

NEAR EAST UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
MASTER OF LAW IN INTERNATIONAL LAW PROGRAM
(LL.M)

MASTER'S THESIS
THE LEGALITY OF ELECTRONIC SIGNATURE

LAVA AZAD ALI

NICOSIA

2017

NEAR EAST UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
MASTER OF LAW IN INTERNATIONAL LAW PROGRAM
(LL.M)

MASTER'S THESIS
THE LEGALITY OF ELECTRONIC
SIGNATURE

PREPARED BY
LAVA AZAD ALI
20156992

I HAVE ADHERED TO UNIVERSITY POLICY REGARDING
ACADEMIC HONESTY IN COMPLETING THIS ASSIGNMENT

SUPERVISOR
DR. DERYA AYDIN OKUR

NICOSIA
2017

NEAR EAST UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
MASTER OF LAWS IN INTERNATIONAL LAW PROGRAMME (LLM)

Thesis Defence

THE LEGALITY OF ELECTRONIC SIGNATURE

INTERNATIONAL LAW

Prepared by

Lava Azad Ali

Examining committee in charge

Asst.Prof.Dr. Resat Volkan Gunel

Near East University
Faculty of Law

Asst.Prof.Dr. Derya Aydın Okur

Near East University
Faculty of Law

Dr. Tutku Tugyan

Near East University
Faculty of Law

Approval of the Acting Director of the Graduate School of Social Sciences

Assoc. Prof. Dr. Mustafa SAĞSAN

Acting Director

YAKIN DOĞU ÜNİVERSİTESİ



NEAR EAST UNIVERSITY
SOSYAL BİLİMLER ENSTİTÜSÜ
GRADUATE SCHOOL OF SOCIAL SCIENCES

Date:/...../....., Nicosia

20___/20___ Academic Year _____ Semester

DECLARATION

TYPE of Thesis: Master ☐ Proficiency in Ar ☐ PhD ☐

STUDENT No:

PROGRAMME:

I.....
....., hereby declare that this dissertation entitled “
.....”

Has been prepared myself under the guidance and supervision of “
.....” in partial fulfilment of The Near East University,
Graduate School of Social Sciences regulations and does not to the best of my knowledge
breach any Law of Copyrights and has been tested for plagiarism and a copy of the result
can be found in the Thesis.

Signature:

ABSTRACT

The electronic signature can be used to accomplish the same functions that traditional signature does in a very secured and reliable way. This new method is what Europeans named as advanced signature. On the other hand, using electronic signature in commercial transaction will help to improve economic activities in Iraq and encourages foreign investment. The thesis therefore, encourages the Iraqi legislators to form committees to monitor and control electronic transactions in commercial and administrative fields. In order to establish the effective use of electronic signatures worldwide, e-signature laws are required. This e-signature law varies from country to country and some countries have not stated specific laws concerning the Electronic signature, but yet. However, a corporate e-signature policy can be developed and adapted by companies that will significantly work worldwide. Any company can use any agreement which can define the e-signature laws that apply to it based on the specified governing law. And when required, business partners can comply with two-tier or prescriptive laws as needed especially if your signature solution supports both e-signatures and digital signatures. E-signature can be used to support business processes, which require e-signatures, digital signatures, or a combination of the two, and business parties can automate approval workflows to route, track, and log every step of the process and then store signed documents in a searchable repository. E-signature also makes it possible for businesses to follow some best practices to help ensure their agreements are enforceable.

Keywords: Electronic Signature, Digital Signature, Electronic Documentation, E-Commerce, Electronic Transaction, Electronic Banking, Electronic Signature in Iraqi Law

ÖZ

Elektronik imza, geleneksel imza ile aynı işlevleri oldukça güvenli ve sağlıklı bir şekilde yerine getirebilmektedir. Avrupa'nın birçok ülkesinde uygulanmakta olan elektronik imza, gelişmiş imza olarak da anılmaktadır. Ticari işlemlerde elektronik imza kullanımının Irak'ın ekonomik gelişimine yardımcı olacağı ve yabancı yatırımı da teşvik edeceği düşünülmektedir. Bu çalışmada da, Iraklı kanun koyucuların ticari ve idari alanlarda elektronik işlemleri izlemek ve denetlemek üzere komiteler oluşturması teşvik edilmektedir.

Elektronik imzanın dünya çapında etkin bir şekilde kullanılabilmesi e-imza hukukunu gerektirmektedir. E-imza hukuku konusunda farklı devletlerin farklı uygulamaları bulunmakta olup, bazı devletlerin de bu konuda herhangi bir hukuki düzenlemeleri henüz bulunmamaktadır. Şirketlerin, dünya çapında işlerliği olacak bir e-imza politikası geliştirmesi mümkündür. Herhangi bir şirketin, bir sözleşmeye uygulanacak hukukun öngördüğü biçimde e-imzayı içeren sözleşmeler yapması mümkündür. İmza konusunda sunulan çözümlerin e-imzaları ve dijital imzaları desteklemesi durumunda iki kademeli bir çözüm sunulabilir.

E-imza ticari süreçleri desteklemek için kullanılabilir. Ticari sürecin tüm adımlarında, iş akışının sevk, izlenmesi ve kaydedilmesine, ayrıca imzalanan belgelerin aranabilir bir depoda saklanmasına yardımcı olur. E-imza diğer yandan işletmelerin yaptıkları sözleşmelerin uygulanabilirliğini sağlamaya yarayan bir imkanlar sunmaktadır.

Anahtar Kelimeler: Elektronik imza, dijital imza, elektronik, dokümantasyon, e-ticaret, elektronik işlem, elektronik bankacılık, Irak'taki hukuki düzenleme

ACKNOWLEDGMENTS

Today we fold the days' tiredness and the grand summing up between the cover of this humble work

I'm Grateful...

- ❖ To the spring that never stops giving, who weaves my happiness with strings from her merciful heart, to my mother...
- ❖ To the soul of my lovely aunt, who inspired me in every step, encouraged me to be the best of the best, Rest in Peace ...
- ❖ To him, whom he strives to bless comfort and shelter and never stints what he owns to push me in the success way who taught me to promote life stairs wisely and patiently, to my dearest father ...
- ❖ To those whose love flows in my veins and my heart always remembers them, to my sisters and niece ...

I'm Thankful...

- ❖ To all supporters and leaders who guided me to step forward, my teachers and supervisors. And never forget the obvious efforts shown by DR. DERYA AYDIN OKUR to and the efficient explanation regarding the concepts, guidelines and the full requirements in compliance with East Near University standards and rules.

TABLE OF CONTENTS

ABSTRACT	i
ÖZET	ii
ACKNOWLEDGMENT	iii
INTRODUCTION.....	1
The Topic Highlight	2
The Study Objective.....	2
The Research Difficulties.....	3
The Scope Of The Research	3
The Theoretical Framework Of The Topic	4
Methodology	4
CHAPETR ONE: DEFINITION OF ELECTRONIC SIGNATURE	5
1.1 Electronic Signature Definition:	5
1.2 Definition of Electronic Signature by International Organizations	6
1.3 Definition of Electronic Signature in UNCITRAL Uniform Laws for Electronic Signatures	6
1.4 Definition of Electronic Signature in European Union Directives	6
1.4.1 Electronic Signature	7
1.4.2 Improved Electronic Signature	7
1.5 Definition of Electronic Signature in International Legislation.....	8
1.6 Definition of Electronic Signature in American Law	9
1.7 Definition of Electronic Signature in the Laws of France	10
1.8 Electronic Signature in Arab Legislations	12
1.8.1 Definition of Electronic Signature in Egyptian Law.....	12
1.8.2 Definition of Electronic Signature in Jordanian Law	13
1.9 Definition of Electronic Signature in Law Statutes	14
1.10 Definition of Electronic Signature in Iraqi Law	14

1.11 Forms of Electronic Signature	16
1.11.1 Biometric Signature	16
1.11.2 Dynamic Electronic Signature in Direct (Domestic) Bank.....	17
1.11.3 Manual Electronic Signature (with Letters)	17
1.11.4 Electronic Pen Signature	18
1.12 Software Accuracy	19
1.13 Signature with Plastic Cards using Pin Number	19
1.14 Digital Signature	20
1.14.1 Digital Signature Definition.....	20
1.14.2 Reliability of Digital Signature	21
1.14.3 Advantages of Digital Signature	22
CHAPTER TWO: ELECTRONIC SIGNATURE APPLICATIONS	23
2.1 Plastic (Magnetic) Cards	23
2.2 Types of Plastic Cards.....	23
2.3 Credit Cards	24
2.4 Charge Card	24
2.5 Debit Card	24
2.6 ATM Card	24
2.7 Secured Credit Card	25
2.8 Smart Cards	25
2.9 Electronic Signature in Plastic Cards	26
2.10 Electronic Check	26
2.11 Electronic Shipping Document	28

2.12 Electronic Signature in Modern Communication Devices.....	30
2.12.1 Telex.....	30
2.12.2 Internet	32
Internet Divisions	32
1. World Wide Web	32
2. Electronic Mail.....	33
3. Chat Rooms.....	33
2.12.2.1 Electronic signature can be performed through the Internet.....	33
2.12.2.2 Electronic Signature in the Internet.....	34
CHAPTER THREE: HOW ELECTRONIC SIGNATURE MEETS SIGNATURE’S FUNCTION	35
3.1 Consideration of Electronic Signature as one of Signature Types.....	35
3.2 Consideration of Electronic Signature as a Typical Signature.....	35
3.3 Consideration of Electronic Signature as Fingerprint.....	36
3.4 Consideration of Electronic Signature as Fingerprint.....	36
3.5 Consideration of Electronic Signature as Seal	37
3.6 Fulfillment of Electronic Signature Conditions	38
1- Signature must be the sign of a particular person	38
2- Signature should be clear and permanent	39
3- The policy should be connected to the Signature	39
3.7 Electronic Signature and Signature Functions	40
1. Electronic signature should identify the client’s identity.....	40
2. Electronic signature should Express the client's approval to the policy contents	41

3.8 Authenticating Electronic Signature	42
CHAPTER FOUR: INTERNATIONAL USE OF ELECTRONIC SIGNATURE ON A DOCUMENT PART 1	45
Background	46
4.1 Forms of Electronic Signatures	46
4.2 The methods of executing electronic signature.....	47
4.3 Other Consideration	48
4.4 Electronically Signed Document and Originality	50
CHAPTER FOUR: UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001) PART 2	51
4.2.1 Definitions For the purposes of electronic Law	51
4.2.2 Background	52
4.2.3 Signatory Conduction	53
4.2.4 Recognition of Foreign Certificates and Electronic Signatures	53
CONCLUSION	55
RECOMMENDATION	57
BIBLIOGRAPHY	59
LEGISLATION	59
BOOKS	59
WEBSITES REFERENCES	64
ARTICLES	66

LIST OF ABBREVIATIONS

TLR: Texts of Laws and Regulations

CMI: Committee Maritime International

UNCITRAL: United Nations Commission on International Trade Law

HIT: Hachage Irreversible Technique

DES: Dynamic Electronic Signature

EDI: Electronic Data Interchange

PIN: Personal Identification Number

EU: European Union

eIDAS: EU regulation on electronic identification and trust services for electronic transactions in the internal market

SWIFT: Society for Worldwide Interbank Financial Telecommunication

WWW: World Wide Web

ATM: Automated Teller Machine

P.:Page

INTRODUCTION

Revolution in communications and technology development as well as the use of computer and internet has led to a major development in trading and e-commerce. This has also contributed to the wide use of electronic signature in electronic contracts concluded on the internet. Recently, electronic signature has become an alternative to traditional handwritten signature to comply with the nature of the legal acts and contracts that are made using modern technology. Electronic signature is characterized by some special features which makes it significantly different from the traditional signature. The Rapid growth and development in communications and information systems meant that the rules guiding internet based transactions have to be different from the rules of traditional trade. This is because there are differences in the nature and way that they are executed. Legal concepts like writing, editing and signature have witnessed some changes due to technological development and advancement in the communication industry. This technological advancement has also increase the ease of doing business across the world. The proliferation of electronic contracts and international trade led legislators to establish rules that ensure dealers recognition during the exchange of information so that business partners are able to identify and know the identity of a transacting party in order to prevent disclosure of their secrets to fraudsters in electronic contracts. As a result, electronic signature was found as substitute for normal collateral signature to verify the identity of the contractors, though this concept lead to doctrinal differences among scholars and judges, especially for the issuance of e-laws. The thesis examines the difficulty of issuing of a formal judicial proceedings using traditional electronic signature on paper struts to improve the judicial procedure and the extent of use of the electronic pillars liberated by the electronic writing for the completion of the various issues without having to undergo nullity of them.

In addition to the relationship between the study and the modern technical concepts that use the internet and computers in the judicial procedures which constitutes an obstacle to take advantage of them and generates doubts in their ability to cope with modern scientific developments in the field of judicial proceedings considering the fact that the implementation of such methods was rare in most of Arab countries. Accordingly, we will discuss about the electronic signature, its properties, advantages and disadvantages. Chapter two discusses the images of electronic signature and its protection mechanisms. Chapter three discusses the conditions that prove the legislation of electronic signature and evidences. And finally, the last chapter discusses the national and international resolutions and recommendations.

