A Study on the Legal Nature of Electronic Signature in Documents Electronic Registration

Somayeh Tafaghodi Zare

Faculty member ,Payam Noor University of Tehran, Department of Law, Baharestan Branch,Tehran,Iran
Email : sofia_tafaghodizare@yahoo.com

Abstract: In written documents, signature is deemed as an approval sign of the accepted obligations. Since "electronic documents" in the electronic commerce have a position identical to the written documents, signature has basically the same positive value. Contract conclusion is the first substantive issue raised in the electronic commerce. It must be considered that to what extent the general principles governing the contract can be exerted in this type of contract, and to what extent the status of Electronic Commerce Law influences these principles. Yet problem emerges when exceptionally observing specific formalities is the requisite of contract validity; for instance "being written" or "having signature" is regarded as will declaration. Since "data message" is not regarded as a writing and signature, electronic commerce acts have inevitably regarded data message as "signature" and "writing". In terms of consensus formation, general conditions governing the contracts are exerted in the electronic contracts to the extent that they are consistent with the nature of this type of contracts. As regards offer, the particular nature of electronic contracts involves declarations stipulated in websites be considered as an invitation to offer. This paper, relying upon experiences of developed countries and studying rules and regulations, investigates how digital signature may be applied in registering documents electronically and what is the best authority for certifying electronic signature and registering electronic documents. This paper has been based on this idea that violation of the existing rules and procedures regarding documents registration and signature certification will bring about harmful legal, social and economic effects. So, electronic signature and documents do not have a feature that resulted in changing the authority of registration and certification.
[Somayeh Tafaghodi Zare. **A Study on the Legal Nature of Electronic Signature in Documents Electronic Registration.** *Life Sci J* 2013;10(7s):1124-1132]. (ISSN: 1097-8135). http://www.lifesciencesite.com. 179

Keywords: digital signature, electronic registration, comparative law, Electronic Commerce Law.

1. Introduction

Emergence and development of modern communication means whose salient features are "speed" and "diversity" led to the introduction and development of "electronic commerce" only when the most complete method of electronic communication, i.e. "internet", was innovated and introduced. Internet, in fact, offered both speed and diversity and provided cheap transactional relations as well. Although these developments occurred in less than one century, electronic communications – due to the tradition of living good people and bad people together - have always been subjected to disorder, deception, fraud, and sabotage. The emerging technology was no longer faced with the matter of "existence", yet it must "continue" its life and acceptance in the Global Village.

In so doing, safety and trust have been discussed and studied by the experts from the beginning of internet emergence. Different methods of encryption and digital signature were created and developed, and later were evaluated and supported in local laws and international regulations.

Besides safety, electronic commerce development requires another technology that – although raised much later than safety methods - is electronic registration and digital certificate of electronic signatures and documents. The issue of electronic registration and certification was raised after 1996 and has not yet entered into the international procedure; however some countries have ratified rules to develop and regulate this issue.

This paper integrates electronic registration and signature. So, it is based on the position of digital signature and certificate, and it investigates how electronic text and signature process may have legal effects identical to paper / traditional signature and documents. After a brief study on the existing laws and regulations (comparative study), it will consider problems related to digital signature and certificate.

Thus, the paper issues are presented in separate section.

2. Concept of Electronic Signature Validity in Documents Electronic Registration

Although electronic registration is more applied for registering electronic – particularly internet – transactions, it does not mean that it cannot be used for normal transactions. So one can prepare electronic copy of paper documents and register them by observing formalities. Albeit, it is evident that parties do rarely accept these formalities and prefer to refrain from using emerging methods when traditional registration method is available. Due to

the application of electronic registration in internet transactions, it is necessary to elaborate briefly the concept of electronic commerce, digital signature and electronic registration, and to specify signature position in the traditional system of documents registration.

2.1 Concept of Electronic Registration

Electronic registration is rather an emerging concept. So with regard to the fact that no electronic notary public has been established in our country, we must refer to the laws and procedures of the countries being pioneer in this regard to find the concept of this term. Of course, "Certification service provider" has been considered in articles 31 and 32 of Electronic Commerce Law which can be applied to the electronic notary public. By virtue of Article 31, "Certification service providers are entities established for providing certification services for electronic signature. These services consist of issuing, saving, sending, approving, voiding and updating electronic (signature) certificates".

In the United States, The Model Notary Act has allocated Article 3 to the issue of "electronic notary public". This Article – from section 14 to 23 – considers all the concepts pertaining to the electronic registration and elaborates the governing rules and principles. In the Comment section, Article 3 stipulates that electronic notary public is not regarded as an entity independent from Notary Public, and any notary may be converted into an "Electronic Notary" through gaining necessary permissions and trainings. However they are not obliged to such a measure (The Model Notary Act, 2002. P. 75).

In paragraph 2 of section 14 of the Act, electronic notary public has been defined as, "an e-notary that is permitted to undertake the affairs pertaining to the notary public, as per the order of the competent authority. According to section 15, only individuals are qualified to open an electronic notary public that are trained and accepted in the related examination (Op cit, P.80). In most regions of the United States, electronic registration has been commenced for which some regulations have been enacted. For example in Florida, Colorado, and Utah, there are rules ratified for "electronic registration" that permit the notary to undertake digital signature certification (Leff, Laurence LeffLaurence, 2002. p. 3). In Arizona, electronic registration has been commenced from 2002 and a particular Act has been formulated in this regard.

