as is appropriate for the purposes for which the data message was created or communicated, in light of all the circumstances of the case, including any relevant action. " (Mitchell & Mishra, 2017:10).

Section 3 of draft article A of WP.71 states that "a digital signature attached to a data message is considered authoritative if it can be verified in accordance with procedures established by a certifying authority"[76].

Organization for Economic Co-operation and Development

The Recommendation of the OECD (Organization for Economic Co-operation and Development) on the use of cryptography (Guidelines for Cryptography Policy) was approved on March 27, 1997. This recommendation has no binding force and points out a series of rules that governments should take into account when adopting legislation on digital signature and trusted third parties, in order to prevent the adoption of different national rules that could hinder electronic commerce and the information society in general[77].

International Organization of Standards

On ISO / IEC 7498-2 (OSI Security Architecture) all subsequent regulatory developments rest, regulates the security services on confidentiality, integrity, authenticity, access control and non-repudiation. Through its subcommittee 27, SC 27, it works on a digital signature standard.

[76] Holzer, M., & Manoharan, A. P. (2016). Digital governance in municipalities worldwide (2015-16). Seventh global e-governance survey: a longitudinal assessment of municipal websites throughout the world. Newark: National Center for Public Performance. Retrieved from https://www.seoulsolution.kr/en/content/rutgers-spaa-digital-governance-municipalities-worldwide-2015-16

[77] Wang, M. (2017). Establishment of an international legal framework for cross-border electronic commerce rules: Dilemmas and solutions. World Customs Journal, 61.

Legality of documents with digital signature

The problem arises that some legislations impose written and handwritten signature requirements as a condition of validity or as a condition of proof of certain contracts and legal acts. Consequently, in order for these contracts to be plausible from a legal point of view, either jurisprudence must interpret the term signature and writing broadly enough to accommodate the digital signature, or the law must be modified trying to assimilate the digital signature to the handwritten signature. The legal validity of the digital signature has not yet been proven in any hearing before the courts of justice, and therefore there are no full legal guarantees for its use.

However, in cryptographic environments the digital signature with a capacity superior to the manuscript is considered, since it not only entails the authenticity of the signed document, but also its integrity; or what is the same, the certainty that it has not been altered in any of its parts. Currently there is no legal problem for the use of the digital signature by a group of users, provided that they sign "manually" a prior agreement about its use in their commercial transactions, as well as the signature method and sizes (and values) of the public keys to be used. Most of the existing legislative initiatives on digital signature, recognize the effects of the same, equating it, with more or less requirements, to the handwritten signature. Certain requirements are made obligatory. The most important is the existence of a trust third party.

Certification Authorities - Trusted third parties

The essential task is to authenticate the property and characteristics of a public key, so that it is trustworthy, and issue certificates. They offer different services, being able to enjoy legitimate access to encryption keys[78].

The functions of a Certification Authority must be, among others, the following:

[78] Hučková et al (2018).

- Generation and Registration of keys.
- Identification of Certificate Petitioners.
- Issuance of certificate.
- Storage in the AC of your private key.

The structure and the functioning chart of the certification authorities (public key infrastructure) generally foresee a hierarchical structure at two levels: The top level is usually occupied by public authorities, which is the one that certifies the subordinate authority, normally private.

Chapter 3: From Digital Signature to Biometric Signature

The signature systems that are as safe as the electronic signature are in demand but more usable, and in this context, biometrics emerge; identification technology based on the recognition of a physical and non-transferable characteristic of people. One of the most interesting biometric systems in terms of security and cost is the biometric recognition of calligraphic features of the firm[79]. The biometric digitized signature is a highly recommended authentication method by:

- The signature is the most widespread authentication and authorization mechanism in the world.
- It is totally independent of the language and the characters used.
- It is a non-intrusive method, it is not perceived as a violation of privacy.