- **The Topic Highlight:**

This thesis highlights as well, the several processes were taken for the acceptance of electronic signature as a formal requirement of judicial proceedings and how it can carry out its numerous functions and what its position is in modern laws.

- **The Study Objective:**

The thesis attempts to keep pace with technological evolution in the judicial framework to define the electronic signature in contractual and various judicial proc and determine its properties, besides showing the legal rules which include the exercise of these measures through the electronic systems and comparative legislations. It attempts to justify the use of technology in the judicial scale in the availability of legal texts and framing theory leading the future legislative steps that has to be implemented if the legislature will be moving toward absorbing these technological developments in the context of the various legal actions. This depends on the analytical study of the Texts of Laws and Regulations (TLR) with the comparison of relevant scientific references. Additionally, it deals with electronic signature, its characteristics and its proof in international efforts and comparative legislation. Chapter one discusses the electronic signature by giving its general overview and the importance of considering the electronic signatures in business systems.

It also looks at how its structure is created in compliance with electronic signature elements and techniques. Chapter two and three discuss the electronic signature applications, functions and requirements and fulfillment. Finally, the study examined the international use of the electronic signatures and the Act of UNCITRAL Model Law on Electronic Signatures (2001).

- **The Research Difficulties:**

The difficulty of this research is in its relative modernity on both legal and judiciary levels in Kurdistan Region of Iraq. Electronic signature is equally a recent phenomenon in many of the other Arab countries. The use of electronic signature remains a limited resource used in the field of legal studies related to contracts and e-commerce and the scarcity of decisions and judicial applications to them. In the first point of view, the limited resources could be as a result of the following:

- The lack of experience in adapting the electronic signature in large corporate enterprises,
- The limited scope of using the electronic signature in public sectors and Banks,
- The importance of using technology base methods in documentation and different procedures,

- **The Scope of the Research:**

Mainly, this research highlights Electronic transactions and the e-signatures along with their usage in the common place of business agreements. The importance of these electronic transactions is seen in real estate contracts and banks contracts that are increasingly being implemented electronically due to the efficiencies involved in paperless transactions. Secondly, this study shall emphasize on the usage of the electronic signatures on legal transactions and discuss the advantages and the disadvantages of the electronic signatures in business documentations.

- **The Theoretical Framework of the Study:**

Generally, the electronic system must ensure that the information received is the information sent; this is to secure the information carried out accordingly. The electronic system does record and document all occasions of the transactions data that result in a certain task. Hence, the design and the operation of the electronic system, including legal and corporate procedures, should make it reasonably certain that the person accessing the system and filing any document is confirmed electronically.

- **Methodology:**

Electronic signatures may be implemented using various methodologies depending on the below:

- Risks and threats related to the transaction speed,
- The quality and security of the electronic signature method shall be commensurate with the risk and required assurance of the authenticity of the signer.
- The plan of the thesis is summarized as per the introduction of electronic signature, functions, applications and requirements. The e-signature methodology shall be commensurate to the assurances needed for the risks identified.
- The Specifications for recording, documenting, auditing the electronic signature as required for non-repudiation and other legal requirements shall also be determined by the unit/ document.

CHAPTER ONE: DEFINITION OF ELECTRONIC SIGNATURE

1.1 Electronic Signature Definition:

The Discussion in this chapter shall be about the definition of electronic signature that has arisen because of the use of computer in transactions between individuals and institutions. The use of telex and the internet has equally brought a huge revolution in the field of information and communication technology, which inevitably affected the nature and speed of interaction between individuals. This has effectively made it possible for individuals to communicate and exchange information digitally. The development and widespread use of the internet has led the trend towards electronic signatures and because the signing in its regular known forms, does not find a place within the spread of electronic processing systems. So, it becomes necessary to find alternatives to traditional signature system that can perform the same functions on one hand and adapt to the modern electronic administration on the other hand. First alternative was Personal Identification Number (PIN) and then the digital signature, which contributed to the spread of e-commerce on a large scale. We will define the electronic signature through¹ the definitions that have been developed by international organizations first and then through the definitions of international and national legislation, which recognized electronic signature and then the definition developed by some Arab countries including Jordan and finally, through jurists interpretations that have been mentioned in the definition of electronic signature.²

¹ Law No. 15 of the year 2004 regulating Electronic Signature and establishing the Information Technology Industry Development Agency; And presidential decree No. 201 of the year 2004 forming the cabinet of ministers,

2) Nasiryat Alaa Eid "*The Authority of Electronic Signature in Evidance A Compative Study*", a research submitted in AL Bait Al Gharaa University, November 2005, p.22.

1.2 Definition of Electronic Signature by International Organizations:

Many organizations tried to define the electronic signature through electronic trade laws or through laws specifically formulated for electronic signature. Our focus in this chapter is on two international organizations that placed a definition of electronic signature, the United Nations organization through the United Nations for International Trade known as “UNCITRAL” and the European Union as an example of a Regional Organization.

1.3 Definition of Electronic Signature in UNCITRAL Uniform Laws for Electronic Signatures:

United Nations Commission of Electronic Commerce “UNCITRAL” has put the following rules:

1. No limitations of how to use Electronic Signatures, which helps in opening the way to any method a countries may find appropriate and suitable to use by encoding or encryption or any other method.
2. The definition emphasizes that any method used for signing should comply with the functions of the signature in determining the identity of the person signing and the expression of his will to agree on the contract's contents.

1.4 Definition of Electronic Signature in European Union Directives: In 1999, the European Commission published its first electronic signature directive³ rather than a regulation. It allowed the EU member states to interpret the new law and impose and effect its provisions based on their restrictions and expectations to it. In 2011, the commission decided to fix these gaps and develop a European digital market, as it conducted a review of electronic signature laws in a member states. The new regulation was adopted in 2014, considering that the key goals were to ensure confidence in electronic signatures and create mutual recognition of electronic signature.

³Overview Of The Electronic Signature Law In The EU". 2017.
<https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/overview-of-electronic-signature-law-in-the-EU.pdf>. [Accessed 20 Mar. 2017].

European Union defines two types of Electronic Signatures:

1.4.1 Electronic Signature is defined as information electronically formed and related to other electronic information using a documenting tool.

1.4.2. Improved Electronic Signature is an electronic signature which is required to be:

- Uniquely linked to the person who signed originally.
- Able to identify the person who made the signature.
- Found using sources which ensures strict confidentiality.
- Linked to the contract contents and can detect any change in the information.

This directive is binding on EU countries and there will be a dual system of electronic signature, regular and advanced. Advanced signature has all the advantages that the traditional signature has, while regular signature is normally less than advanced in terms of legal authenticity in proof. The definition of regular electronic signature⁴ looks like the definition of UNCITRAL.⁵

The eIDAS defined three types of electronic signatures:

- **Basic Electronic Signature:** it is established under the eIDAS Regulation. The same fundamental standard – as the electronic signature shall not be ignored or denied legal effect and admissibility as evidence in legal proceedings solely depend on the fact that the electronic signature is still the rule.

⁴ Sinisi,Vinzenzo, Digital Signature Legislation in Europe, International Business Lawyer, Dec 2000, vol 28, No 11, p. 487

⁵ Sinisi,Vinzenzo Ibid, p. 488, 2000

- **Advanced Electronic Signatures:** the eIDAS⁶ Regulation defines the electronic signature as opposed to the electronic signature that is in place under the current directive – allows unique definition and authentication of the document signer and enables the verification of the integrity of the electronically signed agreement.
- **Qualified Electronic Signatures:** the final type of signature defines in the eIDAS Regulation is the Qualified Electronic Signature (QES). The advanced and the qualified electronic signatures are strongly connected to the signer, as the QES is based on the qualified certificates and verifications.

As at July, 2016, the European Commission was still finalizing a few details before the eIDAS Regulation becomes effective. Taking into account, that it is important for any business to be aware of how the new regulation shall modify the electronic signature law in the EU, QES should figure prominently in any EU Operational plan in the future.

1.5 Definition of Electronic Signature in International Legislations:⁷

This section will explain how the United States of America defines Electronic Signature in which two laws were approved for this purpose to regulate the use of electronic signatures in transactions. United States was taken as an example since it has been one of the most famous countries that use information technology in various fields. France, on the other hand, has amended its laws to regulate the law governing the use of electronic signatures. France will be taken as an example of the European Orientation in this field.

6 Overview Of The Electronic Signature Law In The EU". 2017.
<https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/overview-of-electronic-signature-law-in-the-EU.pdf>. [Accessed 20 Mar. 2017]. [Accessed 22 April 2016]

7 <http://portal.etsi.org/esi/el-sign.asp>; The ETSI Electronic Signatures Workgroup issued also a technical specification for XML advanced electronic signatures (XAdES), <http://tinyurl.com/2v9bsh> [Online] [Accessed 20 Mar. 2017]

1.6 Definition of Electronic Signature in American Law:

Electronic Signature received a great share of the legislative regulation⁸ at both the federal union level or at the state union level. Here we will take the definition of electronic signature on federal level in which two definitions of electronic signature were declared. The definition to be considered is in federal law for electronic signature while the second is in the Uniform Electronic Transactions law. The second law defines it as a symbol or procedure that comes in electronic form logically connected to another document that is issued from the person who will sign that document. While the first law defines it in article (8/102) as the signature that comes in electronic form and connected to electronic document.

We can see the following definitions in American Federal Union:

- 1) The definition has mentioned some of the electronic signature types as an example but not limited. It mentioned voices and symbols, and open the way for any other means located in an electronic format to be able to achieve the electronic signature requirements and then recognize it as a valid signature.
- 2) The definition didn't require to be physically linked to the record that was signed in already, but logically linked as in electronic form⁹, which is the opposite to the case of handwriting signature that is linked directly to writing.
- 3) The definition also states that the implementation process of signing by contractors is not the handwriting method of signing, which was required by legislations so it would only mention the implementation process in any way it can happen.

⁸ Hu, Wensong "Advances in electric and electronics" 1st ed. Berlin: Springer (2012), p.6-20.

⁹ H. Abelson, Fischer, M., Weitzner, D., Perelman, L., and Unger, D., "Ethics and Law on the Electronic Frontier". Massachusetts Institute of Technology, 2010., p 22-28

- 4) The definition considered the implementation of the electronic signature as the intention of signing the record, meaning, it provides the signature without explicitly disclosing all the signature functions and since the word “signature” include the identification of the contractor and express his will.

Uniform Electronic Transactions law’s definition states the following:

- 1) The definition didn’t specify any types of signatures but stated only that it should be in electronic form which is the opposite of federal law that gives some types of signature which considered the best in this field since it gives the chance to state all different types of electronic signatures that comply with the signature functions.
- 2) The definition obliged that the signature should be linked to electronic record only since it is not acceptable to use electronic signature that is linked to a regular record. Electronic record as per the American laws definition is any contract or record that has been used or saved using electronic means which the electronic signature should be linked to.

1.7 Definition of Electronic Signature in the Laws of France:

The French view on the electronic signatures¹⁰ recognition of problems focuses on a different aspect. From the French law perspective in the EU context, the crucial question is: is it possible for one EU jurisdiction or a competent court to recognize the validity of a certified signature, and another one to refuse such recognition? The huge development of electronic commerce in France and its commitment to the European directives to define electronic signature give the French legislator the task of amending the provisions of the special civil law proof (13 /3/2000) and a report has been issued by the French Council of State based on the mandate from the French government in which the focus was on the functions of the signature known in the art.

¹⁰ EUR-Lex - L24118 - EN - EUR-Lex". 2017. Eur-Lex.Europa.Eu. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24118>. [Accessed 20 Mar. 2017].

(4 /1316) of the Civil French Law after amending which states that “It is the signature that defines the identity of the person who did the signature that shows the acceptance to its contents and all the commitments mentioned there”. The French legislature has adopted this definition to be a general definition of signature¹¹. As for electronic signature, the legislature defined it in the second paragraph of the amendment as “the signature that comes out of using any acceptable and reliable means to determine the identity of the contractors and ensure the signature’s connection to the associated document¹². The following observations can be made and considered on the French legislation:

1. The French legislature defined electronic signature generally and functionally allowing widening its scope to include electronic signatures, along with linear countersign considering that each signature complies with the signature’s functions is worth to be recognized.
2. The French definition did not specify the way these signatures are created, but puts a very important condition that this way should be reliable. As in the perspective of people who deal with technologies, this condition is very important to recognize the electronic signature on the basis that any way used in signature should be reliable and precise. The assessment eventually depends on people specialized in electronics and to legislators as well.
3. The legislature stipulated that the way to make the signature should be related to the document associated with it because unlike a manual signature on papers, the communication availability cannot be assumed so a specific way should be provided to achieve this communication.

¹¹ Tunisia, Loi relative aux échanges et au commerce électroniques, article 18; and Viet Nam, Law on Electronic Transactions, article 31 (d), 2002 p.67 - 76

¹² “*Online Services, including E-Commerce in the Single Market*”, Accompanying Document COM (2011) 942, SEC (2011) 1641 final, Commission Staff Working Document, “A Coherent Framework to boost Confidence in the Digital Single Market of E-commerce and other online services”, 11.1.2012, p. 8.

