J. Appl. Environ. Biol. Sci., 5(10S)441-449, 2015

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

Examining the Validity of Electronic Signatures in the Law of the Islamic Republic of Iran

Amir Abbas Shekarian

MA. Low, Azad University Tehran, Markaz

Received: April 20, 2015
Accepted: June 15, 2015

ABSTRACT

Growing increase in Electronic Commerce has been led to the replacement of cyberspace with the traditional way of doing things. Since electronic commerce is the main subject in electronic contracts, and that the contracting parties are almost not present in a same place, and that usually a handwriting document is not set, hence the electronic signatures and particularly digital signature are used as a way to identify the identity and the intention of the parties to be bound to the contents of electronic contracts, as well as to ensure the integrity of an electronic document.
It is explained at this study that the electronic signature, due to its specific rules and provisions, has a distinct nature from handwritten signature and seal.
In addition, according to the provisions of Electronic Commerce Law of Iran (2003), electronic signature is divided legally into two types of simple or ordinary and secure. Moreover, the rights and obligations of the parties as well as evidential value of electronic document along with them are determined on the same basis.
However based on the usual methods of technology, electronic signature may be divided into the simple, biometrics, encryption based, and digital methods, and that these methods determine largely the validity of electronic signature and document with it. According to the mentioned law, electronic signature, whether ordinary or secure, is valid and its validity is determined due to the secure factors such as appropriateness of employed safety procedures with the subject, and the purpose of exchanging the "data message".
According to the terms provided in Article 10 of the law of Electronic Commerce of Iran, an electronic signature will be considered as digital signature if : a) be unique to the signatory; b) Identify the signatory of "data message" ; c) Be signed by the signatory or under his/her sole intention ; d) Be affixed to “data message” in a way that any change in data message can be detected, and according to the article 32, the authorities that issue the secure electronic signature are subject to hierarchy and include" Primary Certification Service Providers” "intermediate Certification Service Providers" and "certificate registration offices.”

KEYWORDS: signature, electronic and digital signature, data message, electronic evidence, legal validity, enforceability, conflict of evidence, cryptography, Certification Service Providers.

INTRODUCTION

By approaching to the global village, and the development of information and communication technologies, we can see overrule of the former traditional system and replacement of cyber and electronic space with it, and adding electronic suffix to all former activities.

Electronic commerce, electronic banking, electronic contracts, electronic signatures, electronic government, electronic university and so on, are of them. Doing things electronically leads to facilitation of affairs, reduction of traffic and movement of persons, elimination of paper and paperwork, reduction of costs and creation of business environment. Imagining a world without computer is not possible anymore. If the banks have once considered encouragements to convince people to pay electronically the bills of water, electricity, gas, and phone, or offices and agencies to do the affairs of clientele in this style, now they force people to do this, and don’t accept anymore doing affairs traditionally.

Implementing affairs electronically require making cultural infrastructures and eliminating the space of doubt and making confidence.

Once electronic commerce had been used simply for buying, selling, and electronic payment among private companies that have invented it, but gradually it has included any production, sending and receiving and processing the data messages by means of optical, acoustic, visual, electronic and other incoming technology means, and that it also contains all natural, judicial, and public persons. Since the use of electronic commerce to carry out its alternative affairs instead of the traditional system, is of western inventions, hence in order to avoid backwardness

*** Corresponding Author:** Amir Abbas Shekarian, MA. Low, Azad university Tehran, Markaz

of development and technology, and in order to be in line with them, regardless of the current legal foundations and only by taking into consideration the technical issues of the case, the regulations of the law of electronic commerce were translated quickly, and the executive By-law of Article 32 of the Law of Electronic Commerce of Iran, which should have prepared by the Ministries of Commerce, Ministry of Communications and Information Technology, Economic Affairs & Finance, and Justice, and the vice president of strategic planning and monitoring of state president, eventually was prepared and the Ministry of Commerce drafted its concerning guidelines. Finally and after completing its work, it was approved by mentioned authorities.