The signature, as a guideline of behavior learned by any human being, is difficult to forget, as it can be the case of many keys and PINs. Likewise, the signature is linked to the person, and it is practically impossible that their identity can be replaced by another person, as could be the case with the theft of keys and PINs[80]. The following quadrant shows that a person can be identified through two bivalent parameters:

Physical versus Behavioral: knowing if it is something linked to the person physically, or behavior patterns.

Biometric versus Object: to know if it is something linked "biologically" to the person, or simply something that the person carries with them.

It can be seen that the dynamic (or biometric) handwriting signature has practically the same recognition power, from a biometric point of view, that facial recognition and more than the recognition of Iris. And it is just as representative (from a behavioral point of view) as the voice[81].

[79] Griffin, P. H. (2018, July). Biometric Electronic Signature Security. In International Conference on Applied Human Factors and Ergonomics (pp. 15-22). Springer, Cham.
[80] Ibid
[81] Ibid

Technology

This technology allows users to make handwritten signatures in electronic format on tablets in a totally safe and reliable way, as if they were signing a paper document. The files are saved and certified not only taking into account the signature of the signatory, but also other biometric data such as the speed or pressure with which the signature is signed.

Comfort

The main advantage of the biometric signature system is its universality of use. It does not require the signer to have a certificate, keep it updated and also carry it with him at the time of signing and remember the passwords.

Security

In order to generate confidence in this type of signature, it is important that during the process of generating and capturing the biometric signature, guarantees can be obtained that the generated biometric signature cannot be reproduced in order to avoid the risk of its use for fraudulent purposes. For this, the encryption of biometric data is used in the same capture device by means of an asymmetric key whose decryption key is only in the possession of a trusted third party. The biometric data once encrypted are incorporated as metadata in the signed electronic document, which is in turn electronically signed using a recognized electronic signature of the organization with a time stamp, in order to safeguard the integrity of all the data it contains. The combination of biometric signature, electronic signature by recognized certificate and time stamp provide authentication features, integrity and non-repudiation of the document. The contribution in judgment of the biometric signature is governed by the general rules of the test and will normally require the generation of an expert opinion.

Difference between the biometric signature and the digital signature

Although at first glance the biometric signature and the digital signature seem similar concepts and are considered by many to be synonymous, the truth is that they are totally different concepts and that it is very important to differentiate. On the one hand, the biometric signature or advanced electronic signature allows not only to capture the graph, but also the biometric features that link the signer uniquely. Among these features are the speed and acceleration at the time of writing, as well as the pressure exerted on the signature and the inflections or changes of direction of this. Therefore, the advantage of the biometric signature over the digital signature allows companies to prevent the identity of the signatory from being impersonated in the documents, thanks to which the authenticity of the signature can be verified. However, the biggest difference with respect to the digital signature lies in the legal aspect. The biometric signatures allow signing any document with full legal validity, the biometric signature is considered as an advanced electronic signature that guarantees authenticity, integrity and non-repudiation of the signer's documents[82].

Privacy Implications

Provision of consent through the use of digital signatures begins to be frequent that users' consent is sought in contracts of financial entities initialed with handwritten signatures digitized in tablet, replacing the obsolete handwritten signatures on paper. By signing on the device that captures our line, the entity associates it with the specific clauses to which it links users, thus achieving the perfection of the contract. In accordance

[82] See Linden, J., Marquis, R., Bozza, S., &Taroni, F. (2018). Dynamic signatures: A review of dynamic feature variation and forensic methodology. Forensic science international, (pp.3-9).

with the current regulations, the perfection of the contract must be carried out without incurring any of the causes of contractual nullity[83].