1.8 Electronic Signature in Arab Legislations: The definition of electronic signature in Egyptian legislation will be discussed due to the wide experience of the Egyptian legislature in legal legislation. Jordanian Electronic Transaction Law will equally be looked into due to its importance in shedding light on Arab legislations on electronic signature.

1.8.1 Definition of Electronic Signature in Egyptian Law:

AHRAM Economic Magazine published in its edition (1679) in March 2001 Egyptian e-commerce law draft in which it defined the electronic signature in the first chapter of the project in the first article as follows: "electronic signature is a letters, numbers, symbols or signals that have a unique character that allows the identification of the contractor who signed the documents"¹³. Through this definition, we can see the following:

1. This definition mentioned all the different shapes and forms that form the electronic signature can take which could be either numbers, words, symbols or signals.
2. The legislature stipulated that the E-signature components should be unique to assure privacy of the signature and prevent using it by someone else in a different document.
3. The legislature stipulated the uniqueness condition to identify the identity of the contractor as one of the signature functions but didn't come through the other function which is the approval of the contractors to the documents contents assuming that the signature itself confirms the approval to the contents though it would be better if there was direct law to state that.

¹³ Boss A.H., and Kilian W. (eds.), the United Nations Convention on the Use of Electronic Communications in International Contracts: An In-Depth Guide and Sourcebook (2008) – p. 1-16

1.8.2 Definition of Electronic Signature in Jordanian Law:

E-signature definition was mentioned in Jordanian temporary electronic transaction law no. 85/2001 in the 2nd art¹⁴. As follows “group of data that comes as letters, numbers, signals or symbols combined in electronic, digital or optic form or any other form that can be used in sending information connected directly to the documents and capable of identifying the contractor’s identity to approve its contents”.¹⁵ We can observe the following from this definition:

1. The definition mentioned different shapes that the signature data may take like numbers, signals or letters without limiting it to one type or shape.
2. The definition stipulated that these data should be displayed in electronic form.
3. The definition stipulated that these data should be listed within the information letter which is group of information have been formed or transmitted using electronic means like E-mail, Telex or Telecopies¹⁶.
4. The definition stipulated that these data can identify the contractor’s identity and connect it to the information letter to insure the contractor’s approval.

¹⁴ Regulation no (13) for the year 2001 Regulation for Registration and Licensing of Enterprises in the Aqaba Special Economic Zone Law

¹⁵ Alhussban, N. (n.d.). Admissibility Of Electronic Signature In Evidence And Its Legal Effect. 1st ed. 2011 p.13-22.

¹⁶ Hassan Abdulbaset Jamee Proof of legal laws, p35

1.9 Definition of Electronic Signature in Law Statutes: Jurisprudence defines the electronic signature as "the signature that is based on different procedures and means that can form electronic letter using numbers or symbols and marked the author with a unique sign. The mentioned letter will be electronically transmitted and encrypted using special codes on them, is known and the other one is private¹⁷. The following important points are noticed from this definition:

1. The definition focused mainly on the means which is used to form the signature like codes and numbers.
2. The definition highlights the outcome of using the means mentioned above which is the electronic letter that has a significant mark to the person who wrote it already that is electronic signature¹⁸.
3. The definition focused on digital signature which is one of the electronic signature types that is based on coding both private and public codes.

1.10 Definition of Electronic Signature according to the Iraqi Legislature:

According to the Iraqi legislation of **Electronic Signature – Article 78 Year 2012**

- Personal sign form of letters, numbers or symbols or sounds, which has unique characters or codes indicate the value of its location in document and is reliable and certified by the person¹⁹.

¹⁷ Ahmad Sharaf Eldeen, "*Electronic Signature, Regulations And Reliability In Electronic Commerce*", a paper submitted to electronic commerce conference, Cairo, November 2000, p3

¹⁸ Stephen E. Blythe, "The Barbados Electronic Transactions Act: A Comparison with the U.S. Model Statute," 16 CARIBBEAN LAW REVIEW (2011). p. 1-35

¹⁹ Al-Rashid, S. Electronic signature in electronic contract in Iraqi legislations. 1st ed. pp.30-38. (2013).

- The term “Electronic Signature” means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. There is another definition for electronic signature that is “the combination of technical procedures that identify the identity of the person who signed that documents and approve this identity based on the circumstance that lead to that signature”. We note on this definition as follows:
1. The definition did not specify types of electronic signatures, but merely saying that it’s the combination of technical procedures (electronic) which make sense as it is unnecessary to mention the forms of electronic signature, rather than that, it will be more reliable to say that electronic signature is the combination of technical procedures that allow the recognition of any other technical method that are efficient and capable to achieve the objectives of electronic signature safely without specifying codes or symbols required to use that which makes the definition more flexible to any future development in technical field. The definition shows the most prominent function of electronic signature, which must need the recognized technical measures, that is to determine the identity of the person and express his will to approve the content of the bond, which was already signed.
 2. Therefore, we believe that this inclusive, adequate definition meet the requirements of electronic signature, leaving the details of electronic signature types and how to identify the person’s identity to the executive regulations established by the competent authority²⁰. For all the earlier mentioned definitions, this particular definition will be critically examined and discussed in more details.

²⁰ Stephen E. Blythe, “*A Critique of India’s Information Technology Act and Recommendations for Improvement*,” 34 SYRACUSE JOURNAL OF INTERNATIONAL LAW AND COMMERCE 1 (2006),

1.11 Forms of Electronic Signature: When discussing about the electronic signature that does not mean to talk about signatures which are taking one form. As traditional signature may have several forms, the electronic signature also has different forms all have the same common factor of using modern techniques that can transfer some of the person's characteristics like numbers and letters to group of data uniquely used by him for signing documents and contracts electronically.

1.11.1 Biometric Signature: This signature is made by using one of the person's intrinsic (iris, hand print, lips or sound prints)²¹ that are compressed and stored digitally so as not to possess a large space inside computer's memory. The client can use this print by inserting a card into the ATM (Automated Teller Machine) then comparing that print on the card with the one saved in computer²².

How reliable is this signature?

The use of this signature encourages the science to study the attributes of each person and then study the outer appearance characteristics as well and comparing between each of them to identify the signature. The studies show the reliability of these characteristics to identify persons and allow using them in ATM and Internet.

Although these qualities are susceptible to fraud by recording new audio or paint the fingers to make matching fingerprint or change lip coating, or even by manually making contact lenses like the iris, which calls to say that fraud can be assigned to scientific development, but this cannot prevent the use of these means, as the relevant experts can uncover fraud and forgery, which is not the case in traditional signature. This quality recognizes this signature as a legislatively reliable method to be used in signing electronic document.

²¹ Pirlo, G., Impedovo, D. and Fairhurst, M. (2014) *Advances In Digital Handwritten Signature Processing*. 1st ed. Singapore: World Scientific Pub. Co., p.55-60.

²² Hazem Alsamadi - *Authentic Of Electronic Signature, Electronic Trade And Banking Services Through Internet* Al Monsif Quortas, Beirut 2000, bank responsibilities in electronic commerce, December 2000,p 11

1.11.2 Dynamic Electronic Signature (DES) in Direct (Domestic) Bank

Direct bank is where the customer can complete his banking activities from home or work or any other place using his computer to make payments and get summary of his account as well. So how does the signing process look like in this case? Customer signs orders using small device no larger than the bank card, which has a microprocessor with algebraic function that generates a secret code as an improbability dynamically almost every minute and in sync with the system of direct bank²³ (home) where it is impossible to be stolen since this symbol is continuously variable. If the client wants to sign and issue his orders he must enter the number that appears on the screen at the time. This machine is sealed and secured and any attempt to undermine the integrity will disable it. The client can use this technique by signing a contract²⁴ with the bank and approving using it wherever needed.

1.11.3 Manual Electronic Signature (with Letters)

This signature is based on adding one key panel to the one existing on the network (MAC / Windows). Each plate has special key letters and one of these keys has the client's signature manually inserted and protected by a password to be used when needed. This technique is preferable to be used in networks like (Internet, Extranet) because they are safer than the Internet and the traders know each other in general. Signature can be transferred using scanner and then transfer the image to a file that is intended to be used to save the signature. This technique is not that much reliable though since anyone can have a copy of that image and can paste it to any other document.²⁵

²³ Jonathan E. Stern, Note, "*Federal Legislation: The Electronic Signatures in Global and National Commerce Act*," 16 BERKELEY TECHNOLOGY LAW JOURNAL 391, 395 (2001).

²⁴ Contract through communications and authentic in civil proof, Amman 1997,p.260

²⁵ Almonsef Quortas, *Authenticof Electronic Signature*, p.236,237 year 2014

1.11.4 Electronic Pen Signature: This technique uses a sensitive pen which can write on computer screen using special software designed for this purpose²⁶. The following are the steps explaining how this technique works:

1. The software will scan the signature using any digital key and pen and save all the data required for the process.
2. The software saves the signature and all the required data using coding algorithm.
3. The saved signature will be used by the client any time needed using a combination of codes known only by the client himself to prevent any fraud.
4. The signature will be tested for accuracy using a comparison program that compare the input signature with the one saved already in the computer. This comparison is based on different biological characteristics like (directional rays, pen position on the keypad, writing speed, pen pressure on the pad, relative time differences and writing directions coordinated both negative and positive). The accuracy can be within the range of (1-100) % depending on the importance of the document.
5. If the program catches any suspicious action to open the file, a warning message will be shown in the system.

Hence, this signature meets two goals:

- 1- Scanning the signature using the provided pen.
- 2- Checking the signature accuracy by comparing the saved and input signatures²⁷.

²⁶ Lopenzina, D. (2012). Red ink. 1st ed. Albany: State University of New York Press, pp.60-78.

²⁷ Aith Elmri E-sign, Pc magazine, February,2001,p.32 Authentic of Technology, p.113

1.13 Software Accuracy: ADAPTE Software Solutions Company has established a signature using a program called (My e- sign) that offers solutions for all the necessary options (previously mentioned). First the program asks to input the signature six times then using “Artificial Intelligence Algorithm” to study all the possibilities to identify the signature. Signature input possibilities were changed using different input possibilities like signing in different speed or pressing the keypad in a different way or change the direction of the pen. Every time the software will send a warning message since the input signature does not match the one already saved in the system.

1.14 Signature with Plastic Cards using Pin Number: Plastic magnetic cards have been used widely in the field of transactions that are used in cash withdrawals through ATMs or by undertaking to pay for goods and services in shops by inserting the card in the dedicated device, as well as being used for payment via the Internet²⁸. The customer inserts these cards into the machine which recognizes the card and then asked him to enter his PIN number to make sure that the card holder is the person authorized to use the card allowing him to do what he needs to, be it withdrawals, deposit and other operations, as well as shopping using internet. The accuracy of this system lies in the fact that it includes a pin number distinct and unique to the client only, so if anyone tries to use the card knowing the PIN number, the client can call the bank and ask them to stop the card at any time.

²⁸ Almonsaf Qurtas *Secure Payment By Check Systems And The Possibility Of Lifting The Injection Character Of Checks Law*, Arabic Banks union magazine, issue 240, December 2000, p.70

1.14 Digital Signature: Digital Signature is one of the most popular signatures that have been all over the world due to its accuracy and high reliability²⁹. We will explain this signature type in more details as follows:

1.14.1 Definition of Digital Signature: Digital Signature is a private code or symbol the client created using special software that used special coding algorithm with public and private coding technique. The digital signature is based on the wide development in using Encryptions and Cryptography science. The encryption used in this signature has two types:

- ❖ **Symmetric Encryption:** This encryption is based on private code that is known to both parties and worked in isolated environment like Telex and plastic cards in which the code is known to both the client and the device only³⁰.
- ❖ **Asymmetric Encryption:** This encryption is based on using a pair of asymmetric keys³¹ (public key and a private key), first one will be known while the second one should be known to the client only. The owner of this key should have both public and private keys to be able to encrypt his message and read its content. This Encryption has a special feature that knows the public key doesn't necessarily mean to know the private key since each one is working in opposite direction to the other one. Here is an example to explain that.

²⁹ Stephen E. Blythe, “*The Electronic Transactions Ordinance As A Facilitator Of Growth For E-Commerce*,” 2:2 JOURNAL OF ISLAMIC STATE PRACTICES IN INTERNATIONAL LAW - (2006)

³⁰ Aith Elmri, *Authentic of Technology* ,p.97, year 1997

³¹ Ibid ,p.98, *Digital Signature Tutrial*, p 14-15

Examples:

Assume that “A” wants to receive a letter from “B”. ”A” will print public key so that “B” can read the message and keeping the private key at the same time. After writing the letter “B” will encrypt the letter using public key and encrypting software resulting in inapprehensible message.³² This message will be coding by the party having the private key of “A” and when “A” receives the message; it will use its private key and encryption software to read it. Assuming that “A” wants to send message to “B” and make sure “B” will receive it,” A” will send a special digital signature using the public key and encryption software. This signature is a combination of data in the message content. When “B” receives, the message, he will use the private key and encryption software to read it. As shown in this example. Digital signature is based on arithmetic equations that transform the ordinary signatures to codes and symbols that can only be read by the party that has the encrypting key (public and private).