The use of non-legal terms such as "deem as official document" and " deem as valid document" in Articles 14 and 15 of the electronic commerce law of Iran, and the fundamental change in definitions of electronic registration and certification in accordance with the terms of the law, and that it is not necessary for the officers of Certification Service Providers to be lawyers and their mere awareness of the technical aspects of electronic and software means will be adequate, and that identifying the identity and the capacity somewhere, issuing the certification elsewhere, are of innovations that are unique in their kind, and that they are the result of neglecting the legal and judicial matters.

In addition, lack of attention of Lawyers and being out of the date of their information, and their inaction, might be involved in this process.

2-Part 1: Identifying the Sign

2-1) Concept, Nature and Types of Electronic Signature

A) Definition of signature and its function

In Arabic, “sign” means to view, and in Dehkhoda’s Dictionary is defined as: to permit-to endorse, to certify and a sign leaved at the end of a document, as well as to write ones name under the letter or document as the confession and acknowledgment.[1] Iran’s law does not provide a definition of the signature, however the most comprehensive definition of signature is "to write name, surname or both, or to draw a certain sign-that indicates the identity of the owner of the mark- in normal or official documents, which involves occurrence of transaction or commitment or confession or testimony and so on, or that later must be recorded on those papers, obligation or transaction.[2]

In most countries, people sign the documents simply by writing their name and surname, while in Iran the signature has mostly a graphical mode.

It is inferred of the whole of definitions of scholars that, the signature does not necessarily include the author's name, but can be a sign that will determine the identity of the signatory, and on the other hand, signature is divided into graphical, linear and handwritten. Therefore, the signature seal, is not considered as signature.[3] Article 311 of the Commercial Code explicitly provides that the check must be signed by the exporter and that this signature must necessarily be handwritten. Therefore, the signature seal has not authenticity in check issuance.[4]

Usually, a signature provides following functionality:

1. Identification and characterization of a person who has signed the document.
2. Attributing the contents of the document to the exporter of signature and certifying his/her consent.[5]
3. Proving the consent of the person upon the provisions of the document signed by other person.
4. Proof of the fact that the person has signed the document in a specified time and place.[6] (It seems be difficult proving this matter except unless for documents set out in the institutions of official documents, governmental offices, and courts.)

B) The Nature of Electronic Signature

Before the development of electronic signature, signature and seal were used to attribute the document and actions that except to the use of signature in issuance of the check,[7] both have the same value.[8]

Now regarding that the law has not defined the signature and that only in Article 1301 of the Civil Code, a reference is made to one of its effects, a question emerges that what is the nature of this newly entered to law phenomenon (i.e. electronic signature).

As to the nature of the electronic signature, three views are suggestible:

---

[1]Dehkhoda, Ali, Akbar, Dictionary, Volume 2, First Publication since the beginning of the new term, Tehran University Press, 1993, P. 2877.
[2]Langeroudi Jafari, Mohammad Jafar, terminology of Law, Vol. 5, Ganje Danesh Pub, Tehran, 1991, p. 81.
[3]Sadrzadeh Afshar, Seyed Mohsen, conflict of evidence in the Law of Iran, Tehran University Press, 1999, p. 129.
[4]Fakhari, Amir Hoseyn, lecture course in commercial law 3, Imam Sadiq University, 2003-04 second semester of study.
[5]Mason, Stephan, Electronic Signature in Practice Journal of High Technology Law. Vol, No 2,2006, p.159.
[6]Uncitral. Model Law on Electronic Signatures with Guide to Enactment 2001, N.530.
[7] Article 311 of Commercial Code: “the place and the date of the check must be written and signed by the exporter. Payment cannot be delayed. "
[8]Rezaei, Ruhollah, authenticity of electronic documents (in accordance with national and international regulations) MA thesis on private law of Imam Sadiq (AS) University, 2006, P. 87, quoting by Yaqubifar, Omid, investigating electronic signature law, master's thesis on International Commercial Law,, Shahid Beheshti. University.

- Given that the legislator in Article 6 of the law of electronic commerce deems electronic signature as handwritten signature, it can be said that handwritten signature is similar in nature to electronic signature, and that there is no difference between the two.
- Other lawyers considered electronic signature as equal to seal.