Biometric identification mechanisms capture, process and store information related to, among others, the physical features of people (fingerprints, DNA, shape or silhouette of the hand, patterns of the retina or iris, facial aspects), in order to establish or "authenticate" the identity of each subject. In the activities of the digital environment, these are another example of electronic signature. The use of these systems is not without worries and praises. Among the first, the phenomenon of the computerization of the body and the use of it as a password is not a peaceful issue. In this sense, a study of the RAND Institute in 2001 is illustrative, in which the juridical, ethical and sociological aspects associated with biometrics were evaluated, highlighting three areas that generate ethical and social concern, namely: the privacy of information, the physical intimacy and religious objections. Regarding the latter, it is common to see advertisements that sell biometric systems as the solution to identity problems. Each biometric method has weaknesses and strengths. The degrees of uniqueness and precision offered by each are diverse. No biometric system is free from failures caused by human or technological errors related to capture and processing, or with conditions such as age, skin color, aging or the ease of handling these mechanisms in certain situations[84].

In the first place, there seems to be a consensus that the use of the fingerprint is infallible in terms of security. Reality shows that the subject is not always like that. The Supreme Court of Justice in Columbia, for example, in 2009, verified the impersonation of the fingerprint of a Rear Admiral of the Navy. Within the process, it was established that "the trace (...) is an imitation obtained by mechanical means". He pointed out how simple it is to impersonate fingerprints, since "it is enough to have the fingerprint on any document, to take the impression that the stamp reproduces from there". Secondly, the future law on the protection of personal data catalogs biometric information as sensitive data and proscribes, as a general rule, the treatment of this information. Exceptionally,

[83] See Govinda, K., Gurunathaprasad, V., &Sathishkumar, H. (2012). Third party auditing for secure data storage in cloud through digital signature using RSA. International Journal of Advanced Scientific and Technical Research, 4(2), (pp.525-530).
[84] Linden et al (2018:3-9).

biometric information can be collected and used with prior authorization, explicit and informed by the owner[85].

Finally, the data protection regulation will irrigate its mandates to scenarios traditionally unrelated to this topic. In effect, issues that we normally see from an area of law should now also be analyzed from the perspective of the protection of personal data. Photos, for example, are usually addressed from the regulation of copyright. However, a photo contains the image of a person, which is a biometric data. Therefore, now we must reflect on the implications of the future regulation of personal data regarding the capture, storage, publication, etc. In a nutshell, biometric systems are not the best, nor the worst, but their use requires reflection and reorientation of the practices that have been taking place before the validity of the new personal data protection law[86].

Personal data protection

The main concern of users who use biometrics is the security with which that information is stored, because there will have to be a database with the digitized information, in this way the system will be able to compare it every time, for example, we try to access our workplace where it is necessary to pass a fingerprint scanner. Is the information stored with sufficient security? The main problem with biometrics is that if they steal this data, they will steal it forever because, for example, your fingerprints or your retina will not change. With passwords this does not happen, because if we lose our passwords, we can always change them easily[87].

Biometric equipment normally registers a digital representation (template) and not a reproducible biometric sample. The biometric system that, through the algorithmization

[85] See Juels, A., Molnar, D., & Wagner, D. (2005, September). Security and Privacy Issues in E-passports. In Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on (pp. 74-88). IEEE.
[86] See Khalilov, M. C. K., & Levi, A. (2018). A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems. IEEE Communications Surveys & Tutorials (pp.4-5).
[87] See Morosan, C. (2018). Information Disclosure to Biometric E-gates: The Roles of Perceived Security, Benefits, and Emotions. Journal of Travel Research, 57(5), (pp. 644-657).

process, generated the template that numerically represents the captured biometric feature, does not allow the reversion and, consequently, to decode and reproduce, in a digitized form, the image of the biometric characteristic (e.g. representation fingerprint, iris, hand geometry, or facial geometry). The controller does not therefore have a database of biometric features, but a structured list of those characteristics.

