Indian Journal of Fundamental and Applied Life Sciences ISSN: 2231– 6345 (Online)
An Open Access, Online International Journal Available at http:// http://www.cibtech.org/sp.ed/jls/2014/01/jls.htm
2014 Vol. 4 (S1) April-June, pp. 1631-1642/ MashakZadeh
Review Article

THE ROLE OF ELECTRONIC SIGNATURE IN THE THIRD MILLENNIUM OF THE DEVELOPMENT OF INTERNATIONAL TRADE TRANSACTIONS

***Seyed Ali Reza Khir Ali MashakZadeh[1]**
[1] *PhD student Private Law, Islamic Azad University, UAE. (Lecturer of Law, Islamic AzadUniversity)*
**Author for Correspondence*

ABSTRACT
Data explosion, in the present era, has created a lot of changes in the social, economic and cultural relationships of all developed societies. Modern areas usually do not have the required legitimacy; however it does not mean that the way for all kinds of violation is open. Social life requires that order and security also govern these areas and protect ethics and public interests. Electronic commerce law is one of these areas – a debatable area filled with innovations and surprises. In this regard, waves of internet revolution and the explosion of e-commerce collide with the legal system and influence the concepts of traditional law. One of the key achievements of information technology is changes in traditional regime of evidence claim. In the system of evidence claim in the majority of countries, written reasons and documents are of undeniable importance, in a way that they are mostly used as citation or to defend the Lawsuit. In fact, a lawsuit and adducing the evidence in our legal life largely depend on delivering or issuance of a written paper such as ID cards, pay stubs, payment receipts, contracts, declarations, warnings, statements, and/or commercial documents.

Keywords: *Electronic Signature, International Trade Transactions, Uncitral, Electronic Commerce, Business Management*

INTRODUCTION
UNCITRAL Model Law on Electronic Commerce Art.11 in 1996 introduced a model law for e-commerce. This law built the foundation of similar laws in Australia, Singapore and some European Union countries by adopting a technology neutral approach and determining general criteria to obtain a reliable electronic signature, many parts of this model law were placed in the context of national law.
American Bar Association formed the e-commerce committee in 1991 that worked for five years in the field of combining modern technology with legal rules and in 1996 issued guidelines for digital Signature. The model law used a special technology method and immediately was manifested as the Digital signature act in the state of Utah in 1995. And within two years, most U.S. states and countries such as Malaysia, Germany, etc accepted it in their own laws.
European Union in 1999 issued instructions for electronic signature by combining UNCITRAL model law with law of the American Bar Association, and introduced a new standard in developing of electronic evidence act. However, this approach is greatly considered a developed model of 1996 and 1998 UNCITRAL (A Position, 2001, 1-2.)
A glance at legal titles proposed in the field of e-commerce indicates that the major problem lies in the proper and effective implementation of the laws rather than the relevant legislation. For law enforcement, judges familiar with informatics rights issues, trained police, and technical and cryptography fields are required. This section of the legal context of electronic commerce is quite breathtaking and overwhelming for the judicial and administrative system of the country. Is there a short-term solution?

1-STUDING THECONCEPT, REASONS ANDELEMENTS OF E-COMMERCE
One of the consequences of globalization is the increased competition in the international economy; because in these conditions, we constantly encounter decrease in shipping costs, astounding growth of information technology, increasing development of e-commerce, minimization of geographic limitations, and increase in competitiveness. And as a result, international economic efficiency will increase.

Here, it can be said that the major consequence of globalization on the economy is the growth of electronic commerce. E-commerce and consequently e-commerce models were introduced for the first time in the early 1970's. In this period, the use of e-business models was very expensive and most of its users were financial corporations, banks and sometimes large industrial companies. The application of e-commerce in the course was difficult and therefore required heavy investments to provide needed platform for it. So, the range of its application was limited financial institutions and large firms. In the next step, electronic data exchange standard was created that was a generalization of the banking and financial transfer model using the new tools of information. But it was different; electronic data exchange had the possibility to be used and utilized in other types of trade too. Electronic data exchange led the application domain of e-commerce models spread broader than the range of large financial institutions. In this topic we are going to explain the concept of e-commerce law and evidence claim. (Smedinghoff, *1997*, 723-768.)

1-1- Explaining the Concepts and the Nature of Electronic Commerce law and Evidence Claim

In order to define e-commerce law, first it is essential to define the terms of trade and trade law, and then according to this description and elements of "electronic" commerce, we are able to provide a definition for e-commerce and e-commerce law.