According to one of these lawyers whose view is placed in this category, "electronic signature is nothing but a set of mathematical formulas that is confirmed by the signature certificate authorities and is presented to the people, and although they are named under the title of signature, but because they are produced by a third party and are allocated to individuals, and that individuals use them only in the form that they are, in legal analysis they are deems as seal.[9]

- The third assumption is the case that due to the unique characteristics of electronic signature, we not try to put it in traditional forms, and accept it as a new concept deriving of development of technology and information.

Legislator, by stating in the Article 6 of the Law of Electronic Commerce that " When the existence of a written document is deemed legally requisite, "data message" can be used as a replacement...." has cleared the task of the documents to which electronic signature is appended, and deemed them written.

2.2- Legislative Views in relation to Electronic Signature

Laws and regulations regarding electronic certification methods developed at national and international levels, are in various forms. Three various understanding may be recognized of certification methods and electronic signature:

2-2-1- Minimal View

Some countries have followed a policy of neutrality of technology about electronic signature, and normally have accepted all forms of electronic signature.

According to this view, electronic signature is considered as functional equivalent of handwritten signature, provided that the used technology has been developed in ways that could lead to some special results, and on the other hand, can answer some expectations in terms of reliability.

UNCITRAl Model Law on electronic commerce contains a set of legal measures that are used widely to realize general functional equality between electronic signature and the handwritten signature. Paragraph 1 of Article 7 of the Model Law provides: when the law requires the signature of special persons, this expectation is met with a data message:

A) If a certain method is used to identify concerned person, which must confirm the information content of the data message;
B) In the event that this method is sufficiently reliable in terms of the subject, for which the data message has been developed or sent, by taking into account all circumstances, including any agreement in this field.

According to this view, all of the technologies that can provide the two main functions, namely identifying the signatory and the knowledge of his/her intention as to signed information, can be perceived as responsive to the requirements, which should be gathered in a signature with legal effect. Therefore, the model law is neutral in terms of technology.

In other words, the law does not require the use of a specific form of the signature, and does not precondition the use of a special method, due to the speed of technological innovation, this neutrality of the law is important, since it may include all future forms of electronic signature, and thus, the future developments in technology are welcomed.

2.2.2- Special Technology View

With the emergence of economic commerce and the replacement of cyberspace with traditional space along with a number of advantages including elimination of paper and paperwork, and reduction in traffic, and intermediation, and reduction of the costs, existence of cyber thieves and hackers, led the legislators' by this view to think about developing some rules concerning electronic commerce, and thereby ensuring the integrity of the exchange and information, and to prevent unauthorized access of data.

From the perspective of special technology view, because of validity of electronic signature according to the law, the applicable rules shall be applied to determine the useable technology.

Similarly is when the law finds necessary the public key infrastructure-based systems to guarantee maximum security. Views that impose the use of a particular technology are also referred to as imperative views.

At this approach, the legislature requires confirmation of a third party for electronic signature that in fact is equal to Certification Service Providers in the law of Iran.

This confirmation is not only used to identify the signatory, but also to affirm the integrity of data message with it. Moreover, in these rules, there is a requirement that the electronic signature shall be under the full control of the signatory.

[9]Sadeghi, Neshat, Amir, .analysis of legal aspects of electronic payment, Essay Collection of the Conference on examining the legal private aspects of Information Technology, 2004, p. 170.

According to this approach, other types of electronic signature except digital signature are not recognized as equivalent to a handwritten signature, and a person that invokes to any type of electronic signature other than digital signature with the conditions prescribed in the law, has to prove its validity.

For example, according to Article 5 of the digital signature act of Argentina: "electronic signature is a set of integrated electronic data that is attached to another data message or is logically associated with it, and is used by a signatory to identification of a person that lacks any element that can be considered it for digital signatures.

3.2.2 Dual View

According to this view, the law specifies minimum requirements that must respond to the electronic certificate methods, so that a minimum legal framework could be shaped. In this view, important legal effects are considered to some forms of electronic certificate (that sometimes are called as secure, advanced, and enhanced electronic signature or valid certificates).