It will be different for the invasion of privacy storage through the digitization and reference of the biometric characteristics or the constitution of a database of the templates of these characteristics. The centralization of biometric features in databases presents additional dangers to privacy, which is why their relationship with other types of technologies (eg video surveillance) is not acceptable in principle. This relationship is without prejudice to the possibility of using 'multimodal systems', characterized by the use of more than one biometric feature in order to give greater efficiency and accuracy to the operations of recognition or authentication. Companies that market biometric systems often ensure that privacy is fully assured as such systems do not allow for the 'rollback' or comparison of templates, especially since the keys of the templates are in the hands of the manufacturer and are inaccessible to the entities that supply or purchase the equipment[88].

[88] See Nandakumar, K., & Jain, A. K. (2015). Biometric template protection: Bridging the performance gap between theory and practice. IEEE Signal Processing Magazine, 32(5), (pp. 88-100).

Conclusions

The work has tried to give an idea of the important changes that the firm has experienced from its origins to our days and how they should try to adapt these changes to the social reality and leave the door open to other future changes and new technologies that will undoubtedly come. The new information and communication technologies, together with other techniques, give reliability to the electronic document and try to achieve greater security through the development and extension of technical remedies and control procedures based on cryptography. This greater security that is intended with a regulatory adaptation will lead us towards electronic authentication. The fear that exists for these new information technologies is not in the electronics, nor in the communications, but in their misuse due to the lack of training and adaptation of people and means to the social reality. The creation of electronic public certification authorities (trusted third parties) will lead us to superior guarantees in the authentication of the documents circulating through the communication lines, as well as the creation of a public control file with greater guarantees than the current ones.

The current EU legislation entrusts the role of trusted third party responsible for providing security to electronic signatures, establishing a link between the verification element and a specific person to entities that it calls certification service providers (community terminology option that it shows a willingness to avoid even the appearance of attribution of a public nature that could be suggested by other denominations such as, for example, certification authority). The eIDAS Regulation defines the certification service provider as the person or entity that issues certificates or provides the public with other services related to electronic signatures; such services may be inherent to the certificate itself and necessary (revocation and suspension in case of loss of the private key or other element of signature), others rather debatable as well as other complementary but equally necessary for the security of the certificate system in particular or of electronic commerce in general.

A single Certification Body of universal scope is not viable, therefore there must be one or several networks of national or sectorial authorities, interrelated and that in turn

provide service to the users of their respective fields. The digital signature, with the guarantees demanded by an increasingly necessary legal security, can open a promising path that leaves in question the real effectiveness of the traditional public faith. Among the objectives of the digital signature is to achieve a universalization of an electronic signature standard, which could be favored with the elaboration of a global regulatory framework.

Knowing how to make a digital signature on mobile phone is a differential to be offered to customers of a company, as well as optimizing the day to day of business, reducing expenses, time and paperwork. From contracts to e-mails, everything that is electronically signed with this certificate becomes legal. This allows for sales contracts to be closed in minutes or in hours, as there is no longer any need to move. Many companies are using the Digital Certificate to sign all their documents that need legal validity, making it possible for their representatives to sign from anywhere in the world, with only a computer / cell phone and internet access. Digital signature is a new global trend. Focusing on users, this technology has come to simplify the process of signing documents, making it cheaper and more agile.

Bibliography

Abbott, K. W., Keohane, R. O., Moravcsik, A., Slaughter, A. M., & Snidal, D. (2000). The concept of legalization. International organization, 54(3), 401-419.

Abidi, A., Bouallegue, B., &Kahri, F. (2014, June). Implementation of elliptic curve digital signature algorithm (ECDSA). In Computer & Information Technology (GSCIT), 2014 Global Summit on (pp. 1-6). IEEE.

Abu-Hakima, S. (2004), "Concept identification system and method for use in reducing and/or representing text content of an electronic document", U.S. Patent No. 6,823,331. Washington, DC: U.S. Patent and Trademark Office.

Attström, K., Ludden, V., Lessmann, F., Weström, P., Conrads, J., Carrapico, H. F., ... de la Maza, C. (2017). Study on the Evaluation of the European Union Agency for Network and Information Security. Luxemborg: Publications Office of the European Union. DOI: 10.2759/674883

Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016, May). Blockchain-the Gateway to Trust-Free Cryptographic Transactions. In ECIS (p. ResearchPaper153).