Commerce: Various explanations have been offered for commerce. Some of them are as follows:

- Commerce is a transaction, a purchase or sale of goods, productions, or property of any kind.
- Commerce is any purposeful activity that includes exchange of goods and services with money. This definition involves production and manufacturing.

Commerce often takes place within the country and sometimes between two or more countries. Therefore, from this perspective, commerce is divided into domestic commerce and international commerce.

Domestic commerce: It includes commerce between natural or legal persons within the same country.

Commerce between the states of a country: Such as the commerce among the states of America (Interstate Commerce).

International commerce: It includes the commerce between countries or natural or legal persons in a country with natural or legal persons in other countries. (Ramberg, *2001*, 2-3.)

Commercial law: Definitions of commercial law in civil law systems and common law are different.

In common law systems, "Commercial Law is a branch of the law which deals with the law and obligations arising from the supply of goods and services during the commerce."

In French legal system, commercial law has a more extended meaning and commercial law includes not only commercial transactions but also other activities such as law of the firms, bankers NAIC (National Association of Investment Companies), transport operators and etc.

France and Iran commerce laws do not provide a direct and consistent definition of commerce, but have enumerated a list of acts that are considered commercial.

Domain of Commercial law: According to the above definitions, commerce legally encompasses a wide range of actions. This term not only includes activities of people who are attempting to buy and sell goods, but also covers activities of industrialists, bankers, insurers, NAIC, brokers, agents and organizers of public exhibitions, transport operators and etc.

Electronic Commerce: Defined by the European Commission, E-commerce is based on electronic processing and transmission of data such as text, sound and image. This commerce includes other activities such as electronic exchange of goods and services, immediate delivery of digital content, electronic funds transfer, electronic stock exchange, electronic bill of lading, business plans, joint engineering and design, financial resources, government purchases, direct marketing after-sale service (Gladman, 1999, 5-7.)

- E-commerce consists of purposeful business activities accompanied with technical data that is done through electronic means.
- Sales of goods and services via computer through internet network.

- Using the internet for procurement, management and trade. According to this definition, activity of pharmacies and large retail stores is considered e-commerce.
- E-commerce is defined as the trade of goods and services with the help of telecommunications and telecommunications-based tools.

Some have used the term «E-Trading» and it also meant «E-commerce». Others have used the terms "preparation and distribution of goods the help electronic equipment", "electronic shopping", and "electronic marketing". Despite this, we should remember that usually a more broad meaning is meant by E-commerce – it means electronic business activity. Examples of e-business that are not considered E-commerce include patent, student enrollments and the work of the court.

1-2- Agents of The Parties of E-commerce

In traditional business, parties of the commerce include:

- Individual or natural persons such as a deal or commercial operations between natural merchants;
- between legal entities such as a trade between two companies;
- between legal entities and natural persons such as a trade between a corporation and a natural person;
- parties of an electronic commerce; in addition to the parties above, the e-commerce is also possible without the physical presence of persons or agents
- Commerce between a natural person and a computer system; in this case, when a base is the place of human interaction, a natural person originally by a legal entity enters into a contractual relationship with the computer system of another natural or legal person.
- Commerce between two computer systems; in this case, two computer systems are the parties of a contract or trade, and commerce takes place by means of two computer systems that act as the agent of natural or legal persons.

Considering that internet is rooted both in technology and the government it is that inevitable terms are used to describe common electronic commerce. The most familiar form of electronic commerce is "online" retail. And generally this method of commerce is called business to business (B2B). It is a kind of trade and commerce between companies or business units. The following terms are considered important in e-commerce and during the past decade have been defined in legal texts. Despite this, these terms continuously undergo revisions. (Freedman, *2002*, 9-10.)

1-3- Importance and Benefits of E-Commerce Law

In association with the benefits of e-commerce and electronic payment the followings can be outlined briefly:

- By using e-commerce and electronic payment, delays due to preparation of documents are over.
- By using e-commerce, since the data are not frequently logged in, potential errors are reduced.
- By using electronic payment, the time required to re-enter data in the system can be saved.
- By using e-commerce and electronic payment, cost of labor is reduced due to lack of re-entering the data into the computer.
- By using e-commerce and electronic payment, time delays in information flow become smoother and more reliable.