1.14.2 Reliability of Digital Signature: The reliability of this signature will be discussed through the party that has the responsibility to check its accuracy. This can be done in two ways:

1. The receiver will check the message using the public key and encrypting software, if the result is the same that means the sender is the same person and the message is correct³³, if not that means the sender is not the same person and the message has error.
2. Documentation Authorities will give special digital certificates to their clients authorizing them to use these codes on the internet to protect the message contents. Such authorities have special domains and time frame. These certificates will be saved on line and their accuracy can be checked using public and private codes.

³² Hassan Abdul Basit Jumea Proof of Legal Contracts,p42

³³ Harralson, H. and Miller, L. (2015). *Developments In Handwriting And Signature Identification In The Digital Age*. 1st ed. London: Routledge, Taylor & Francis Group p. 41-52

1.14.3 Advantage of Digital Signature

1. Identifying the signature of the client: This signature achieves the identification of the client by using the public and private codes. No one can duplicate this identity only if it has the private code and if he loses it by mistake or through careless handling there are ways for it to be recovered. Through using hash function, the receiver can know that the sender is the same person no one else.
2. Message Documentation: this signature can save the message content and checkout its accuracy since it is based on public and private codes. The processing of signing and sending the message will be processed through Hash function to detect any change or duplication in the message³⁴.
3. Effectiveness: this signature is very effective and accurate as regarding identifying the client and the document contents. Even within the possibility of fraud or duplicate which can rarely happen compared to other signature types, it is still considered the safest and most reliable signature.

³⁴Aith Elmri, Authentic of Technology p99. Almonsef Quortas Authentic of Electronic Signature by,p239

CHAPTER TWO: ELECTRONIC SIGNATURE APPLICATIONS

The discussion is about the applications of the electronic signature and the fields that this signature can be used in. We will discuss in details three different applications that are: plastic (MAGNETIC) cards, electronic checks and electronic charging bonds and the applications of electronic signatures in modern communications devices like Telex and Internet. All these applications will organize the legal relationships between institutions and individuals.

2.1. Plastic (Magnetic) Cards:

Plastic cards have been widely used recently in banking and online transactions as a way of payment instead of using cash. These cards are basically depending on using pin number to complete the transaction³⁵. There are different types of these cards that will be discussed in details.

2.2. Types of Plastic Cards:

Withdrawal of money used to be done in banks manually in which the client will be personally shown up in the bank and sign a request to withdraw money so the bank will have proof of the transaction. Nowadays with all the development that has happened in technology and the constantly pressure on banks, the banks tend to use more simplified ways to do transactions like the use of ATM cards. There are different types of these cards which will be discussed as follows.

³⁵ Stašelytė, N., Šešok, N. and Iljin, I. (2014) *Investigation into Plastic Cards*. Science – Future of Lithuania, 6(6), pp.598-602.

2.3. Credit Cards:

This card is issued to the client by the bank and provided him a credit line that can be used to do all his shopping online and pay later on monthly basis³⁶. If the agent could not pay back for any reason, he can rotate the payment or part of it to be paid later with adding interest rate on his credit. These cards can be used in online shopping and have different types like Visa, Discover and Master Card³⁷.

2.4. Charge Card:

This card allows the consumer to use the money in his transactions and pay later without credit line, which means the consumer has to pay as soon as he gets the bill from the source without any additional interest rate.

2.5. Debit Card:

This card allows the client to do his transactions using his checking account in the bank. That means during the buying process, the money will be transferred from the agent's account directly to the buyer. If the card is online, the transfer will be daily if the card is offline the transfer will be scheduled on different days.³⁸

2.6. ATM Card:

The agent can use³⁹ this card in the reliable websites and the networks connected with them including the different banks dealing with them. The agent can do different transactions like withdraw, deposit, bills payment and money transfer as well. These types of cards have been used widely in different banks around the world.

³⁶ Credit cards 1st ed. London: Mintel International Group Ltd. (2005).

³⁷ Hussam Elabd *Fraud And Duplicate Plastic Cards*, Banks magazine in Jordan, 5th issue, June 2nd 1999. Khlaid Al Rawi Banking transactions by, Jordan, p.30

³⁸ Bâtiz-Lazo, B. and Hacialioglu, N. (2005) Barclaycard: still the King of Plastic? In: Exploring Corporate Strategy: Text and Cases, G. Johnson, K. Scholes and R. Whittington (EDS) 7th edition, London: Prentice Hall/Financial Times, pp. 886-900

³⁹ Alvarez, F. & F. Lippi (2009). '*Financial Innovation And The Transaction Demand For Cash.*' E- conometrica 77(2): 363-402.

2.7. Secured Credit Card:

These cards are guaranteed with saving deposit with interest rate to guarantee the credit line provided for the agent⁴⁰. This card is mainly issued to the agents who have no credit score in their history to help them do their transactions as if they have credit cards.

2.8. Smart Card:

This card is one of the most important plastic cards used nowadays. These cards are provided with smart chip called (Microprocessor PUCE) that is mainly a small computer not bigger than the size of the finger nail and it can be programmed to do specific functions. These computers are programmed by specialized companies to enter the client's information like his name, his job, and information about his companies to the memory of the smart chip. The programmer will use algebraic function to generate pin number. Whenever the client is using the card, the computer will compare the pin number the client entered with the one saved in the memory, if they match then the client can use the card by passing a security check (fingerprint, signature, personal code, etc)⁴¹. If there is no matching, the computer will give the agent three trials to enter the correct pin number. If the client could not enter the correct pin number, the microprocessor will automatically send a signal to disable the card. This card is considered as one of the most reliable cards in the world. The Credit Card Committee - (Cartes Bancaires) located in France declared that the fraud and duplicating incidents decreased to 50% since using these cards began. These cards are used to enter the internet as well. As an example, CITIBANK used these cards to help their clients to enter Home Bank Network as well as in different fields.⁴²

⁴⁰ Bolt, W., D. Humphrey & R. Uittenbogaard (2008). 'Transaction pricing and the adoption of electronic payments: a cross-country comparison.' *International Journal of Central Banking* 4(1): 89-123

⁴¹ ISO/IEC 24727, *Identification Cards -- Integrated Circuit Card Programming Interfaces. Part Architecture*, ISO, 2007. Part 2- Generic card interface, ISO, 2008. Part 3- Application interface, ISO 2008.

⁴² Khlaid Alrawi *Banking Transactions*, p.31. Mohammad Zahra, *electronic signature proof*, p.19.

2.9. Electronic Signature in Plastic Cards:

All the plastic cards have common feature, that is, using the pin number according to the application required. This can be done as follows:

1. Inserting the card which has mainly the client's information in the designated machine.
2. Writing the pin number.
3. Giving the proper instruction and pressing the designated key to complete the transaction.

The pin number is a special code used to define and sign the banking transactions on computer without printing them out on papers. These numbers will be sent to electronic processors inside the bank computer so the bank will have a record of all income and outcome on long term. The banks are using smart cards along with the pin number to sign payment order of the clients through the largest network (SWIFT) that connects 90% of the banks worldwide⁴³.

2.10. Electronic Check:

Bank check is considered one of the most important paper documents used in banking transactions.⁴⁴ The Jordanian Law defines it as "a written document that is subjected to special conditions which includes instruction from the client to the bank to pay a third party a specific amount of money as soon as the check is reviewed". To confirm the check authenticity, the client has to sign the check or use his fingerprint. In case of using fingerprint, there should be two witnesses at the time of signing to confirm the client has already reviewed the check contents. Today it is possible to issue electronic check and sign them without using any printers or papers. Since the check is seen as a very important loyalty tool, it is absolutely necessary to check the client's signature on the check.

⁴³ Almonsaf Quortas Electronic Signature Proof, p.32. Ibid., David Kosiur Ibid (5), p.71, Understanding Electronic Commerce, p.51

⁴⁴ Almonsaf Quortas Electronic Signature proof, p.30. Almonsaf Quortas Legal sides of Electronic Cards and legal effects of using computers in Banks, Beriut, 1999 p.177-178.

This is considered nowadays a big obstacle especially to the banks to complete all the transactions in a fast and accurate way. This has caused many banks around the world to issue electronic checks. This action started first in France and the USA to solve the state safety problem of issuing more than 400 checks to pay the federal administration's expenses or social services costs. Electronic checks have many advantages like:

1. Replacing the paper check book with an electronic one which the client can get from the bank through the internet safely and accurately. Both paper and electronic check books do the same function⁴⁵.
2. All the checks are cashed electronically in different transactions like commercial or administrative and attached with electronic receipt which the client can receive it to his e-mail.
3. Electronic checks are subjected to the same legal framework of paper checks. The most important questions to be answered is; how will the electronic checks be signed? And how can this signature be checked? Electronic checks are signed through electronic signatures which are based on public keys infrastructure along with the pin code and smart cards which help to save private codes and electronic certificate, so the client can use that private code to sign the electronic check.

Electronic signature (Pin Code) verification is accomplished by electronic comparison. Electronic signatures verifications have the same standards of the paper checks verification except what is related to physical characteristics. The employee that is responsible to verify electronic check has to insert the check into special machine that decodes all the Electronic codes and symbols inside the checks in a short time comparing to verify paper checks. Verification of electronic signatures in electronic checks used in Internet network is usually done by using Publicity Authority (Documentation) that verify both the client and his signature.

⁴⁵ Vagner Schoaba, Felipe Eduardo Gomes, Luiz Castelo Branco, Digital signature has same value as the physical signature on paper 2011, p.23-36

Electronic checks are used widely worldwide to reduce the problems that may happen if using paper checks like fraud, duplication, and theft. Despite all the advantages of electronic checks over paper checks, electronic checks still cannot be used instead of paper checks within a short time.

These types of checks may be used in states administrative interests or within companies and people that are authorized to use modern information technology. The US government used electronic checks for the first time to sign a contract of \$22,000 for one of their companies. This process proved the reliability of using electronic checks that depends on using digital signature⁴⁶. Jordanian electronic transactions law approved electronic checks, Art. (19/C) states that “Art. (20/21/23/24) will not apply to electronic checks only with the central bank approval that put the instructions to use these checks”. This approval is necessary to approve using electronic checks in commercial transactions and deals and accomplish them safely and accurately within a short time compared to the use paper checks.

2.11 Electronic Shipping Document:

This document is very important when using sea freight shipping⁴⁷. This document is a contract in which the shipmaster admits receiving cargos and shipping them to a designated location⁴⁸. This document achieves different functions since it is considered a proof of shipping as captured in the Jordanian marine merchant law art. This document is also considered a shipping contract as seen in art. (198) of the same Jordanian law mentioned above and considered also a proof of the ownership of the cargo to the person who signs the contract (9). One of the most important conditions that this document should comply with is the availability of the shipmaster or the owner’s signature. This is what makes this document completely legal and meets all the legal conditions of a contract.

⁴⁶ Abdul Kadir Ghalib Comparison of legislations, p,116

⁴⁷ Chan, F., Ng, J. and Wong, B. (2002). *Shipping And Logistics Law*. 1st ed. Hong Kong: Hong Kong University Press.

⁴⁸ Baughen, S. (2015). *Shipping Law*. 1st ed. Hoboken: Taylor and Francis, p.30-61

Modern technological development and the wide use of computers in different fields have led to the use of electronic shipping document. Committee Maritime International (CMI) adopted special regulations for exchanging electronic shipping documents through electronic data exchange system. This system simulates the function of these documents within electronic environment. These electronic regulations permit goods' sequential ownership transfer through electronic messages, so if the person who is in charge of goods shipping chooses someone to receive it and he noticed the transmitter of this and the mentioned received this notice, then he has the authority to receive the goods and disposing them.

This process can be repeated as much time as needed through shipping and this is how goods' sequential ownership transfer is done during shipping. Now the question is; how are the goods that are being transferred verified through electronic shipping documents? This process is done using "private code"⁴⁹ which is a technical code that combines different numbers and letters used to achieve the electronic transition.

The transmitter will give the code to the designated person by the client himself, this code will do the same function as of paper shipping document and can be changed in each transition. That person has to notify the transmitter that he will give the goods to another person then the transmitter will confirm receiving the notice by giving description of the goods to the new receiver. When approving, the code will be change and this will be repeated every time the goods is transferred. Issuing the new code in each transition will do the same function as of issuing a new shipping paper document. The transmitter will deliver goods to the person who has the right code initiated from the beginning by the client⁵⁰.

⁴⁹ Part 4—Application programming interface (API) Administration, ISO, 2008. Part 5—Testing procedures, ISO, 2011. Part 6- Registration authority procedures for the authentication protocols for interoperability, ISO, 2010.

⁵⁰Ahmad Sharaf Eldeen *Electronic Trade, Legal Consideration*, Onctad studies, 1999, Electronic Trade contracts, p.49 - Abbas Alaboody Previous References Contracts through communication devices, p.298

Private code (electronic signature) has been considered as traditional signature during goods transition as article (14) of Hamburg agreement (1978) stated that “Signing the shipping document can be done manually, voice command, facsimile, sealing or any other electronic means as long this does not contradict the regulation of the country where the document was issued” and this is what CMI approved for electronic shipping documents.