Unlike the approach of special technology on which the legislature considers electronic signature as the only acceptable type of secure digital signature, and considers acceptance of its other types subject to proving their accuracy by the claimant.

In dual approach, according to the legislature, validity of secure electronic signature is depended on specific conditions that is already achieved mainly through digital signature. However, evidently with advances in technology, more safe methods in future will be possible.

For example, in electronic commerce law of Iran there is not a provision that validate only the digital signature. In fact, in this Law even the name of digital signature is not mentioned.

This view is mainly followed by countries that believe their legislators must determine a number of technical standards, and yet open the way for advances in technology. The discussed view is seeking to balance between flexibility and confidence in context of electronic signature, in a way that the parties be free to decide-with regard to trade procedures- whether according to their needs, the required costs and difficulties of the use of safer method is justified or not.

Singapore and the EU countries are the first countries that have adopted laws based on the dual view.

3.2 Comparison of the electronic and traditional signature

3-2-1- Differences

1. Electronic data can be stored and signed in a very compact form, so they can be filed easier due to their low content. On the other hand, they can be easily hidden. for example a hard drive contains more than 5.1 million pages of data and a corporate backup tape, about 4 million pages of data, while, if these documents are stored in paper form, their keeping requires a large space.[10]
2. Electronic signature, despite signing a piece of paper, is not tangible and objective, and therefore is not easily achievable, but is simply readable through the software that has created it, and if the program is not available, the document will not be available.
3. Electronic signature is almost never wasted. Although users often assume that they destroyed the folder by a delete command, the deleted copies are usually retrievable. This feature is a golden advantage for electronic signature because the litigants will faced an unexpected situation, while by ripping and discarding the paper document, one can be permanently sure of its destruction.

4-Electronic signature as electronic data are easily multipliable and when concluded are stored in various locations such as log files and document header, hence it is difficult to remove them all. Therefore, even if the main folder is deleted, the backup copies will remain.[11]

5-electronic signature often contains valuable information such as date of creation, change and deletion of folders, and the date of changing the password that can be evidence in detecting the truth, while the traditional signature lacks such information.[12]

6- people often save their confidential information on computer and send their unofficial letters via e-mail, and in these cases, are less inclined to use paper document, therefore, the computer data often contain information that change the course of the proceedings.

7- The electronic signature is subtle and so can easily be changed, and that one can easily hide its change with the help of technical knowledge. However, traditional signatures are in fact the unique physical samples, and for

[10]Rockwood, Rebecca, "Shifting Burdens and Concealing Electronic Evidence: Discovery in Digital area", Journal of Law & Technology, Volume xll, Issue 4,2005,p. 120

[11]Gatten, Allen, electronic evidence, translated by Mosayyeb Ramezani, Tehran, Secretariat of the Supreme Council of Information communication, 2004, PP. 9-11.

[12]Young, Douglas, "Advising the Corporate Client on the Duty to Preserve Electronic Evidence", 2001, p.3. aa: www.fbm.com/docs/publications/e 4 c58e30-9D15/4950-9AC8-30CCB4.document.pdf.

changing a paper document, it must be physically manipulated. Therefore, its change is difficult, and that this change is readily discernible.[13]

2.3.2-Commonality Aspects

To see what commonalities exist between traditional and electronic signature we have to see what is the function of traditional signature and that whether such function can be found in electronic signature.

As we know, the signature is used to identify the person who has signed the document, as well as to identify the person's intention to confirm the contents of a signed document.

In other words, through the signature we can determine attribution of the document to a person, and what is confirmed by His/her signature, so we must consider the document before signing as a draft that is the subject of study and contemplation about which a final decision has not been made yet.[14]

As to the influence of the signature, it can be said that by signing a document, some right and duty will made to the person.

A right is made because the person can invoke his/her signed document as evidence, and a duty is imposed since others can use his/her signature in the document against him/her.

However, in Article 1301 of the Civil Code, there is only a reference to the second effect i.e. the signature may bebe used as an evidence against the signatory. However, the person can also invoke subsequently to the contents of a document that has signed it in-for example- notary publics and courts.