2-THE LEGALSTATUS OFELECTRONICDOCUMENTS

2-1- The Elements and Principles of Electronic Document

As defined in Article 1283 of the Civil Code: "Document is every script that is attributable as a claim or defense." And according to Article 6 of the law on electronic commerce, that "whenever a script is required by law, data message acts as a script" and according to the terms mentioned in the law of electronic commerce regarding data message, electronic document is considered "evidence" when it meets the following conditions:

2-1-1- The Ability ToInvoke

As previously mentioned, in order to call, in legal terms, script or data message a document, the script or data message must have the ability to be considered evidence in trial and be used to prove the claim in the lawsuit. In this regard, e-commerce law in Article 12 has explained: "Documents and evidence to prove the claim may be in the form of data message. And in any court or governmental body, the proof value of data message cannot be denied based on rules of available arguments simply because of the format of data message."

Therefore, acceptability and proof value of data message and electronic document have been emphasized. And data message, that certainly has the capability to solve dispute case and judicial unknown and create knowledge and certainty for the court, can be accepted as evidence. In digital environments, recording document should be in a way that in times of need it would possible to deliver and retrieve document and legislators officially recognize its validity.(Thaw, the NotaryPublic and its Impact in 21st Century, 2000, 18)

2-1-2- Access

Information and data messages can be accepted in the court as evidence when they have the ability to be retrieved and reviewed. In paragraph (A) in Article 8 of the law of electronic commerce in Iran this subject is clarified: This article states: "the desired information are available and can be used and referred to in the future." In the last part of Article 11 of Law on Electronic Commerce, definition of secure electronic record emphasizes that: in this Article, "secure electronic record is data message that is saved and stored by observing the conditions of a secure information system and, when necessary, it is accessible and understandable." (Valera, 2000, 18-19.)

2-1-3- Safe Production and Maintenance

Acceptance of documents in electronic format does not legally mean creating validity for all electronic information and data; but technical terms in the law of e-commerce have anticipated that if data messages do not have these conditions, they will not have the required legal validity. Article 14 of the Law on Electronic Commerce provides: "All data messages that are securely created and stored are valid and reliable in courts in terms of contents and signatures contained therein, obligations of the parties, or the party that has committed, and all persons who are considered legal surrogates." Therefore, data messages, firstly, should be created securely and, secondly, be kept in a safe place.

2-1-4- Electronic Signature

A letter or a figure that is printed at the foot of a letter or document is "Signature". And in some foreign texts, signature is defined as a name or symbol that shows signatory intent upon his/her acceptance of a script and its obligations, the signature is attached to the script or document. Electronic signature refers to any type of confirmation that is generated electronically and may be a sign, password, word, number, a typed name, a digital image of a handwritten signature or any electronic sign that confirms the identity. The signature is adopted by the person or his deputy and is attached to a contract or any other document. According to definitions of some jurists: Signature is to write first name or last name or both or draw a particular sign, indicating the identity of the owner of the mark, under the papers and regular or official documents, and this signature guarantees transaction, commitment, confession, testimony and so on.

One of the essential requirements of any document is the existence a sign on it. In fact, unsigned documents are unvalued and invalid. Documents assigned to individuals are attributable when they are signed. Unsigned document is incomplete and does not have the most important element of validity. However it may be used as an emphasizing symmetric for other evidences.

In paragraph (a) of Article 2 of UNCITRAL model law regarding electronic signatures that were approved on July 5th 2001, electronic signature is defined as: "Data in electronic format that is attached to a data message, or has become a uniform, associated and inseparable component of it; this data can

identify the signer of the data message and be used to verify the information contained in the data message signed by that person.(UNCITRAL Model Law,1996, 5-6.)

In paragraph 7 of Article 14 of the law model of the United States official documents office, electronic signature is defined as: "any sound, symbol or electronic process that is attached to the electronic document and is signed by someone who is going to accept the documents or has ordered the documents designed for him/her." In paragraph (J) of Article 2 of Iranian Law on electronic commerce, electronic signature means "any sign attached or reasonably connected to the "data message" that is used to identify the signer "data message".