2.12 Electronic Signature in Modern Communication Devices:

Modern communication devices have been used in different fields⁵¹ and for different purposes like making payments, storage devices or establishing contracts between institutions and individuals because of their high speed and reliability to reduce the chances of fraud and duplication. Some of these devices use electronic signature like Telex and Internet.

2.12.1 Telex:

Telex is one of the modern communication devices that have been used to establish contracts between individuals and companies. Telex is defined as “an electronic cabled device connected to special operator which prints data coming from transmitter with red and data coming from receiver with black. So the client can call any other subscriber who has the same device anywhere in the world by using the country code since each country has its own code in a fast and reliable way to exchange data. Telex transfers the written letters through wireless communication to electrical pulses so the pressure on letters will be transferred to electric signals that will transferred to electromagnetic⁵² waves going through wire to the receiving device in which the process will be the opposite to print response.

⁵¹ Huang, D. (2011). *Advanced Intelligent Computing*. 1st ed. Berlin: Springer.

⁵² Pelosi, G., Coccioli, R. and Selleri, S. (2009). *Quick Finite Elements for Electromagnetic Waves* 1st ed. Boston: Artech House, p. 21-26

Telex has many characteristics which include, speed, reliability, accuracy and it provides written proof of the documents sent. This device is based on using symmetric encryption technique in which it can use “call back” system where two connected devices can receive data and use “answer back” system to reply back. Telex has been used in different fields like banks and Marine field. The following is an example of how to use this device in banks. The bank will send a telegram of payment request to the receiving bank including the beneficiary name and date then sign it with a private code at the edge of the telegram.

This code is known only to the transmitting and receiving bank and the authorized employees. As the receipt bank gets the telegram, they will compare the codes with the one already saved in the system if they were matching, the request will be answered. If not, the process will be denied⁵³. The explanation given above is showing that the telex can be considered as a reliable environment to exchange letters among banks and companies. This process is controlled by neutral a person who defines both transmitter and receiver and dates the transition by keeping a proof to the process. Authentic Telex is divided between supporter and operator. Recently the Jordanian law verified Telex in the law numbered (37/2001) article (6) that adjusted article (13) of the original law by adding:⁵⁴

1. Telex, Fax and E-mail letters have the same supporting proof of verification if it did not prove the opposite; it means if the transmitter did not confirm receiving the information.
2. Telex with codes will be proof for both transmitter and receiver.

We can see that Jordanian law verified Telex letters and provided them with the same supporting proof of any document or paper.⁵⁵

⁵³ Abbas Alaboody *Contracts Through Communication Devices*, p.259

⁵⁴ Almonsif Quortas Electronic signature authentic, p.229, Ayth Elmry Technology Authentic, p.35, 1999

⁵⁵ Ahmad Sharraf Eldeen *Electronic Commerce Contracts*, 2008 p.241, Technology authentic by Ayth Elmry, p. 102-103

In order to comply with all the proof conditions, signature should be provided with these letters as captured in Article (10) that states “the regular document should have the signature of the person or his seal to give it the support proof”. That means the law verified the electronic signature in Telex as it is a combination of private codes between the transmitter and receiver and can be decoded between them by using pin number.

2.12.2 Internet

Internet network is one of the largest networks used to communicate around the world. This network was the result of all exchange data, media and communications.⁵⁶ As the computer appeared with all its advantages and features and the ability of connecting these devices together through separate lines or phone lines which forms what is known as specialized information banks. Technology development leads to the ability of connecting these banks together through advanced system that connects computers around the world which forms what is known today as “Internet”. Internet was used initially by military institutions in the United States and then these institutions approved that it can be used to exchange information between individuals all over the world.⁵⁷ Till today, it has been used in different fields like commercial, economics, administration and many others.

Internet Divisions

- 1. World Wide Web (WWW):** This web contains many saved documents that permit any person to view the information of other companies or individuals who put this information through technical mean called “hypertext” that can organize information and call them back as needed. These websites are designed by special companies in which they can display this information as documents, pictures, movies etc.

⁵⁶ Pelosi, G., Coccioli, R. and Selleri, S. (2009). Quick finite elements for electromagnetic waves. 1st ed. Boston: Artech House.

⁵⁷ Rami Alwan Will expression through Internet, Jordan 2001, p.1-2

2. **Electronic Mail:** This is one of the most important services through the Internet that allows the user to send and receive messages and save them in special inbox. The user can read the message immediately or later whenever he can. This service can exchange different types of files like pictures, movies or documents in a fast and reliable environment.
3. **Chat Rooms:** These rooms are known spaces inside cyber space⁵⁸ that allow the users to communicate and send messages between each other through small boxes for both parties. Later on, headphones and microphone were added to this service to allow the users to see and hear each other.

2.12.2.1. Electronic Signature Can Be Performed Through Internet:

Electronic commerce has been connected widely through the Internet network and it has been known as the trade done through Internet. This trading system has different types like displaying goods, services through websites, establishing shopping websites, financial services, airline services, shipping services, internet banks, booking services and tourism. This network is considered as an effective environment for exchanging, trading and permitting at the same time payment services through credit cards and electronic checks. Internet network due to its global position permits users to increase the exchange in stock market. It is expected that Internet website can be used by government to establish what is known as “Electronic Government”⁵⁹ that stay in contact with citizens 24/7 to provide different services that reduce the expenses the government has to pay to offer them through institutions and hire a large number of employees and paying their salaries⁶⁰.

⁵⁸ Gregory, J. and Pestaina, G. (2001). *Law In Cyber Space*. 1st ed. Londres: Commonwealth Secretariat.

⁵⁹ Raunmüller, R. and Lenk, K. (2006). *Electronic Government*. 1st ed. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, pp.23-34.

⁶⁰ Yousif Arab Electronic Commerce, Jordan, volume 1, p.25, David Kosiur, p.23-35

2.12.2.2. Electronic Signature in Internet

Electronic mail and web network use electronic signatures between parties. For example, in e-mail electronic signature is used between individuals through special agreement between them to exchange information. This signature can be digital, electronic or biometric which forms contracts. This process is known as Electronic data exchange.

Electronic signature as per the above definitions is now considered as a certified electronic document that identifies the client's identity and expresses his will during this exchange. Electronic transaction law has verified electronic message as a contract between two parties that express their will and guarantee their response to it by accepting or rejecting in article (13). Evidence adjusted law gives electronic messaged support proof in article (6) of the adjusted law that adds to article (13) item (3) that states in part (A) "Fax, Telex and e-mail has the support proof of paper documents if it is not confirm by the transmitter". The second field of using electronic signature is in web network⁶¹, in which the client displayed all the goods in shopping website and when he/she decides to buy the required one, the screen will display the contract agreement that the client has to accept or reject. If the client accepts the agreement, he has to press yes or otherwise press no. To finalize this transaction the client has to sign by entering his credit card number in the required field. Digital certificates which are issued by specific and authorized companies⁶² can also be used to finalize the transaction by expressing the will of both parties to complete the transaction.

⁶¹ Pino, R. (2014). Network Science And Cybersecurity. 1st ed. New York: Springer Science + Business Media.

⁶² Gladney, H. (2007). *Preserving Digital Information*. 1st ed. Berlin: Springer.

CHAPTER THREE: HOW ELECTRONIC SIGNATURE MEETS SIGNATURE'S FUNCTION

This topic is considered one of the most important topics that should be discussed regarding electronic signature. This signature should comply with the regular signature functions which are identifying the identity of the client and expressing his will. The discussion in this chapter will be centered on whether electronic signature can be considered as a typical type of signature or a new form and then examine how this signature can achieve the signature functions.

3.1. Consideration of Electronic Signature as One of the Signature Types:

There are three main types of signatures which were verified by most of the Arabic legislations which are: signature, seal and fingerprint. The following subjects will be discussed regarding how we can consider electronic signature as each one of these types.

3.2. Consideration of Electronic Signature as a Typical Signature:

Signature⁶³ is considered legally as one of the most verified types and was defined as “combination of lines that take unique geometric shape that is far away from the regular writing shape”. This signature should express the personality of the client and should be done by him personally. The client can use any pen and usually can sign at the bottom of the document to express his approval to everything mentioned inside the document. Jordanian legislator stipulates in article (156) of Jordanian commerce law (12/1966) that “the client has to put his signature at the beginning of the document so that the other party receiving the document can verify it”⁶⁴

⁶³ Jos Dumortier and others, “*The Legal And Market Aspects Of Electronic Signatures*”, pp. 92-94

⁶⁴ Jos Dumortier and others, “*The Legal And Market Aspects Of Electronic Signatures*”, study for the European Commission Directorate General Information Society, Katholieke Universiteit Leuven, 2003, p. 58.

3.3. Consideration of Electronic Signature as Signature:

Electronic Signature is that type of signature that depends on symbols, letters and codes and the client can use electronic pen to do it. Such signature cannot be considered as a regular signature since the signature is done by handwriting using specific shape determined by the client himself. From this point, electronic signature cannot be considered as a regular signature since it does not qualify the condition of being done by handwriting. Legally, electronic signature can be verified as a signature if it is proven that the technology used with this signature is reliable enough to identify the client and express his acceptance to the document contents.

3.4. Consideration of Electronic Signature as fingerprint:

Fingerprint is one of the signature types which verified by the Jordanian legislature because of its high reliability since it is very hard to duplicate a person's fingerprint and it can express his will if he chooses this type of signatures.⁶⁵

Egyptian legislature has verified fingerprint⁶⁶ as a means of signature as well as Iraqi legislator except the latest stipulates that there should be two witnesses to confirm the client's signature or the process should be done in front of an official to prevent duplication and fraud. Jordanian legislator did not put the two witnesses as a main condition to complete the process. The different views between Iraqi and Jordanian legislators have led to criticisms of the use fingerprint as a signature especially if it is very easy to be duplicated or done without the client's approval or if the client might not be able to read the document since fingerprint is usually used by illiterate people.⁶⁷

⁶⁵ Mason, S. (2012). *Electronic Signatures in Law*. 1st ed. Cambridge: Cambridge University Press, pp.100-120.

⁶⁶ History of Digital Signature Law, 2013, Recently the growth of e-commerce and e-business has altered the digital signature and its law..

⁶⁷Mustafa Majdi Harja Authentication Law, p.217, Ayth Elmri Authentication of Technology, p.79-80

The difference between fingerprint and electronic signature is that fingerprint usually leaves a trace on the document which is the part of the skin that has lines and it is different from one person to another while electronic signature cannot be a fingerprint since it depends mainly on codes and symbols. These codes are not made by the client but designed for him and approved to be used as a signature. They don't leave a trace from human body except for the case of biometric signature used in ATM where the machine asks the client to input his fingerprint and compare it with the one programmed inside the machine. Sometimes these machines ask for a pin number besides the fingerprint as well.

3.5. Consideration of Electronic Signature as Seal:

Seals are the oldest means that have been used as a mean of signature.⁶⁸ They are usually made of wood and contained the client's name, job and address. Legislations did not put these seals in a specific shape or design but left that open depending on the client's request. Countries like Iraq and France did not accept seals as a signature since they are so easy to be duplicated, but French legislators have verified using them in signature by using (Griff) them in some exceptions like trade papers in law number (380/1966) issued in June 16, 1966 when signing checks, drafts or policies.

As the Jordanian legislature takes into consideration the possibility of fraud when using seals, the law number (12/1966) states in art (21):

1. The name "signature" can be used in signature, seal and fingerprint.
2. There must be two witnesses available at the time of signing.

Within these two conditions, using seals will be more reliable and safe. Some legislators consider using electronic signatures with pin number in plastic cards as using seals since the signature in this case is not done by handwriting but in different writing styles. French Court of Cassation has approved using seals in signature as per the law issued in (26/6/1996).⁶⁹

⁶⁸ Davidson, A. (2009). *The Law Of Electronic Commerce*. 1st ed. Port Melbourne, Vic.: Cambridge University Press.

⁶⁹ Farouk Weshahi, A. and Mestre, J. (2004). *Le droit face à l'objectif de sécurité du paiement dans le commerce électronique*. 1st ed.

If we assume this consideration is right, this cannot be generalized on all signature types. There are few differences between electronic signature and signatures with seals. The latest leave trace or marks after dumping them with ink and pressing them on papers, while electronic signature with pin number leaves only stars on the screen and no one can know what these numbers are except the client and the bank. Based on all these facts, we can say that electronic signatures are new types of signatures based on using recent technological techniques to accomplish all the financial and commercial documents through computers and because of the wide use of this technology around the world, these signatures have replaced the traditional signatures that were used earlier.

3.6. Fulfillment of Electronic Signature Conditions: We will discuss the signature conditions that the electronic signature must fulfill to consider it one of signature types. These conditions are:

1- Signature must be the sign of a particular person: The signature has to be a specific and special sign of the person to comply with the signature conditions. That means, it should be a linear or biometric sign that identifies the person's identity⁷⁰. As discussed earlier, the signature, seal and fingerprint were considered signature types since they were special signs of the clients that is different from one person to another. We can say that the electronic signature is a special sign of a person. For example, biometric signature is based on special signs of the person himself. ⁷¹.Pin number is also considered a special sign of the person since each client has different pin number and cannot be the same with that of some other clients and no one can know this number only if the client was not able to memorize it. Same case applies for electronic pen signature in which the process cannot be done only if the client's signature is matching with the one saved in computer.