Beenau, B. W., Bonalle, D. S., Fields, S. W., Gray, W. J., Larkin, C., Montgomery, J. L., & Saunders, P. D. (2008). Method and system for proffering multiple biometrics for use with an FOB, U.S. Patent No. 7,360,689. Washington, DC: U.S. Patent and Trademark Office.

Ben-Assuli, O. (2015). Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments. Health Policy, 119(3), 287-297.

Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In Post-quantum cryptography (pp. 1-14). Springer, Berlin, Heidelberg.

Bisbee, S. F., Carpolette, B. K., & Moskowitz, J. J. (2010). "System and method for electronic transmission, storage, retrieval and remote signing of authenticated

electronic original documents", U.S. Patent No. 8,924,302. Washington, DC: U.S. Patent and Trademark Office.

Blythe, S. E. (2005). Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security. Richmond Journal of Law & Technology, 11(2), 6.

Bouchard, T., & Benson, G. (2006), "Electronically verified digital signature and document delivery system and method", U.S. Patent No. 7,082,538. Washington, DC: U.S. Patent and Trademark Office.

Boutant, Y., Labelle, D., & Seux, H. (2015). Use of a digital signature obtained from at least one structural characteristic of a material element to protect the direct reading of sensitive data and method for reading this protected data, U.S. Patent No. 8,943,325. Washington, DC: U.S. Patent and Trademark Office.

Bresciani, P., Donzelli, P., & Forte, A. (2003, May). Requirements engineering for knowledge management in eGovernment. In IFIP International Working Conference on Knowledge Management in Electronic Government (pp. 48-59). Springer, Berlin, Heidelberg.

Buchanan, B., & Naqvi, N. (2018). Building the Future of EU: Moving forward with International Collaboration on Blockchain. The JBBA, 1(1), 3579.

Castellani, L. G. (2016). The United Nations Convention on the Use of Electronic Communications in International Contracts at ten: practical relevance and lessons learned. Journal of Law, Society and Development, 3(1), 132-152.

Chamberlin, C. R., &Reck, B. A. (2016). Apparatus and methods for the secure transfer of electronic data, U.S. Patent No. 9,252,955. Washington, DC: U.S. Patent and Trademark Office.

Chen, J. J. C., & Chia, L. (2014). Authentication of unknown parties in secure computer communications U.S. Patent No. 8,667,154. Washington, DC: U.S. Patent and Trademark Office.

Chernyi, S. G., Ali, A. A., Veselkov, V. V., Titov, I. L., & Budnik, V. Y. (2018, January). Security of electronic digital signature in maritime industry. In Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018 IEEE Conference of Russian (pp. 29-32). IEEE.

Del Duca P., (2010), CHOOSING THE LANGUAGE OF TRANSNATIONAL DEALS: PRACTICALITIES, POLICY AND LAW REFORM, American Bar Association.

Ford, W., & Baum, M. S. (2000). Secure electronic commerce: building the infrastructure for digital signatures and encryption. Prentice Hall PTR.

Friedman, J. (2015). Signing Your Next Deal with Your Twitter@ Username: The Legal Uses of Identity-Based Cryptography. Canadian Journal of Law and Technology, 13(1).

Ginter, K. L., Shear, V. H., Spahn, F. J., Van Wie, D. M., & Weber, R. P. (2006). Digital certificate support system, methods and techniques for secure electronic commerce transaction and rights management, U.S. Patent No. 7,133,846. Washington, DC: U.S. Patent and Trademark Office.

Govinda, K., Gurunathaprasad, V., &Sathishkumar, H. (2012). Third party auditing for secure data storage in cloud through digital signature using RSA. International Journal of Advanced Scientific and Technical Research, 4(2), 525-530.