Paragraph (k) of Article 2 and Article 10 of the mentioned law also consider conditions for "secure signature and electronic record". Mentioned definitions of electric signature are almost equal and from these definitions it can be concluded that this signature should be something that proves the followings:

1. Invoke; by signing a document electronically, the contents are attributed to the person and therefore can invoke him/her.
2. Formalities; digital signature of an electronic document indicates that all the formalities required by the law for regulating the document are done.
3. Verification; in case of using a digital signature to confirm the contents of electronic documents, this kind of signature functions like a signature in paper documents.
4. Having legal effects; digital signatures have all legal effects required for traditional signatures. In Article 7 of the Law Model (1996) and Article 3 of the Law Model (2001), "the principle of the unity of the effects of signatures, traditional and electronic documents» has been emphasized.
5. By a digital signature, special authenticity is given to electronic documents, thus the sender of the message or the verifier of the document can safely and reliably be identified. As a result, electronic documents are traceable, so activity of individuals in cyberspace finds legal aspects and therefore laws for paper documents are applicable in the case of electronic documents.
6. On the other hand, due to the impossibility of forging a digital signature, signed documents or messages cannot be denied by the signatory. Thereby, judicial authorities can use this feature to legally cite to an electronic document.
7. However, digital signature has another feature that manual signature does not. With digital signature, we can be sure that the content of the message or document will not change after signing and unauthorized individuals cannot alter the electronic document. This is because digital signature is produced for each document or message and is related to the text of the message. The produced signature for each document is unique.
8. Thus, by having the text of the document or message in addition to its digital signature, and by validating the digital signature, we can be assured that the content will not change. Hence, using the digital signature in addition to identifying the signatory adds a specific security to electronic documents and is called maintaining the integrity of the document. It means that the document can be seen and read but it cannot be altered or in other words distorted.(Electronic and Digital Signatures, 2004, 1-2.)

2-2- Reliable Electronic Interaction

Beyond the compliance with legal requirements concerning the feasibility, the main concern of the parties of electronic transactions is the issue of "trust". Conformity of electronic signature with legal requirements is one thing, and having a sufficient degree of reliability in electronic interaction – in a way that the person is satisfied with sending his/her products, transferring funds, and immediate commitment to contractual obligations – is another. Without a doubt, trust is very important in almost all interactions.

Regardless of interactions in cyberspace or in the traditional paper-based world, each party should have a level of trust and Reliability in order to be willing to do it. But trust has different elements and levels. Trusting business partners has always been important. Are they reliable? Will they fulfill their promises? But nowadays, in the electronic business environment, parties also need to trust the interaction itself. What is the meaning of "trusting the interaction"?

In important interactions associated with business which are dependent on the availability of computers and networks, the parties will need to know if these tools work effectively and without any interruption. When telecommunications replace physical meeting or reliable mediums such as post, the parties must be able to recognize each other's identity. When the electronic documents, that can easily be reproduced and changed, replace signed paper documents, the parties need a guarantee that ensures these documents are not counterfeit or changed. And when sensitive data are stored electronically, the parties should be ensured that the data are protected and available whenever they need them.(Menais, Electronic Signatures in France, 2002, 7-8.)

2-2-1- Recognizing The Authenticity of the Sender's Identity

Are the individuals, who we communicate with and exchange messages, really those they claim? Do identity and details posted by them really belong to them? As we said, the virtual environment of e-commerce has caused people to do their transactions remotely without seeing or hearing each other, and consequently, receiver of an electronic message has the right to be more cautious and authenticate the identity of message sender, he/she can recognize the real identity of the other party and be sure that the message is really sent by him/her. For example, in case a bank electronically receives a payment order to a third party, this institution must be able to identify the source of the order and ensure that there is no trick, and then the bank can proceed to make the payment.

The purpose of identification is to identify a user or any other entity, such as a software or hardware, in cyberspace. The service is used in many the security services in order to uniquely identify the relevant user, the authorized service or the target machine. In the real world for this case ID cards can be cited as an example. In the internet-based electronic interaction, the receiver must ordinarily ensure that the sender or the signatory of electronic letter is the same person who has sent the letter.

In order to achieve this trust, the Identity of the sender or the signatory needs to be determined and authenticated. It means determining whether the person is the one he/she claims to be. More specifically, this process includes confirming the identity of the alleged person. In the course of determining for example: Who is the source or origin of the letter? Who created or signed the document? Who has sent the document? Is the document genuine or false? (Lekkas, 2004, 11-12.)

2-2-2- Integrity of Data

The discussion on data integrity is about accurateness and completeness of the data such as documents and electronic messages sent by the internet or stored on the computer and guaranteeing that there are no unauthorized changes on the data whether intentional or unintentional. Guaranteeing data integrity requires protection of the data against destruction or adverse modification, for example by guaranteeing the originality of the data and the inability to deny it.