⁷⁰ Hassan Jumea Legal Law Authentication, p.31, Mohammad Zahra Electronic Signature Authentication, p.7

⁷¹ RFC 5652, Cryptographic Message Syntax (CMS), IETF, September 2009. Available <http://www.ietf.org/rfc/rfc5652.txt>

Digital signature has the same feature, in which the private key is known only by the client himself.⁷²

- 2- Signature Should Be Clear And Permanent:** Signature is considered a type of handwriting that should be clear and can be read either directly or by using a special device like computers⁷³. It should be written and saved in a way that it is easy to be reviewed anytime. Does electronic signature fulfill this condition? The electronic signature can be said to fulfill this condition since it leaves different data that can be read and reviewed using special programs that can convert the binary symbols of zero and one to a readable language. As for the continuity, though there are some doubts about it due to the chemical characteristics of the floppy discs and CDs that may cause some damage to them if the power went off, but there were other alternative use that makes them more reliable than papers which can be easily damaged due to bad storage conditions.
- 3- The Policy Should Be Connected To The Signature:** One of the signature conditions is that the policy that includes the client's signature should be connected directly to the content of the policy⁷⁴. Does electronic signature fulfill this condition? This issue depends on the techniques used to connect the signed policy with its contents. One of these techniques is digital signature that is based on two keys, public and private and no one can know the private key except the client himself. Public key converts the signature to arithmetic equation which cannot be read only by using private key through Hachage Irreversible Technique (HIT) which means the contents are connected to the policy in a way no one can read it only the client himself. As for signature with pin number, the machine will print out receipt after each transaction but the signature cannot be seen on the receipt itself. There may be some techniques in the future that will show the connection between signature and the receipt on one document when using ATM.

⁷² Traverso, G., Demirel, D. And Buchmann, J. (N.D.). Homomorphic *Signature Schemes*. 1st Ed.

⁷³ Koh, T. (2013). The Tommy Koh Reader. 1st Ed. Singapore: World Scientific Pub. Co.

⁷⁴ Mohammad Zahra Electronic Signature Authentication, P.9, Hassan Jumea, P.22

3.7. Electronic Signature and Signature Functions

There are some functions⁷⁵ that should be available in electronic signature. Some of these functions are:

1- Electronic signature should identify the client's identity:

Identifying the client identity is an essential function that should be available in electronic signature. Most of the laws state that “if the client does not want to admit what is written inside the policy he has to deny everything inside that policy whether it was a signature, seal or fingerprint otherwise the policy will be used as a proof against him”⁷⁶. This law shows clearly that identifying the client's identity is one of the significant functions that electronic signature should fulfill. For example, in signature, each person will choose a specific shape that he/she can be recognized with. Sealing is also a special sign for each client that has his own information. Fingerprint is a special sign for each person in a way that there cannot be two similar fingerprints of two different persons. Client identification is very important especially in electronic world like ATM, Telex and Internet network which needs a special means to identify the identity and prevent fraud and limit underage activities. If each type of electronic signature is discussed, it can be seen that they all comply with this condition.

Biometric signature has the client's special signs that could not be mix with someone else which is the same case for both electronic signature with pin number and electronic pen. These signatures have special signs that only the client is aware of and he is the only person authorized to use them. Digital Signature also complies with the condition of identifying the client's identity and it is considered very reliable and safe in which only the client can know the private key to activate the signature. This signature is more favorable than the regular signature since the identity can be checked every time the signature is used⁷⁷.

⁷⁵ Ioannidis, J., Keromytis, A. and Yung, M. (2005) *Applied Cryptography And Network Security*. 1st ed. Berlin: Springer.

⁷⁶ Schneider, G. and Evans, J. (2013). *New perspectives on the Internet*. 1st ed. Boston, MA: Course Technology/Cengage Learning.

⁷⁷ Ahmad Sharaf Eldeen *Electronic Commerce Contracts*, p. 132

2- Electronic Signature Should Express the Client's Approval to the Policy Contents:

The law assumes that the client's signature on the policy means his approval to anything written inside that policy as we explained earlier in one of the articles in Jordanian Law that if the client does not want to admit the policy contents he has to deny any signature, seal or fingerprint inside that policy. Signature is considered as one of the will expression means that the client can use to sign a contract and approve it. Article (93) of the civil Jordanian law explained will expression as "will expression can be defined through pronunciation, signal or writing and actual initiative that expresses approval to the policy contents" which the signature, as we discussed earlier, can achieve. Signature gives the legal action or power and credibility and this was shown through the different types of signature that have already discussed earlier.

What signature has accomplished as discussed is that signing the policy means approving to all its contents. Fingerprint expresses the client's approval though it was not viewed as reliable signature in some countries due to the high chances of fraud and wide spread illiteracy among people at that time⁷⁸. For this reason, some laws stipulate that there must be two witnesses at the time of signing the signature to be approved. Some legislators approved the fingerprint as the saw it might be needed in some cases though it might not be a reliable means to be used. Legislatures did not limit will expression with specific means but provide the way to any reliable means to accomplish this mission especially after the huge development in Technology and the wide use of Internet and computer in different fields. Electronic Signature proves that it is the most reliable way to express the client's approval since other traditional ways like seal and fingerprint have higher chances of fraud and duplication.

⁷⁸ See Alliance for Global Business, "A discussion paper on trade-related aspects of electronic commerce in response to the WTO's e-commerce work programme", April 1999, p. 29 (available at <http://www.biac.org/statements/iccp/AGBtoWTOApril1999.pdf>, accessed on 6 June 2008)

Biometric electronic signature with pin number and digital signature are all safe and reliable means to express client's approval since the client approved to the policy contents by giving his pin number or signing the screen. Based on all that have been mentioned, it can be seen that digital signature which is a type of electronic signature can express the client's approval in a secure and reliable way since the client is the only one who can use his private key to process the transaction and no one else can know the codes of his key. So, any means that is secure and reliable and expresses the client's willing can be used as signature and replacement for the traditional one⁷⁹.

3.8. Electronic Signature Authentication:

Electronic signature has been verified by the law due to its important functions. These functions take two forms. First, it is the traditional function in which the signature identifies the client or agent and expresses his/her will and approval to the policy contents and this will eventually guarantee satisfaction of all parties.

The second type of function is the unconventional function compared to traditional signature. For example, coding in electronic signature provides high reliability besides checking with the client about his identity is done every time he/she is using the plastic card which gives higher security to the process more than if the documents were hand written. Based on the previous considerations, Jurisprudence started searching on the basis that leads to verify electronic signature.⁸⁰

There were two directions were taken leading towards this goal. First, considering what credit cards do especially when it is required to enter the pin number every time the cards is used which is the same as signing the policy electronically. Second direction went against the first one in which they did not approve the electronic signature in plastic cards since there is high possibility the pin number or the card may be stolen and the whole process will not be secured.

⁷⁹ Hassan Jumea Legal Laws Authentication, p. 46-47

⁸⁰ Stephen E. Blythe, "*Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security*," 11: 2 RICHMOND JOURNAL OF LAW AND TECHNOLOGY 6 (2005)

People who supported the first direction did not approve this assumption based on fact that the fraud and duplication happened at a higher frequency with the handwriting signature more than with the electronic one in plastic cards since the pin number itself is known only to the client and the bank and there is no connection between the electronic signature on the cards and the client since it depends mainly on the party that issued the pin number which is the bank in this case.

This is why one of the French courts rejected one of the cases that the bank claimed against one of their clients since the signature was not issued by the client but by the bank himself. Another opinion sees that the electronic signature is not issued by the computer but by the person using it, that is to say,, the client can issue his own signature using the computer by following special directions. This opinion was confirmed after one of the French courts decrees the authenticity of electronic signature based on the fact that when the client enters his pin number that means he states and confirms his approval to the process. The conclusion that can be reached from the discussion so far is that the electronic signature can perform the same functions as the traditional one with higher reliability especially after confirming that the signature in the plastic cards can be issued through the computer and only the client and the bank know about it. French law has approved and verified the authentic electronic signature. For Instance, a bank in MONBELEE has issued a ruling approving the electronic signature as means authentic⁸¹ means through which the bank transaction can be accomplished with credit cards.

American law has also approved the authentic use of electronic signature by approving the use of electronic signature on documents exchanged on Fax machine. Iraqi law on the other hand did not approve the electronic signature as an authentic means for the execution of electronic transaction.

⁸¹ Neef, S., Dijck, J. and Ketelaar, F. (2006). Sign here!. 1st ed. Amsterdam: Amsterdam University Press.

This is considered a failure in this field since it is expected that it should go in the same direction with the French and Egyptian law which all goes towards confirming the effectiveness of modern technology in issuing electronic signature. Iraqi electronic transactions and signature⁸² was going straight towards that direction in which article states that “electronic signature has the same authenticity in commercial and administrative transaction as the traditional signature”. Article (16) states that: “if the policy has to have a signature that confirms the party’s approval to its contents; electronic signature can be considered as a replacement to the traditional signature in this case”.

Egyptian electronic signature law states in article (14) that electronic signature in commercial and administrative transaction has the same authenticity as the traditional one based on the conditions mentioned in article (18) of the same law. Jordanian law also approves electronic signature as an authentic means of electronic transaction as stated in article (7/A) based on the conditions mentioned in article (10/A) of the same law. French legislature goes in the same direction in article (4/1316).

American federal electronic signature law in article (101) states that “the role of electronic signature should not be neglected just because it was in electronic form”.⁸³ Typical law of electronic signature approves the electronic signature as being authentic too as stated in article (1/6) “when it is necessary to have confirmation from the client to proceed with the commercial transaction electronic signature can be used as replacement of the traditional one”. Typical law of electronic commerce states in article (7) that electronic signature can be used to express the client’s approval to the policy contents.

⁸² Waheeb, R. (2015). *Electronic Signature Under Iraqi Law*. 1st ed. Kuala Lumpur: Ahmad Ibrahim Kulliyah of Laws, International Islamic University Malaysia.

⁸³ Bouchoux, D. (2009). *Legal research and writing for paralegals*. 1st ed. New York: Aspen Publishers.

CHAPTER FOUR: INTERNATIONAL USE OF ELECTRONIC SIGNATURE ON A DOCUMENT

The discussion in this chapter shall be based on two major parts:

PART 1

This topic and discussion has been developed to assist all parties (and their legal advisers) who aim to implement commercial contracts, by having official documents using electronic signature or who aim to enter into a commercial contract with multiple parties that intend to execute that contract using an electronic signature. Accordingly, this chapter shall summarize the concept of how the electronic signature can be put to effective use, considering its functions and the necessary procedures to executing the electronic signature on a document.

The JWP84 has acquired legal advice from leading counsel (Mark Hapgood QC85) on how to use electronic signatures and considers it as a valid method of executing documents. This note has also been approved by leading counsel. This subject note is entitled to the commercial contracts entered into (and certain other documents signed) in a business context. Hence, it is recognized that certain principles and frames that are considered in this note may also be applicable to documents entered into in other contexts. However, each transaction should be approached according to its own facts and should take into account the wider implementation of the transaction, including any relevant rules or tax implications.

⁸⁴ Law Society Company Law Committee and the City of London Law Society Company Law and Financial Law Committees

⁸⁵ Mark Hapgood was called to the Bar in 1979 and was the most junior member of the Bar to be appointed Queen's Counsel in April 1994. He is widely recognized as a leading Silk in commercial litigation..

Background

Recently, where any party in a certain transaction is not physically available to sign formal documentations, it is often familiar to the lawyers who are involved to arrange a signature via email, following the procedures set out in the guidance note ⁸⁶. This particularly involves the signatory signing a hard-copy document in wet-ink, converting the document and signature into electronically registered form (e.g. by scanning or photocopying it) and later sending it by email. As a result, a market practice and technology evolved. The use of electronic signatures is becoming increasingly common in a range of commercial transactions and that case is expected to expand and spread all over the world with time.

4.1 Forms of Electronic Signatures:

Electronic signatures can take different forms and shapes, which are as follows:

- i.** Person typing his / her name into a contract or into an email including the terms and conditions of a contract,
- ii.** Electronically, a person tries to paste his / her signature (eg as an image file) into an electronic (soft copy) version of the contract in the signature place (next to the relevant party's signature block), considering the formatting and the picture brightness
- iii.** If someone is accessing a contract through a web-based e-signature platform⁸⁷ and clicking to have his / her name in a typed or handwriting font automatically inserted into the contract in the appropriate place (next to the relevant party's signature block),
- iv.** Person using a finger, light pen or stylus and a touch screen to write his / her name electronically in the appropriate place (next to the relevant party's signature block) in the contract.

⁸⁶ Note on Execution of Documents at a Virtual Signing or Closing (PDF) prepared by a joint working party of the Law Society, prepared by a joint working group of the Law Society Company Law Committee and The City of London Law Society Company Law and Financial Law Committees in May 2009.

⁸⁷ Lehnert, W. (2001) *Web 101*. 1st ed. Boston: Addison-Wesley.

This note does not focus on any one method of electronic signature, but rather on setting out the requirements for deciding whether a certain document signed with an electronic signature has been *validly executed*.