As we know a claim for forgery or denial and doubt may be filed about the signed ordinary documents, in other words, someone who wants to invoke to the ordinary document as evidence, has to prove its correctness, and the correctness of its signature. However, as to the official documents, the correctness principle is prevailing and only a claim for forgery may be brought on them.[15]

It should be noted that according to the Article 1291 of the Civil Code, ordinary documents in two cases have the influence of official documents, and are valid on the parties, and their heirs and deputies.

1. Where the party who the document is filed against him, confirms its issuance by alleged person. 2.Whenits proved in the court that the concerned document is in fact signed or sealed by the party that has rejected this.»

Now that we are familiar with the function and the effects of the handwritten signature, it must be seen that whether the electronic signature has these two functions. In paragraph (j) of Article 2 of the Law of Electronic Commerce, legislator with the term "data message is used to identify the signatory", and also in paragraph (b) of Article 10, has referred to such function of the electronic signature in relation to the secure electronic signature. However, the question arisen here is that, as we know, according to the law of electronic commerce, electronic signature can be any sign that is annexed to the data message, or is attached it in a logical manner.

3- Electronic Reason

3-1- Definition, Resources and Consideration of Electronic Signature is as a Reason

3-1-1- Definition of Electronic Reason

Literally, "Reason" means to guide, and in customary term, refers to anything that would prove the unknown. Reason has two functions in law.

The first category contains reasons that are made before occurrence of any dispute and difference, as the keeper and protector of the right, so that be invoked in case of arising a dispute, like a contract concluded between people. Such reasons are referred to as prepared reasons.[16]

The second category consists of the reasons such as examination of the situation and investigation of witnesses that are used by parties when an action is filed, and during the proceedings to prove or defend the claim. This category is called formal or phenomenal reasons.[17]

Philosophy of this division is underlying in the law governing the reasons. As to the validity and the influence, the prepared reasons according to their law, are subject to the time of conclusion, but formal reasons are subject to the law applicable in the proceedings. Moreover, the examination and study position of the prepared reason is in civil law, while as to the formal reason, this happens in the civil procedure.[18]

In civil code, there is no reference to the definition of the reason, but in Article 194 of the Procedure Law of Public and Revolutionary Courts of Iran, the reason is defined as follow:

"Reason is a tool that the parties to a dispute invoke to it in order to prove or defend a claim."

[13]Zarkalam, Sattar, "The Law of Electronic Commerce and Electronic alphabet", Ibid., PP. 285-302.
[14]Katouzian, Naser., proof and Reason of proof, Ibid, P. 202.
[15]According to Article 70 of Law of Document Registration, a document that is officially registered under the applicable laws, all contents and signatures contained in it shall be assumed as valid, unless its forgery is proven."
[16]Ibid., P. 42.
[17]Ibid., P. 42.
[18]Madani, Jalal, Proof Evidence, Vol 5, Paydar publication, 2000, p. 27.

According to Article 1258 of the Civil Code and the section 10 of the Procedure Code of Public and Revolutionary Courts on Civil Matters, the reasons are as follow:

1. Confession
2. The written documents
3. Testimony
4. Evidence
5. Oath
6. Examination of the situation
7. Local Research
8. Expertise

3-1-2- Electronic Signature as Reason

According to article 194 of the Code of Civil Procedure (2000), "Reason is a tool that the parties to a dispute invoke to it in order to prove or defend a claim." Of course, it is important to mention that the reason may be invoked in non-litigious matters, or that in some cases, the judge and not the parties, invoke to it.[19]

Article 1301 of the Civil Code provides that "a signature on a writ or document is a reason against the signatory". The article has ignored the issue that the reason may be evidence for the signatory.

The first raising question is whether one can principally consider the data massage which the text of contract is in its form, and that is associated with the electronic signature, as a writ?

In fact, this question is referring to the challenge that is facing the electronic documents, which is unconformity with the old and conventional concepts and categories of evidence. Regulations of Some countries like Germany do not consider the electronic document as writ.[20]

Article 6 of the Law of Electronic Commerce of Iran gives another answer to this question: "When the existence of a written document is deemed legally requisite, "data message" can be used as a replacement. "However, it should be noted that this written is capable of being invoked if is signed and before signing, is not a perfect and renderable document, and lacks the most important element of validity.