3-THE NATURE OF DOCUMENTATION ELECTRONIC SIGNATURE AND PUBLIC KEY INFRASTRUCTURE

In today's commercial environment, defining a framework to authenticate computer-based information requires familiarity with concepts and professional skills of legal and security aspects of computer. Combining these two areas is not an easy task. Concepts of the field of data security often do not match with the concepts of law. In terms of data security, "digital signature" is the result of a specific technical process on specific data.

The historical legal concept of "signature" is broad. From this perspective, any sign that intends to authenticate certain evidence is a signature. According to digital technology, nowadays, the broad concept of signature can include: signs, digital images of printed signatures and so on. From the perspective of information security, these simple electronic signatures, as already described, are distinctive from digital signatures. However, "digital signature" sometimes refers to computer-based signatures.

Proving the existence in a legal relationship, authentication of the relationship parties, and integrity of the content of the exchanged information are all required in the electronic environment which is immaterial

and virtual. This has guided practitioners of informatics law to find "electronic signature" or "ICT signature". To understand what is called the electronic signature, first, it is necessary to define it and then electronic signature types are examined. Then, we must investigate how secure digital or electronic signature is authenticated and can be invoked (Boss, 2001, 87-88.)

3-1- The Concept of Electronic Signature

Lexically it means Attending, finishing or enforcing a matter. In colloquial meaning it means writing the name or family name or a particular sign that shows the identity of the owner of the sign below the papers and documents (regular or official) and ensures the occurring of the transaction.

3-1-1- Imminent Signature

It is a signature that cannot be rejected or denied; such as the signature below an official document or the signature that its signatory confesses to issuing it. Imminent signature is used for comparison during addressing the authenticity of the denied and doubted signature (Article 225 of the Civil Procedure Code). Registered and validated signature is considered imminent signature by the certificate authority.

3-1-2- Signature and Rights

Signature is not part of the nature of the transaction; it confirms the form of the deal. The purpose of signing the script is one of the following:

(A) Reason: Signature acknowledges the script in addition to announcing the identity of the signer. When the signer uses a unique and distinctive sign, the sign is attributed to him/her.

(B) Formality: Signature makes the signer to consider to his/her act official and formal.

(C) Verification: In some cases, in accordance with law or custom, signature is an endorsement or confirmation of the script or the signer intends to create legal effects.

(D) Efficiency and Certainty: Signing a written document often shows the occurrence, clarity and certainty of the deal. Conditions of official legal transactions and required signature in various legal systems are not the same. And these conditions will change over time as well.

In some legal systems, deal or document do not invalidate due to the absence of a signature, but the courts, do not consider the lawsuits of these documents enforceable. Over the past century, in most legal systems, conditions have become more limited, or at least effects of failure conditions have been reduced to a minimum. Written documentation is likely to continue, and the beneficiaries or the parties are trying to comply with the formality, but in some cases information are computer-based, and in this way the paper is not used.

Although the basic nature of trading has not changed, but the law has been considering technological advances. Legal and business communities must adopt rules and procedures which use new technology To obtain the conventional effects of paper. For this purpose, signature must have the following attributes:

(A) Signature Authentication: Signature must show who has signed the document, message or evidence. It must also show that other entities cannot offer or use it without the permission of the owner of the signature.

(B) Document Authentication: Signature must show what is signed and prevent denial and rejection of the document or altering the document or signature. Signer authentication and verification of the document are tools to deal with fraud and forging. In terminology of information security, these tools prevent denial and refusal and these services are named "denial and refusal prevention services". These services provide the data source or data delivery by the sender and prevent denial and refusal of the receiver.

(C) Positive and Practical Action: Attaching signature should be a positive action that provides the procedures and means transaction.

(D) Efficiency: Signature creation and its verification process should authenticate the signature and document and also have the lowest cost (Winn, *2005*, 13-15.)

3-1-3- Digital Signature Technology

Digital signature is a kind of electronic signature which consists of series of mathematical data (codes) alongside a particular person who is the sender of the electronic documents. Digital Signature, with the help of a mathematic changing program, has a cipher form and authenticates the content of the message and the signer's identity. This signature also has a method to provide evidence of the specific sender. This feature prevents denying and rejecting the owner of the signature. Because of the secure encryption, the possibility of extracting the signature and attaching it to another document is almost ruled out.

Digital Signature is created and verified through encryption. Encryption is a branch of applied mathematics whose duty is to change messages into seemingly unintelligible forms and return them to the original form. Digital signatures often used "public key encryption".