4.2 The Methods of Executing Electronic Signature:

If one (or some) parties to a document (including any witnesses) aim to sign using an electronic signature, while another (or others) would prefer to use another acceptable method (wet-ink signature), there is no reason why the document cannot be signed using a combination of different methods, so long as each party uses a valid signature method, although there may be practical advantages (electronic storage) if a document is created only in an electronic process.

The Concept of Originals and Counterfeit: An elading counsel has advised the following:

- it is possible, based on some facts, to have multiple originals of a document in both electronic and hard-copy form (including, where the parties intend for multiple originals to be produced in electronic and/or hard-copy form)⁸⁸, but it would not be appropriate if it would conflict with other legal requirements (as would be the case with, promissory notes)
- Where a document has been electronically executed with each signatory applying his / her signature to the same file uploaded to the relevant electronic signature platform, the signatories will be deemed to have signed the same counterpart.
- Where a document has been executed by using a combination of electronic and wet-ink signatures, the parties or their legal advisers may wish to create a composite document (either by using a hard-copy print out of the electronically-signed document and the wet-ink signed pages or by scanning the wet-ink signed pages and creating a composite electronic document) and to the extent that the document is required to be produced in evidence, an English court would accept this composite document

⁸⁸ Faria J.A.E., The UN Convention on the Use of Electronic Communications in International Contracts – An Introductory Note, ICLQ 2006, p. 689

- When the original document has been executed electronically, it is required to be produced in evidence; a court (English court) would accept an electronic version of that executed document or a hard-copy document.
- Where an undated document is executed electronically, it may be validly dated with the authority of the parties:
 - (i) by inserting the date electronically,
 - (ii) by printing it out and writing the date by hand,
- After a document has been executed electronically, amendments can be made to it (electronically or in manuscript) to the same extent as amendments may be made in manuscript to a document executed in wet-ink.

4.3 Other Considerations:

This practice note is entitled to question whether or not an electronic signature can be used to validly execute a commercial contract as per English law. However, where one or more parties wish to agree on a contract are contemplating using an electronic signature, there are a number of other legal and practical matters which they / their legal advisers might need to consider, including the following:

- ✓ Prepare an entity that intends to execute the contract using an electronic signature⁸⁹, the **question is does it have the corporate capacity or the authority to do so?**

Well, this will depend on the facts, but should not vary from the position where the party is executing the contract with a pen, unless there is something in its constitutional /legal documents or board resolutions restricting the use of an electronic signature.

⁸⁹ Jin, D. and Lin, S. (2012). Advances in Electronic Engineering, Communication And Management. 1st ed. Berlin: Springer p 101-133

In the absence of any specific restriction, it is not necessary to include a reference to electronic signature in any board resolution or for the constitutional documents to specifically reference the fact that the entity can enter into agreements or transactions which are electronically signed.

- ✓ **Is it certain that the person is supposed to sign using an electronic signature is in fact that person or another person acting under the authority of that person?**

Factors that might assist in this regard include (particularly, where the contract has been executed by an e-signing platform) whether the signatory had accessed the document using a particular email address or by putting a unique access code and whether or not this can be confirmed (via a certificate or otherwise) by the platform provider.

- ✓ **Is the document to be distributed, signed and held electronically in a manner of security insurance?**

This will be based on the method used and on the importance placed on IT and network security by the parties. The question to be answered is, for example, how valuable is the contract; how important is it to keep it confidential and secured? So it is a matter that each party should consider on a case-by-case basis and draw its own conclusions.

- ✓ **Which documents require to be filed with an authority or registry, will that authority or registry accept electronic signatures?⁹⁰**

For example, as at the date of this note:

- i. The Land Registry and the Land Charges Registry require a wet-ink signature on a paper version of any document submitted to them for registration (although the Land Registry has announced plans to launch an electronic mortgage service).

⁹⁰ Miller, R. (2013). Business law today. 1st ed. Mason, ohio: South-western.

ii. The stamp duty is payable on a document, H.M. Revenue & Customs would normally expect to stamp a version of the document with a wet-ink signature.

- ✓ **In case if the place of signature or the location of the document has particular legal consequences (In relation to the payment of stamp duty), where will a document executed using an electronic signature be treated as having been executed or located?**

The answer is based on certain factors, including where the signatory is physically located when signing and where the server on which the document is stored is located. In such circumstances, it may be better to have a physical signature.

- ✓ It is not necessary to include any specific reference to electronic signatures in the document itself in order for it to be validly executed using an electronic signature.
- ✓ This note refers to certain European Union Regulations, the status of which under English law may be affected by the United Kingdom ceasing to be a member of the European Union.⁹¹

4.4. Electronically Signed Document and Originality This practice note gathers and considers principles around what constitutes “original” documents for these purposes⁹². The practice note provides that:

1. Originals can be held in hard copy or electronic form, and multiple originals can be created, or copies
2. Where signatories sign the same document uploaded to an electronic signature platform, they will each be deemed to have signed the same counterpart
3. Where a document has been signed by a combination of methods, a single “composite” or “Extensional” document can be created.

⁹¹Achache, V. and Piquemal, A. (2008). *L'approche juridique de la sécurité des paiements dans le commerce électronique*. 1st ed. Lille: Atelier national de reproduction des thèses.

⁹² Anderson, M. (2016). *Drafting And Negotiating Commercial Contracts*. 1st ed. Place of publication not identified: Bloomsbury Professional, p.82 -99

CHAPTER FOUR: INTERNATIONAL USE OF ELECTRONIC SIGNATURE ON A DOCUMENT

PART 2: UNCITRAL Model Law on Electronic Signatures (2001)

4.2.1 Definitions for the Purposes of Electronic Law

- ❖ **“Electronic Signature”** means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message;
- ❖ **“Certificate”** means a data message or other confirmed records certify to the link between a signatory and signature creation of the data;
- ❖ **“Message Data”** means generated information, sent, received or stored by electronic, optical or similar means including, but not limited to, Electronic Data Interchange (EDI), electronic mail, telegram, telex or telecopy;
- ❖ **“Signatory”** means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;
- ❖ **“Certification service provider”** means a person that issues certificates and may provide other certification services related to electronic signatures;
- ❖ **“Relying Party”** means a person that may act on the basis of a certificate or an electronic signature

4.2.2 Background:

In preparing and adopting the UNCITRAL Model Law on Electronic Signatures (also called “**the Model Law**” or “**the new Model Law**”), the United Nations Commission on International Trade Law (**UNCITRAL**) was conscious that:⁹³

- The Model Law would be a more effective tool for States modernizing their legislation if background and explanatory information were provided to executive branches of Governments and legislators to cooperate and guide them in using the Model Law.⁹⁴
- The Commission was also alerted of the Model Law would be used in a number of States with limited familiarity with the type of communication techniques considered in the Model Law.
- The present Guide to Legislation has been prepared by the Secretariat pursuant to the request of UNCITRAL made at the close of its thirty-fourth session⁹⁵, in 2001. It is based on the deliberations and decisions of the Commission at that session, that the Model Law was adopted, as well as on considerations of the Working Group on Electronic Commerce, which managed the preparatory work process.

⁹³ PUBLIC LAW 106–380—OCT. 27, 2000". 2000. <https://www.gpo.gov/fdsys/pkg/PLAW-106publ380/pdf/PLAW-106publ380.pdf>. [Accessed date: 1 March 2017]

⁹⁴ The Electronic Signatures Act: 15 USC Chapter 96, Model Law on Electronic Signatures, p. 150. United Nations Convention on the Use of Electronic Communications in International Contracts (Including explanatory notes by the UNCITRAL secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts) (New York: United Nations, 2007), paragraphs 147–64.

⁹⁵ Official Records of the General Assembly, Fifty-sixth sessions, Supplement No. 17 (A/56/17), paras. 201-284.

4.2.3 Signatory Conduction:

Where signature creation data is used to create a signature that has legal effect, each signatory should take into consideration the following:

- a) Exercise reasonable care to avoid unauthorized use of its signature creation data;
- b) Without further delay, utilize means that are made available by the certification service provider or otherwise, use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature in case the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;
- c) And where a certificate can be used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its structure or that included in the certificate.

4.2.4 Recognition of Foreign Certificates and Electronic Signatures:

1. Determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had on:
 - i. Geographic location: where the certificate is issued or the electronic signature created or used or
 - ii. Geographic location of the business place of the issuer or signatory.
2. A certificate issued outside the enacting State shall have the same legal effect in the enacting State as a certificate issued in the enacting State if it offers a substantially equivalent level of reliability.
3. An electronic signature created or used outside [the enacting State] shall have the same legal effect in the enacting State as an electronic signature created or used in the enacting State if it agrees to offer a substantially equivalent level of reliability.

4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be given to recognized international standards and to any other relevant factors.
5. Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition⁹⁶, unless that agreement would not be valid or effective under applicable law.

⁹⁶ Article 5 section 2 reads: "Data in electronic format signed with safe electronic signature verified by valid qualified certificate are equivalent in their legal effects with documents signed by hand unless specific provisions of law provide otherwise." 5 A list of entities rendering the certification services may be viewed on the web e.g. at <http://www.centrast.pl/?i=10>

CONCLUSIONS

The discussions in the thesis in the electronic signature have revealed that the electronic signature is based on using modern techniques like computer and Internet networks which means it takes the form of electronic data processed through computer. It has different types and forms based on the technology used to form that signature. It may be in the form of numbers, symbols or codes. Electronic signature has many applications like plastic cards, checks and electronic shipping documents. By time, it shows its capability in fulfilling the functions of the traditional signature in identifying the client's identity as well as expressing his will and approval to the policy contents.

Since traditional signature cannot be fit in electronic environment, it was replaced by electronic signature since it has high reliability and security in identifying the client's identity and depending on authentic certificates. That means the authentic electronic signature was verified and approved and has been used widely. This signature was able to identify the identity and offer high security since the data used was connected to the source itself and under its full control which reduce the possibility of fraud and duplication.

Consenting parties to a transaction should determine the appropriate authentication technologies and implementation models for the transactions, with assurance that those technologies and implementation models will be recognized and generally used. Consenting businesses or parties to a transaction that have reasons to disagree can extend their opportunity to prove in court or other proceedings that their authentication approaches and methods are valid. As well as, take a nondiscriminatory approach to electronic signatures and the authentication methods from other jurisdictions.

Finally, the Approval of Electronic Signature Methods by the authority that is concerned explains why the final approval of any electronic signature method is given by the authority that is approving. The determination of whether to approve a particular electronic signature resides with the authorizing body after giving due consideration to system of type of electronic signature under consideration. On the other hand, the use of the electronic signature is at least reliable as the existing method has been effective. This determination is made by the approval authority through the careful selection of a sufficient electronic signature service and reviewing all types of the electronic signatures.

RECOMMENDATIONS

The recommendation of this study is that the Iraqi legislature should verify the authenticity of electronic signature and issue a special law for controlling electronic transactions and legislate on the effective ways of resolving disputes and arguments between parties electronically and they should be guided by the European law. The legislators should also put appropriate laws in place that can control the use of this technology in commercial and administrative field guided by a typical law of electronic signature and commerce to improve the Iraqi economy and encourage foreign investments.

This study also recommends that enabling legislation should be put in place by the Iraqi legislators to ensure strict punishments of fraudsters. This will go a long way in preventing any fraud in this field. The Iraqi legislation should be guided by the Jordanian, Egyptian and French law. Finally, the thesis encourages the formation of special committees to control electronic commerce and by holding conferences on a regular basis to discuss the importance of electronic signature and its high reliability in commercial transactions. The government should look for certain solutions that will help accomplish e-transactions and they should try and ensure that there is a permanent (unchangeable) attachment of a signature to a formal related document (for example, using a PDF or similar document that cannot be altered or via appropriate encryption software. In addition, there should be a permanent audit to trail the use of the electronic signature in documents. In case of any change/ amendments made to the signed documents, it will automatically alert the reader of those changes

However, risk assessments should be should be done regularly in order to fall stall the possibility of fraud, error or misuse of the various types of electronic signatures. There should also be an analysis of the cost-benefit of the different alternatives of electronic signatures, and get the required consultation of legal counsel on the implications of using electronic signatures.

This era of technology development in which we live in now, which can also be called the era of information revolution has led to the emergence data tools as a new method of the conclusion of the contracts which were not known a few years ago are now very popular. This requires the development of a permanent, continuous and a fast law that mirror the reality of the present day. The legislators have the task and duty of developing a new legislation that will treat what has been updated as new means and method and ways to enter into contracts and sign them to suit the electronic era. The use of electronic signature in general is the most prominent way of expressing the will of the owner and approval of the content of the contract. The use of electronic signature may make the use of traditional signature and legislation more complex.

The absence of physical media or traditional media that can proof the existence or execution of an agreement is a challenge that electronic signature has overcome. The electronic signature has had a special significance in many of the modern legislation, both the global or national legislation that recognized the e-signature and organized its provisions. Obviously, it was imperative for the researchers with interest to study electronic signature laws and learn all of it with regard to its electronic system in order to identify how to proof legal contracts which are made through the Internet, without the use of the papers and know how authoritative the outputs of these methods is in the event of a need of proof, especially that countries such as Iraq is still not yet organized in this respect. The rules of law are consistent with the privacy and the needs of the community, leaving sufficient provisions of the rules of conventional or public proof, so it had to be with this knowledge of how to absorb the traditional rules of that electronic output as well as the extent of adaptation with the current provisions of this means of executing contract.