Griffin, P. H. (2018, July). Biometric Electronic Signature Security. In International Conference on Applied Human Factors and Ergonomics (pp. 15-22). Springer, Cham.

Hamel, L. (2004). Case & Statute Comments: The Massachusetts Uniform Electronic Transactions Act: Continuity and Change, Massachusetts Law Review, Issue v89 n1 January

Handley, M. (2018). Schnorr's Digital Signature and its Applications. Review of Computational Science and Engineering, 4(1), 47.

Hansen, M., Obersteller, H., Rannenberg, K., &Veseli, F. (2015). Establishment and prospects of Privacy-ABCs. In Attribute-based Credentials for Trust (pp. 345-360). Springer, Cham.

Hedley, S. (2017). The Law of Electronic Commerce and the Internet in the UK and Ireland. Routledge-Cavendish.

Holzer, M., & Manoharan, A. P. (2016). Digital governance in municipalities worldwide (2015-16). Seventh global e-governance survey: a longitudinal assessment of municipal websites throughout the world. Newark: National Center for Public Performance. Retrieved from https://www. seoulsolution. kr/en/content/rutgers-spaa-digital-governance-municipalities-worldwide-2015-16.

Hučková, R., Sokol, P., &Rózenfeldová, L. (2018). 4th Industrial Revolution and Challenges for European Law (with Special Attention to the Concept of Digital Single Market). EU AND COMPARATIVE LAW ISSUES AND CHALLENGES SERIES, 201.

Juels, A., Molnar, D., & Wagner, D. (2005, September). Security and Privacy Issues in E-passports. In Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on (pp. 74-88). IEEE.

Khalilov, M. C. K., & Levi, A. (2018). A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems. IEEE Communications Surveys & Tutorials.

Kim, D., &Benbasat, I. (2003). Trust-related arguments in internet stores: A framework for evaluation. J. Electron. Commerce Res., 4(2), 49-64.

Kim, S. H., Cho, Y. S., Noh, J. H., Cho, S. R., Choi, D. S., Kim, S. H., ... & Cho, H. S. (2015). U.S. Patent Application No. 14/243,081.

Kobayashi, S., Kane, T. B., & Paton, C. (2018). The privacy and security implications of open data in healthcare. Yearbook of medical informatics.

Κόμνιος Κ., (2003), «Η ηλεκτρονική διακυβέρνηση (E-Government) και οι ηλεκτρονικές υπογραφές στη δημόσια διοίκηση», Περιοδικό Δίκη Τόμος 2003

Langheinrich, M. (2001, September). Privacy by design—principles of privacy-aware ubiquitous systems. In International conference on Ubiquitous Computing (pp. 273-291). Springer, Berlin, Heidelberg.

Linden, J., Marquis, R., Bozza, S., &Taroni, F. (2018). Dynamic signatures: A review of dynamic feature variation and forensic methodology. Forensic science international.

Lloyd, I. (2017). Information technology law. Oxford University Press.

Lodder, A. R., & Murray, A. D. (2017). The European Union and e-commerce. In A. R. Lodder, & A. D. Murray (Eds.), EU Regulation of E-commerce: A Commentary (pp. 1-14). Edward Elgar.

Mana, A., & Matamoros, S. (2002, September). Practical Mobile Digital Signatures. In International Conference on Electronic Commerce and Web Technologies (pp. 224-233). Springer, Berlin, Heidelberg.

Markos, E., Milne, G. R., & Peltier, J. W. (2018). Information sensitivity and willingness to provide continua: a comparative privacy study of the United States and Brazil. Journal of Public Policy & Marketing.

Martinez-Diaz, M., Fierrez, J., & Ortega-Garcia, J. (2015). Dynamic signature verification using portable devices.

Mazzotta, F. G. (2006). Notes on the United Nations Convention on the Use of Electronic Communications in International Contracts and Its Effects on the United Nations Convention on Contracts for the International Sale of Goods. Rutgers Computer & Tech. LJ, 33, 251.