Paragraph (e) of Article 2-1633 of the California Civil Code (America) states: "electronic signature is an electronic sound, symbol or process that an individual accepts it and attaches it to electronic documents."

Paragraph (y) of Article 2 of electronic commerce project states: "Electronic signature is any sign reasonably attached to the data message which is used to identify the signatory of the data message."

On the validity of electronic signature, Article 1633-7 of the Civil Code of California states: "(A) It is not possible to consider any document or signature without legal effect just because it is in electronic format. (B). No contract can be considered without legal effect because just it was signed using electronic equipment, facilities or documents. (C) If any law orders the requirement of written evidence, electronic document in this respect will suffice. (D) If any law orders the requirement of the contractor's signature, electronic signature will suffice."

Signatory of the electronic signature can be a natural person, a legal person or a computer system controlled by him/her.

Currently, there are at least three types of common electronic signature:1. Secure electronic signature2. Enhanced electronic signature3. The advanced electronic signature

3-2- Terms and Features of Electronic Signatures

Signing the document is a social affair not a scientific one. Document signing is an act upon which a person (A) shows he/she confirms the contents of the document and another person (B) checks this confirmation shows that he/she understands it. But making (A) committed to the document is never quite reliable. Any evidence that implies on such commitment is subject to question and doubt; in other words, signing documents requires take the risk.

3-2-1- Signed with The Private Key

The assumption is that when the document is signed with the private key of any person, it involves that person's liability. That person can deny and refuse; it is not impossible, but it is very difficult. This means that:1. Signature recipients have strong reasons that the signatory is the guarantor.2. Owner the key needs to be cautious; because the key can be used to sign any legal transaction and the owner of the key is responsible to prove that the signature is not authentic.

According to paragraph (b) of regulations of computer information networks approved in 2001 by the Supreme Council of the Cultural Revolution: "using any password for information exchange requires approval of authorities of registration, algorithms, and password key; applicant information is also in the secretariat of the information supreme council (or introduced authority). Otherwise it is prohibited."

3-2-2- Terms of Secure Electronic Signature

According to Article 10 of the electronic commerce project, secure electronic signature must meet the following terms:1. It is unique for every signatory2. It determines and shows the identity of the signer of the "data message"3. It is issued by the signer or his/her exclusive will4. It is somehow attached to a "data message", so that any changes in the data message can be detected and found.

3-2-3- Legal Signatures for Electronic Commerce

Signature in legal terms is a symbol adopted someone. To accept responsibility of the transaction, basically law does not prescribe that the act of signing must be accompanied with the safety rules. Therefore, signature, safety rules and reasons are separate topics. Not observing safety rules does not mean that the signature is void.

Signature righteousness and signature belonging to the signer are another matter. For example, a court in America considered the signature on a fax that this sentence was on it "I, X, immediately pay X $ in case of receiving X products from you" valid, because ownership of the text, handwriting and signature were proved and even more importantly the message also had the signature.

3-3- Validity and Effects of Electronic Signature

Article 14 of electronic commerce project states: "The keys of data messages are securely created and maintained. These keys are valid in terms of contents and signatures of the document, obligations of the parties or the party who has committed and persons who are considered their legal deputies. These keys can be invoked in the court and judicial system."

Article 15 of mentioned project states: "Denial and doubt cannot be claimed towards secure data messages, secure electronic records, and secure electronic signatures; it can only be claimed that the mentioned data message is a fraud; it is also possible to prove that the mentioned data message is legally invalid."(Berbecaru and et al, 2002, 15-16.)

3-3-1- Electronic Certification Service Provider

Article 13 of the electronic commerce project states: "Electronic certification service providers are units that are established in the country to provide services for electronic signature certification. These services include: production, export, storage, delivery, verification, cancellation and updating electronic signature authenticity certification."

Although the realm of electronic signature is wide, but it is not official and does not have credibility in case of testament, deed of trust, adoption, or divorce.