BIBLIOGRAPHY

Legislations

Iraqi Law in Electronic Signature Article No. 78 year 2012.

European Union – Electronic Signature Definition July, 2016.

UNCITRAL Model Law on Electronic Signatures (2001).

Jordanian Commerce Law 12/1996/ Modified 2001 Article 7.

The Electronic Signatures in Global and National Commerce Act (ESIGN, Pub.L. 106–229, 114 Stat. 464, enacted June 30, 2000.

Books

Achache, V. and Piquemal, A. *L' approche juridique de la sécurité des paiements dans le commerce électronique*. 1st ed. Lille: Atelier national de reproduction des thèses (2008).

Ahmad Sharaf Eldeen *Electronic Signature, Regulations And Reliability In Electronic Commerce*, a paper submitted to electronic commerce conference, (Cairo November 2000).

Ahmad Sharaf Eldeen *Electronic Trade, legal consideration, Onctad studies, ,Electronic Trade Contracts*. Abbas Al-Aboody Previous References Contracts through communication devices (1999)

Ahmad Sharraf Eldeen *Electronic Commerce Contracts. Technology Authentic* by Ayth Elmry (2000)

Aith Elmri *E-sign*, Pc magazine, February, *Authentic of Technology* (Cairo 2001).

Aith Elmri, *Authentic of Technology* p99. Almonsef Quortas *Authentic of Electronic Signature*, (1997)

Alhussban, N. (n.d.). *Admissibility of electronic signature in evidence and it's legal effect*. 1st ed (2011)

Almonsaf Quortas *Electronic Signature proof*, p.30. Almonsaf Quortas *Legal sides of Electronic Cards And Legal Effects Of Using Computers In Banks*, Beriut, (1999)

Almonsif Quortas *Electronic signature authentic*, Ayth Elmry *Technology Authentic*, https://www.csb.gov.kw/images/Magazine_E.pdf (2014)

- Al-Rashid, S. *Electronic Signature in Electronic Contract In Iraqi Legislations*. 1st ed (2013).
- Alvarez, F. & F. Lippi. 'Financial innovation and the transaction demand for cash.' *E- conometrica* 77 (2009)
- Anderson, M. "*Drafting and Negotiating Commercial Contracts*" 1st ed. Place of publication not identified: Bloomsbury Professional (2016)
- Bátiz-Lazo, B. and Hacialioglu, N. Barclaycard: still the King of Plastic? In: *Exploring Corporate Strategy: Text and Cases*, G. Johnson, K. Scholes and R. Whittington (EDS) 7th edition, London: Prentice Hall/Financial Times, (2005)
- Baughen, S. *Shipping Law*. 1st ed. Hoboken: Taylor and Francis (2015).
- Bolt, W., D. Humphrey & R. Uittenbogaard 'Transaction pricing and the adoption of electronic payments: a cross-country comparison.' *International Journal of Central Banking* (2008).
- Boss A.H., and Kilian W. (eds.). *The United Nations Convention On The Use Of Electronic Communications In International Contracts: An In-Depth Guide and Sourcebook* (2008)
- Bouchoux, D. *Legal Research And Writing For Paralegals*. 1st ed. New York: Aspen Publishers (2009).
- Chan, F., Ng, J. and Wong, B. *Shipping and logistics law*. 1st ed. Hong Kong: Hong Kong University Press (2002).
- David Kosiur, *Understanding Electronic Commerce*, (2006)
- Davidson, A. *The Law of Electronic Commerce*. 1st ed. Port Melbourne, Vic.: Cambridge University Press (2009).
- Faria J.A.E., *The UN Convention on the Use of Electronic Communications in International Contracts – An Introductory Note*, ICLQ (2006).
- Farouk Weshahi, A. and Mestre, J. *Le droit face à l'objectif de sécurité du paiement dans le commerce électronique*. 1st ed (2004).
- Gladney, H. *Preserving Digital Information*. 1st ed. Berlin: Springer (2007).
- Gregory, J. and Pestaina, G. *Law in Cyber Space*. 1st ed. Londres: Commonwealth Secretariat (2001).
- H. Abelson, Fischer, M., Weitzner, D., Perelman, L., and Unger, D., "Ethics and Law on the Electronic Frontier". Massachusetts Institute of Technology, (2010).

- Harralson, H. and Miller, L. "Developments in handwriting and signature identification in the digital age". 1st ed. London: Routledge, Taylor & Francis Group (2015).
- Hassan Jumea Legal Law Authentication, Mohammad Zahra Electronic Signature Authentication, (1997)
- Hazem Alsamadi - *Authentic of Electronic Signature, electronic trade and banking services through Internet* Al Monsif Quortas, Beirut 2000, bank responsibilities in electronic commerce, December (2000).
- History of Digital Signature Law, *Recently The Growth Of E-Commerce And E-Business Has Altered The Digital Signature And Its Law* (2013)
- Hu, Wensong "Advances In Electric And Electronics" 1st ed. Berlin: Springer (2012).
- Huang, D. *Advanced Intelligent Computing*. 1st ed. Berlin: Springer (2011).
- Hussam Elabd Fraud and Duplicate plastic cards, Banks Magazine in Jordan, 5th issue,. Khlaid Al Rawi Banking transactions by, Jordan June 2nd 1999
- Ioannidis, J., Keromytis, A. and Yung, M. Applied cryptography and network security. 1st ed. Berlin: Springer (2005).
- Jin, D. and Lin, S. *Advances in Electronic Engineering, Communication and Management*. 1st ed. Berlin: Springer (2012)
- Jonathan E. Stern, Note, "Federal Legislation: The Electronic Signatures in Global and National Commerce Act," 16 BERKELEY TECHNOLOGY LAW JOURNAL 391, 395 (2001).
- Jos Dumortier and others, "The Legal and Market Aspects of Electronic Signatures",
- Jos Dumortier and others, "The legal and market aspects of electronic signatures", study for the European Commission Directorate General Information Society, Katholieke Universiteit Leuven, 2003.
- Khlaid Alrawi Banking Transactions, p.31. Mohammad Zahra, *Electronic Signature Proof* year (2008).
- Koh, T. The Tommy Koh Reader. 1st ed. Singapore: World Scientific Pub. Co. (2013)
- Lehnert, W. *Web 101*. 1st ed. Boston: Addison-Wesley (2001).

- Lopenzina, D. "Red ink". 1st ed. Albany: State University of New York Press (2012)
- Mason, S. Electronic Signatures in Law. 1st ed. Cambridge: Cambridge University Press, (2012)
- Miller, R. Business Law Today. 1st ed. Mason, ohio: South-western (2013)
- Mohammad Zahra Electronic Signature Authentication, 1989
- Mustafa Majdi Harja Authentication Law, p.217, Ayth Elmri Authentication of Technology,
- Nasiyrat Alaa Eid "The Authority of Electronic Signature In Evidance A Compartive Study", a research submitted in AL Bait Al Gharaa University, November (2005)
- Neef, S., Dijck, J. and Ketelaar, F. Sign here!. 1st ed. Amsterdam: Amsterdam University Press (2006)
- Pelosi, G., Coccioli, R. and Selleri, S. Quick finite elements for electromagnetic waves. 1st ed. Boston: Artech House (2009).
- Pelosi, G., Coccioli, R. and Selleri, S. Quick finite elements for electromagnetic waves. 1st ed. Boston: Artech House (2009).
- Pino, R. Network Science And Cybersecurity. 1st ed. New York: Springer Science+ Business Media (2014).
- Pirlo, G., Impedovo, D. and Fairhurst, M. "Advances In Digital Handwritten Signature Processing". 1st ed. Singapore: World Scientific Pub. Co., (2014)
- Raunmüller, R. and Lenk, K. Electronic Government. 1st ed. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, (2006).
- Schneider, G. and Evans, J. (2013). New Perspectives on the Internet. 1st ed. Boston, MA: Course Technology/Cengage Learning.
- Sinisi,Vinzenzo, Digital Signature Legislation in Europe, International Business Lawyer, No 11, Dec (2000)
- Stašelytė, N., Šešok, N. and Iljin, I. Investigation into Plastic Cards. Science – Future of Lithuania, 6(6), (2014).
- Stephen E. Blythe, "A Critique of India's Information Technology Act and Recommendations for Improvement," 34 *Syracuse Journal of International Law And Commerce* 1 (2006),
- Stephen E. Blythe, "Digital Signature *Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-*

Commerce with Enhanced Security,” 11: 2 RICHMOND JOURNAL OF LAW AND TECHNOLOGY 6 (2005).

Stephen E. Blythe, “*The Barbados Electronic Transactions Act: A Comparison with the U.S. Model Statute*,” 16 CARIBBEAN LAW REVIEW- (2007).

Stephen E. Blythe, “the Electronic Transactions Ordinance as a Facilitator of Growth for E-commerce,” 2:2 JOURNAL OF ISLAMIC STATE PRACTICES IN INTERNATIONAL LAW - (2006)

Traverso, G., Demirel, D. and Buchmann, J. (n.d.), Homomorphic Signature Schemes. 1st ed (2002)

Vagner Schoaba, Felipe Eduardo Gomes, Luiz Castelo Branco, Digital signature has same value as the physical signature on paper (2011)

Waheeb, R. Electronic signature under Iraqi law. 1st ed. Kuala Lumpur: Ahmad Ibrahim Kulliyah of Laws, International Islamic University Malaysia (2015).

Yousif Arab Electronic Commerce, Jordan, volume, David Kosiur, (2009)

WEBSITES REFERENCES:

Overview of the Electronic Signature Law in the EU". 2017. <https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/overview-of-electronic-signature-law-in-the-EU.pdf>. [Accessed 20 Mar. 2017].

Overview of the Electronic Signature Law in the EU". 2017. <https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/overview-of-electronic-signature-law-in-the-EU.pdf>. [Accessed 20 Mar. 2017]. [Accessed 22 April 2016]

EUR-Lex - L24118 - EN - EUR-Lex". 2017. Eur-Lex.Europa.Eu. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3A124118>. [Accessed 20 Mar. 2017].

RFC 5652, Cryptographic Message Syntax (CMS), IETF, September 2009. Available <http://www.ietf.org/rfc/rfc5652.txt>

PUBLIC LAW 106-380—OCT. 27, 2000". 2000. <https://www.gpo.gov/fdsys/pkg/PLAW-106publ380/pdf/PLAW-106publ380.pdf>. [Accessed date: 1 March 2017]

The Electronic Signatures Act: 15 USC Chapter 96; <http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/content-detail.html> [Online] [Accessed 22 March 2017].

<http://portal.etsi.org/esi/el-sign.asp>; The ETSI Electronic Signatures Workgroup issued also a technical specification for XML advanced electronic signatures (XAdES), <http://tinyurl.com/2v9bsh> [Online] [Accessed 20 Mar. 2017].

RFC 5652, Cryptographic Message Syntax (CMS), IETF, September 2009. Available at <http://www.ietf.org/rfc/rfc5652.txt> [Online] [Accessed 30 November 2016].

See Alliance for Global Business, "A discussion paper on trade-related aspects of electronic commerce in response to the WTO's e-commerce work programme", April 1999, p. 29. Available at <http://www.biac.org/statements/iccp/AGBtoWTOApril1999.pdf>,

Accessed on 6 June 2008) (4) Ayth Elmree Technology Authentication, p. 86 [Online] [Accessed 30 November 2016].

“Online Services, including E-Commerce in the Single Market”, Accompanying Document COM (2011) 942, SEC (2011) 1641 final, Commission Staff Working Document, “A Coherent Framework to boost Confidence in the Digital Single Market of E-commerce and other online services”, 11.1.2012, p. 8. http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf[Online]

[Accessed 22 April 2016]

ARTICLES:

Tunisia, Loi relative aux échanges et au commerce électroniques, article 18; and Viet Nam, Law on Electronic Transactions, article 31 (d) 2002

Almonsaf Qurtas Secure payment by check systems and the possibility of lifting the injection character of checks law, Arabic Banks union magazine, issue 240, December 2000,

Part 4—Application programming interface (API) administration, ISO, 2008. Part 5—Testing procedures, ISO, 2011. Part 6- Registration authority procedures for the authentication protocols for interoperability, ISO, 2010.

Note on Execution of Documents at a Virtual Signing or Closing (PDF) prepared by a joint working party of the Law Society, prepared by a joint working group of the Law Society Company Law Committee and The City of London Law Society Company Law and Financial Law Committees in May 2009.

ISO/IEC 24727, Identification cards -- Integrated circuit card programming interfaces. Part Architecture, ISO, 2007. Part 2- Generic card interface, ISO, 2008. Part 3- Application interface, ISO 2008.

Law No. 15 of the year 2004 regulating Electronic Signature and establishing the Information Technology Industry Development Agency; and presidential decree No. 201 of the year 2004 forming the cabinet of ministers.

Regulation no (13) for the year 2001 Regulation for Registration and Licensing of Enterprises in the Aqaba Special Economic Zone Law