McCabe, A. D., & Gosner, T. H. (2014). Systems and methods for distributed electronic signature documents, U.S. Patent No. 8,655,961. Washington, DC: U.S. Patent and Trademark Office.

Mitchell, A. D., & Mishra, N. (2017). International trade law perspectives on paperless trade and inclusive digital trade (No. 170). ARTNeT Working Paper Series.

Morosan, C. (2018). Information Disclosure to Biometric E-gates: The Roles of Perceived Security, Benefits, and Emotions. Journal of Travel Research, 57(5), 644-657.

Mukherjee, D., Godara, S., Das, A. K., Dey, S., Kumar, S., Islam, R., ... & Mukherjee, C. (2017, October). Unique digitized activity signature for human authentication. In Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2017 8th IEEE Annual (pp. 714-720). IEEE.

Nandakumar, K., & Jain, A. K. (2015). Biometric template protection: Bridging the performance gap between theory and practice. IEEE Signal Processing Magazine, 32(5), 88-100.

Nguyen, K. (2018). Certification of eIDAS trust services and new global transparency trends. Datenschutz und Datensicherheit-DuD, 42(7), 424-428.

Peterson, D. G., Rybacki, D. P., & Wald, D. E. (2018). System and method for rules-based control of custody of electronic signature transactions, U.S. Patent No. 9,893,895. Washington, DC: U.S. Patent and Trademark Office.

Pilkington, M. (2016). 11 Blockchain technology: principles and applications, in “Research handbook on digital transformations”, edited by F. Xavier Olleros and Majlinda Zhegu, Associate Professors of Innovation Management, École des Sciences de la Gestion, Université du Québec à Montréal, Canada, (p. 225).

Piva, A., Tinnirello, I., &Morosi, S. (Eds.). (2017). Digital Communication. Towards a Smart and Secure Future Internet: 28th International Tyrrhenian Workshop, TIWDC 2017, Palermo, Italy, September 18-20, 2017, Proceedings (Vol. 766). Springer.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), 638-646.

Poullet, Y. (2018). Law Facing Information and Communication Technology (ICT)—Conflict or Alliance? In Progress in Science, Progress in Society (pp. 91-108). Springer, Cham.

Poullet, Y., &Rouvroy, A. (2007). General introductory report. In ethical aspects of the author Information Society Conference organized Jointly by UNESCO Cancel of Europe Start book Text available on the national website

Regulation, E. U. (2014). No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation). European Union, 44-59.

Saxena, N., Kumar, D., & Pandey, A. K. (2018). Electronic signature framework with enhanced security, U.S. Patent No. 9,935,777. Washington, DC: U.S. Patent and Trademark Office.

Shih, F. Y. (2017). Digital watermarking and steganography: fundamentals and techniques. CRC press.

Skiles, D. (2012). Digital Signature Technology. Technology Tools for Today's High-Margin Practice: How Client-Centered Financial Advisors Can Cut Paperwork, Overhead, and Wasted Hours, 129-138.

Smejkal, V., Kodl, J., Novák, D., & Schneider, J. (2015). Strong Identification and Authentication Using Dynamic Biometric Signature. In Computer Science and its Applications (pp. 1245-1252). Springer, Berlin, Heidelberg.

Wang, M. (2017). Establishment of an international legal framework for cross-border electronic commerce rules: Dilemmas and solutions. World Customs Journal, 61.

Wu, C. C., Hsu, C. W., & Cheng, R. S. (2018, April). The digital signature technology for access control system of mobile. In 2018 IEEE International Conference on Applied System Invention (ICASI) (pp. 896-898). IEEE.

Zank, A. E., & Stevens, D. R. (2001). Electronic signature management system, U.S. Patent No. 6,307,955. Washington, DC: U.S. Patent and Trademark Office.

Zissis, D., &Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. Government Information Quarterly, 28(2), 239-251.