It is worth noting that some laws, concerning the electronic validity, have focused their attention solely on electronic signature (for example, laws that only follow the instructions of the Europe Union). And others include regulations that are about contract and related issues. From the latter category, there are laws inspired from the model law of electronic commerce of the United Nations Commerce Commission (such as e-commerce law in Hong Kong and e-commerce plan in Iran). Almost all laws consider fundamental and legal effects for electronic documents and signatures.(Birnbaum, Electronic Signature Comparison, 2001, 9-10)

3-3-2- Traditional Paper and Pencil Strategy

Signing traditional paper documents is subject to numerous risks; there is no standard method for signing with a pen. How to sign documents in order to find legal validity is not taught to anyone. The person is free to sign in any way he/she wants and even can change his/her sign every minute; conventional signature can be forged. Science can only help us know if the signature is authentic or not. Signature matching in this context can help us. As common signatures and recorded in the paper documents are at risk of denial and rejection, electronic signature can also be subject to such situations. To make the owner of the electronic signature committed to his/her signature, technology, offers a variety of new tools and strategies and electronic signature laws have also enacted provisions in this area.

Public key encryption, "PENOP" is among these strategies. In "PENOP" biometrics technology of pen is used. PENOP is a part of computer software which increases the performance of other applications. This method has two features:

1. Signature-Record Service: Specific data of handwritten signature is captured and saved on the screen of pen-based computer; this service receives information such as ID or user name which represents user's

identity based on his claim. It then commands the user to use the pen and write his/her signature on the computer screen. Therefore, the "PENOP» is legally equivalent to a signature on paper.
2. Signature Check Service: This service investigates and reports the authenticity of a signature.
Based on "PENOP" strategy, party (b) asks party (a) attach the biometrics sign to the document in order to sign the electronic document. In this method, signature's data such as signature's image, signature's writing speed, and other biometrics measures, are stored in computer memory and form the signature. This biometric signature is incorporated with the document encryption index; and the result is a signed document (Bacchetta et al, *1998*, 7-9.)

CONCLUSION

Considering basics and infrastructures is the first condition to enter the world of e-commerce and progress in this field. E-commerce law, despite some flaws and defects, should be considered as the Starting point of this process. Experience of other countries shows that in case of the realization of e-commerce, safety on one hand and rational claims on the other hand would be discussed. At first, creating and recording digital signature and then electronically recording electronic documents help with many imaginable problems in this field. In the case of electronically recording signatures and documents, the important thing is to "trust" the head of the bureau and try to achieve the latest standards. The latter one is so important without which electronic, efficient, and systematic recording would be unimaginable.
Every act of assigning recording, as described above, to a new organization or persons who do not have any expertise in the recording affairs, because they are unfamiliar with the principles and rules of recording, would be doomed to failure. Recording signatures and electronic documents obeys the same rules and principles that other documents and signatures (on paper and manual) obey. Contrary to the opinion of some, we cannot consider technology developments a pretext to violate principles and rules. Before anything "electronic recording" has to be recognized by approving proper legislation and assigning some of the official document bureaus to it after necessary training. Possibility of recording in both electronic and paper-based methods in these bureaus is the best available way to stop deviating from the principles and rules. Electronic recording bureau can record digital signature while backing up recorded documents, it can also deal with its daily affairs such as recording real estate.
The claim that creating centers, for signature certification and electronic recording, separately lead to more complex and formal electronic transactions, therefore, lack of interest in them is also doomed to invalidity. Just to be faster and cheaper makes major problems such as cheating, fraud and abuse in cyberspace, and proving issues harder. We cannot accept these major problems. However, by making detailed regulations, it is possible to certificate and record electronic signatures in one bureau in the minimum possible time. Making a balance between philosophy of expanding e-commerce and safety and reliability of it is the best option that can easily be achieved by electronically recording signatures and documents. As it was mentioned, about rules governing contracts, attempts have been made through electronic intermediaries so that significant differences and distances between the methods and tools of traditional commerce and electronic commerce do not affect legal aspects of the issue. Although UNCITRAL law model and the law of e-commerce in Iran do not have specific rules and basically their intention is not to login to the field of substantive law, but validity of contracts and contracts effects have been explicitly subjected to general rules. In conducting regulations of e-commerce, they have tried well to remove any inconsistency between these regulations and general rules as much as possible.

CHALLENGES AND SOLUTIONS

Launching and developing electronic commerce in our country face obstacles and challenges such as the followings:
1. The absence of necessary legal fields to use electronic commerce such as disclaiming electronic documents and signatures in current rules and regulations the country.
2. The absence of the system of electronic transfer of funds and credit cards.
3. Limited communication lines that are also slow in transferring electronic data.