3-2-legal principles governing the positive aspects of electronic signature and the proof of evidential valueit in the open and closed systems.

A) Principle of the Acceptance of Electronic Signatures

Among the principles that govern the evidential aspects of the electronic signature, is the principle of acceptance of electronic signature in the courts and offices, and any court and office cannot reject this kind of reason due to its form. This issue is also stated explicitly in Article 12 of the Law of electronic commerce. Evidence and any supporting document may be in the form of "data message". The evidential value of a "data message" can by no means be repudiated solely due to its form and framework at any court or governmental office. The law of electronic commerce in most countries accepts this principle.

B) The Principle of Equality of Handwritten Signature and Electronic Signature

As mentioned in previous discussions, because of the necessity to use cyberspace for removing the paper and to facilitate the direction of legislator camaraderie with advance and technology, Article 7 of the law of economic commerce that provides "Where the law requires a signature, an electronic signature may suffice", has passed.

According to this principle, which its equivalent is provided in paragraph one of Article 6 of the model law of electronic signature(2001),and paragraph one of Article 7 of the Model Law of Electronic Commerce(1996,) there is no difference between handwritten signature and electronic signature, and both of them are indicating the intention and identification of the person, confirmation of the contents of the document, and the attribuance of the document to the signatory.

C) The principle that "data message" is deemed written

According to the Article 6 of the Law of Electronic Commerce of Iran: When the existence of a written document is deemed legally requisite, "data message" can be used as a replacement..." namely data message has the same evidential power as the paper. In this regard, the judgments issued by foreign courts are confirming these subjects:

1- In case "Carlos Samper v. Jain Taypas" the judge held that wherever the regulations require the information being in the written form, an electronic letter will be sufficient, provided that the parties have not access that letter after sending it.[21]

[19]Langroudi Jafari, Mohammad Jafar, Law Encyclopedia, V 4, 4[end] Edition , Tehran, AmirKabir, 1997, p. 313.

[20]Wike, Daneil, Providing Evidence with Transformed Signal Documents, 2006: aa: www.dzi.th.darmastadt.de/fileadmin/content/veranstatal tungen/2006 060609- etricks/wilk. pdf.p.6.

[21]Mason, Stephan (2006) Electronic Signatures in practice, Retrieved 2008/4/20 from http://www.Law, Suffolk.Edu/highlights/ strops/ jht/pdohcation/ v,n2/mason pdf.

2- In case “Rudder v. Microsoft” the Court stated that “electronic contracts concluded by clicking are given the same validity as written contracts”.[22]

It is noteworthy that according to the principle that "any generic is allocated by an specific”, the general rule that the data message is deemed written, faces with exceptions under the continuance of Article 6 of the Law of Electronic Commerce .Exclusions are as follows: "(a) Ownership documents of immovable property. b) Sale of medical materials to the final consumers. (c) Announcements, notifications, warnings or the like statements issuing a particular provision on the use of goods or prohibiting the use of certain methods or their omission hereto.

Paragraph 3 of Article 6 of the Model Law on economic commerce (1996) has devolved the exceptions of this principle to domestic law of the countries, with the exception that "national laws have not permission to impose unlimited exceptions to this rule, because otherwise the possibility of implementing the model provisions cannot be provided."

3-3-the Burden of Proof on the Electronic Reasons and Their Conflict by other Reasons

3-3-1- Burden of Proof

As we examined, the evidential value of the electronic proof is determined regarding the type of proof, so in order to determine the evidential value, the judge must at first know the form of reason.

But what is the burden of proof? In electronic commerce law, the general principle is normality of electronic documents, and in order to be considered as a secure reason, these documents must have the conditions mentioned in the law. We have analyzed in detail these conditions. So if one claim that the reason is secure, he will considered as a claimant in this case, because his/her statement is opposing to the principle, and according to the rule "exceptions strictissimae application is”, claimant undertakes burden of proof, and in order to prove this, the following point is to be proved:

1. That the signature contained in the document has the criteria laid down in Article 10 of the law of electronic commerce about secure signature.
2. That the created, stored, or document processing information has the conditions mentioned in paragraph (h) of Article 2, about the secure information system.
3. That the document after being created is kept secure by respecting the terms laid down in Article 11 of the Law of Electronic Commerce about the information background.