4. Lack of E-commerce home network and related hardware and software in the country.
5. Large and small domestic organizations have little information on e-commerce and its benefits.
6. Relatively high initial cost of e-commerce for public and private companies especially small firms and lack of motivation in them to use this method.
7. Lack of culture and knowledge to use electronic commerce and internet network.
8. The need to protect the rights of consumers in electronic commerce.
9. Customs duties and receivable taxes of electronic commerce.
10. Providing necessary safety for electronic transactions and confidentiality of relevant information.

Considering the rapid expansion of electronic commerce in the world, using it is inevitable. The role of e-commerce in preservation, promotion and development of Iran's competitive position in the world and saving resources due to the implementation of e-commerce have made the government the Islamic republic of Iran use and expand e-commerce in accordance with following principles and policies: government of the Islamic Republic of Iran provides required basic infrastructures and legal and administrative fields to be used in e-commerce.

REFERENCES

Aliahmadi, M, (2001), A Position on Misleading Usage of Notary Terms in the Electronic Age A PositionStatement from the National Notary Association. Vol:2. Iran.

Bacchetta, M., et al.(1998) Electronic Commerce and the Role of the WTO, World TradeOrganization Special Studies 2, Geneva: World Trade Organization.

Berbecaru and et al, (2002) Toward Concrete Application of Electronic Signature, vol 4.http://security.polito.it/doc/papers/e_sign.pdf.

Birnbaum-Sarcy, Laurence & Darques Florence.(2001) Electronic Signature ComparisonBetween French&U.S. Law, International Business Law Journal, April .

Boss A, (2001) The Uniform Electronic Transaction Act in a Global Environment, IdahoLaw Review, Vol. 37.

Directive 1999/93/Ec Of 13 December (1999) On a Community Framework For Electronic Signatures, A Copy of Electronic Signatures Directive is Available At:
www.europa..eu.int/hnformationsociety/topics/ebuisness/ecommerce/8epolicy_elaw/law_ecommerce/legal/index_en.htm.

Electronic Records Management Guidelines Electronic and Digital Signatures (2000).

Electronic and Digital Signatures, State Archives Department, MinnesotaHistorical Society March (2004), Vol. 4

Electronic Signature in Global and National Commerce Act [Esign].EffectiveOctober.1, (2000).

Freedman, Bradley J. ,(2002) Electronic Contracts Under Canadian LawA Practical Guide,Manitoba Law Journal, Vol 28 N0 1.

Gladman, Brian, Ellison, Carl and another author. (1999). Digital Signatures ,Certificates & Electronic Commerce, Version 1.1, revised 8th June, Digital Signatures, Certificates and Electronic Commerce. http://jya.com/bg/digsig.pdf

Lekkas, Dimitris&Gritzalis, Dimitris. (2004). Cumulative Notarization for Long-TermPreservation of Digital Signatures, Computer&Security Information .Vol 3.

Menais, Alexandre. Electronic Signatures in France (2002), Vol 6, Available at
http://www.juriscom.net/en/pro/1/ec20020730.htm

Ramberg, Christina Hultmark. (2001). The Ecommerce Directive and Formation of Contractin a Comparative Perspective, 1Global Jurist, Iss. 2, art. 3, Availableat:
http://www.bepress.com/gj/advances/vol1/iss2/art3.

Smedinghoff, T. J. and Bro, R.H. (1999), "Moving with Change: ElectronicSignature Legislation as a Vehicle for Advancing E-Commerce," The John MarshallJournal of Computer&Information, Vol 17, pp. 723-768.

Thaw, Deborah M. (2000), the Notary Public and its Impact in 21st Century, APresentation at the NACO/NACRC Annual Conference, Available.

UNCITRAL Model Law On Electronic Commerce With Guide to Enactement(1996), Available atwww.uncitral.org/english/texts/electcom/ecommerceindex.htm.

UNCITRAL Model Law on Electronic Signatures (2001), Available at: www.uncitral.org/english/texts/electcom/mlelectsige.pdf.

Valera, Milton G. (2000), A Presentation To The Multi State Digital Signature Summit ,National Notary Association,Vol 3, Chatsworth, California Marines"" Memorial Club&Hotel San Francisco, California Friday, August 11.

Valera, Milton G. (2006). In Notarization, There is no Substitute for PersonalAppearance–Despite Technology, A Presentation to the Property

Winn, J. K., (2005), Idaho Law Review Symposium: on Uniform Electronic Transaction ActThe Emperor""s New Clothes: The Shocking Truth about Digital Signatures andInternet Commerce ,Vol 4, at:http://www.smu.edu/jwiztn/shockingtruth.hlmt.