In order to identify these cases, the court refer the matter to an expert, and identifying each one of these matters requires spending a lot of cost and time, and that this difficulty reduces the admissibility of electronic evidence and the holder of a secure electronic evidence may lose in action due to the inability of proving the proof.

In order to dispense with the claimant of this difficult task, it is appropriate to introduce some available technical procedures that have confidence conditions, as evidence of proof certainty.

Draft Law of Electronic Commerce, in Article 127 was predicted a committee called technology and standard committee of information systems, so that through studying on the latest scientific achievements, introduce the best available methods by publishing a guidance, and that the introduced technologic methods could be accepted in courts without the need to prove the certainty, but unfortunately this paragraph was removed in the final regulation.

Currently, the digital signature issued by certificate service providers are assumed as secure, the standard used in these institutions are always updated by the governmental Commission of public key infrastructure, and complies with the prevailing international standards. Therefore, if the parties to a dispute invoke to the signature issued by these institutions, they will be excluded from proving the certainty.

In addition, the Law of Electronic Commerce in Article 16, gives accuracy to any data message that is recorded and retained by a third party in accordance with the provisions of Article 11 of this Law, is deemed valid.

It seems that the purpose of this Article is providing the assumption of certainty to the data message that is recorded and retained by electronic service offices. However, there is no authority to perform this task yet.

3-3-2- Denial of Authenticity of Electronic Documents

Denial of the authenticity and credibility of electronic documents occurs in two ways. Sometimes a denial is launched on its authenticity, and occasionally a claim for forgery is expressed. We will illustrate these as follows:

A) Statement of Denial and Doubt

As we know, only in respect of ordinary electronic documents a denial or doubt can be stated, because under Article 15 e of the law of electronic commerce, secure documents may not be questioned or denied; only a claim of forgery of a "data message" or a proof of its invalidity on a legal basis may be considered and denial means declaring the

---

Quitted by Mazaheri, Rasoul, and Nazem, Alireza, “ the Concept and the Effects of Electronic Signature in the Law of Iran and UNCITRAL Provision, Journal of Clerks and Notaries, No. 86, pp. 103.

[22]Mason, Stephan Electronic Signatures in Law, London: totted publishing 2007.

rejection of pertaining manuscript, signature, seal, or fingerprint of the informal document to attributed person by his/her. Uncertainty means refusing the assignment of manuscript, signature, seal, or fingerprint of informal document to assigned people by someone else,[23] which in electronic proof, is realized in the form of refusal of attribution of the electronic signature under document.

Proofing for attribution in paper documents is implemented through comparing the manuscript, stamped signature or fingerprint of the denied or doubted document with the manuscript, signature or fingerprint of the certainly issued documents. But in the case of electronic documents, except documents authenticated by bioassay signature with biological-behavioral characteristics, and by comparing the existing sample with what is archived in database, in other cases, the technical safety methods used in the document shall be applied to prove the authenticity of the assignment of the document. Legislator in Article 13 of the Law of Electronic Commerce has assigned to the judges the determination of the effect rate of safety methods in attributing document to the issuer by considering secure factors, and the judge make decision taking into account the private agreement of the parties, circumstances and customs prevailing the occurred exchange, if they, regarding the ruling custom as to using the password for withdrawal of a bank account, and regarding the obligation of the account holder not to disclose his/her password, consider it as the reason of assigning the document to issuer.

(B) Claim of Forgery

A claim of forgery is a claim that may be filed against both the simple and the secure electronic signature. In accordance with Article 523 of the Islamic Penal Code, forgery is: "creating writ or document by the signature of official or unofficial persons, (by) scratching or scraping or removing or accession or sealing or proofing or(by)blacking or advancing or delaying theactual date of the document, or attaching a writ to other writs, or using other's seal without his/her consent and so on with the intention of forgery. "

Obviously, some of the mentioned examples of forgery in the above article are appertain to the paper documents, and there is no words such as corrosion, scraping, and scratching. Legislator in section 2, sub-section 4 (fines and penalties) of Article 68 of the law of electronic commerce, under the title of computer forgery has listed instances that can be considered as forgery in cyberspace, and among themwe may refer to change, fade andto stop the data message in the context of electronic transactions, to interfere in processing the data message and computer system, an unauthorized use of operational devices of encryption systems such as specific key in creating the signature, as well as creating signature without precedent in the list of electronic offices.

If a forgery is executed in the case of electronic documents verified by digital electronic signature, according to the algorithm (hush Function) it can be proved that the signed text has changed.

Conclusion

This study has attempted to introduce a satisfactory answer as to the important and essential issues in relation to the electronic signature, and because of existing reasonable and yet controversial views and arguments in this field as other fields in law, we were trying to choose the best ideas with logical arguments, and to examine other views.

In summary, it can be said that the results of this research are as follows:

1.as to the nature of the electronic signature it has been argued that some consider it as a handwritten signature, and some other see it as a seal, and of course, the criteria of these two views is similarity and the same function of a handwritten signature, and seal with the electronic signature. However, it seems that the electronic signature be a new concept that has entered into the legal literature of the country, and given that the legislator has introduced the new and separate rules in this regard, then there is no need to analyze it according to traditional rules.

Nonetheless, in accordance with Article 7 of the law of electronic commerce, electronic signature, whatever its nature, can be used at least in most of the fields instead of a handwritten signature.

2.`The second question answered in this article was about the types of electronic signature and the evidential value for each of them.

As mentioned above, commercial code of Iran has not divided the electronic signature in technical terms, and only in article 10 has listed the terms of a secure electronic signature. Although in this case, legislator has not mentioned the other type of electronic signature, but due to the context of the provisions, as well as paragraphs (I)and (J)of Article 2 of the mentioned law, and the background of drafting similar laws in other countries, we find that each electronic signature that lacks the conditions stated in Article 10, shall be identified by another title that Iranian lawyers have chosen the title of "simple ordinary electronic signature" for it.

According to Article 13 of the Law of Electronic Commerce "positive evidential value of data message is, both normal and safe, is determined considering the safe factors such as congruence of safety procedures employed with the subject and aim of exchanging the data message.

[23]Shams, Abdollah, Civil Procedure Code, Vol. 3, PP. 182 -184.

Thus, according to this article, electronic signature and document, both normal and secure, is valid, but this article gives a certain validity to electronic signature and documents with it, so that in accordance with Article 15, simply a forgery claim can be brought about this type of signature, and denial and doubt it is not heard about them.

In this respect, electronic signature, has an “administrative capability" like official documents ", but unlike some official is not "binding".

REFERENCES

1.Ahani, Batoul, "conclusion the proof of electronic contracts", PhD thesis on Private Law, Faculty of Law, Tehran University, 2005.

2. The Ministry of Commerce, the Executive By-law “law of the electronic certificate issuance of the certificate of origin", Department of Planning and Economic Affairs, 2006

3. Akbari, Mohsen., "Examining legal barriers in development of the purchase and sale of electronic", plan of The Institute for Trade Studies and Research,2005.

4. Alsan, Mostafa.,"electronic trade documents", PP. 51-70, notaries and secretaries association journal, No. 42.

5. Mason Stephan, "The formation of electronic contracts", pp. 189-174, Journal of Commerce, No. 36, 2005.

6.A Critique of the current status of electronic certificate in Iran", Journal of the Association of notaries and secretaries , Volume II, No. 81- 82, year 50, June and July 2008.

7. the Concept of various aspects in registration and certification of electronic signature", Journal of the Association of notaries and secretaries, Volume II, No. 76, pp. 20-9, 2007.

8. BazyariSarvestani, Gholam,Ali, "Using the rules of notaries in the electronic age", Journal of notaries center, No. 56, 2005.

9. Bajaj and Debjani Nag, "From electronic exchange of information to electronic commerce", pp. 43-3, translated by Iraj. Behnam. Mohammadi, priest, Tehran, Institute for Trade Studies and Research, 13