3. Substantive and Formal Rules in Electronic Registration

The claim indicating that the nature of electronic registration is different from traditional registration is doomed to be invalid. Hence, discussing about "nature" is in fact an emphasis on the old concepts in a new format. However, electronic registration and signature certification are different from traditional registration system in terms of storage, processing and registration.

3.1 **Nature of Electronic Registration**

From what was mentioned about formalities of electronic registration, one can find out that electronic registration firstly, is not confined to merely design, registration or certification of the signature (as considered by Article 31 of Electronic Commerce Law regarding Certification service provider and its bylaw). Secondly, establishment and management of electronic notary do not involve a new or tough endeavor compared with existing notary public, and there is no need to a technical expert (non-lawyer) to manage it. Rather, by designing a technical system, the management must be assigned to the organizations competent in the field of registration alike with Notary Public, and any purely technical thought must be avoided in this arena. Thirdly, converting a notary public into an electronic notary public has only one condition and that is the required technical and scientific facilities and capabilities. To achieve this requirement, a Notary Public may employ the related experts. It is obvious that the notary public is not obliged to undertake electronic registration. And in case of undertaking this kind of registration, it cannot be confined to this type of registration and be refrained from doing paper registration.

Thus, electronic registration does not have a nature distinct from paper registration in terms of legal effects; because what has been changed is the means applied in different stages of registration (related evidence, storage, archive, retrieval, access, print, copy, etc.) and this must not be logically deemed as a change in the nature of electronic official document versus paper document. The principle of "equality of nature and legal effects of electronic documents with paper documents" is as below:

1. To actualize the equality principle, the electronic document, if official, must have three main conditions of official document (by virtue of Article 1287 of Civil Law: being regulated by a competent authority, within the limits of its jurisdiction, and based on regulations). Otherwise, document generated or sent by the electronic means may not be considered official. It indicates that merely giving the title of official document – though by the legislator -

will not make it official. So, Article 15[1] of Electronic Commerce Law is contrary to the rules specific to official documents and positive evidences.

2. If a part of document is official or a part of electronic document has been approved by the competent authority, the whole document is not regarded official. As per Article 31 of Electronic Commerce Law, "Certification service providers are entities established for providing certification services for electronic signature. These services consist of issuing, saving, sending, approving, voiding, and updating electronic (signature) certificates". By mentioning "electronic signature certificates", this Article intends to infer that through signature certificate issued by certification service provider, document in which the signature has been inserted must be considered indisputable. However, extending legal effects of electronic signature that is substantially separate from the text or when or it is applied for only a part of the text, to the whole text is not right; unless Notary Public approves validity of electronic signature and its inclusion to the whole text.
3. Development and progress of technology over time involves another requirement to maintain the official "nature" of electronic documents that possess all legal conditions which is "consistency of the technology of document and the inserted electronic signature with updated advanced circumstances". Legislator may determine a specific respite to stabilize this requirement after which the Notary Public is obliged to improve software and hardware equipments applied for different stages of electronic registration.

3.2 Validity and Principles governing Electronic Documents

By registering documents electronically, necessity of the features appointed for paper normal or official documents in formal or substantive rules is not removed. As an electronic official document possesses all protections and guarantees provided for other document, formalities and criteria must be observed in a way that no doubt remains in documents security. Various laws have eliminated the matter whether electronic documents are valid or not. For example, in the United States and Utah, Electronic Signature in Global and National Commerce Act, 2000 (p. 24) that has practically been converted into a standard law in the global level, has regarded an identical validity for electronic documents compared with paper documents. This trend was completed by two UNCITRAL model laws enacted in 1996 and 2001.

Article 62 (a) of Malaysian Digital Signature Bill ratified in 1997 has implicitly confirmed the validity of data message applied for creating electronic document. By virtue of this paragraph, "Notwithstanding any written law to the contrary, a document signed with a digital signature in accordance with this Act shall be as legally binding as a document signed with a handwritten signature, an affixed thumb-print or any other mark..." (Malaysian DIGITAL SIGNATURE BILL 1997, p. 77)

In Iran Law, as per Article 6 of Electronic Commerce Law whenever existence of a written document is necessary according to law, except in exceptional cases, "data message" is regarded as a written document. And as per Article 8, "whenever law requires that information be offered or maintained originally, this is feasible in the form of data message as well". And as per latter part of Article 9, "substitution of paper documents for "data message" will not have an effect on the previous rights and obligations of both parties". And ultimately, Article 12 has been formulated in a way that removes any doubt regarding validity of electronic documents: "positive evidences and documents may be in the form of data message, and no forum or governmental office may reject positive value of "data message" merely due to its form".

However it must be underscored that no electronic document, record or signature is regarded official before meeting legal formalities of registration. In so doing, one can refer to judicial verdicts which contain general rules for "official" documents; though this matter has not been considered directly as electronic documents have not been prevalent.

As per a verdict issued by one of the courts, "forging a normal check is not regarded as forging an official check". (Notwithstanding any written law to the contrary, 2007, p. 217) Also Registration Council provides that, "... first; Article 1 of 22.6.27 law {Reform Law of some Articles of Registration Law and Law on Notary Public} states, "whoever considers implementation of official documents as being contrary to the document provision or law, can

[1] Article 15: "as regards reliable "data message", reliable electronic records and reliable electronic signature, no doubt or denial is heard and it is just possible to claim the "data message" forgery and/or prove that "data message" has become invalid due to a legal reason."

raise an action based on Civil Procedure". This Article is applied when an obvious official document exists or at least there is not an evident knowledge that document is not official. If an evident knowledge exists that document is not official, this Article is not applicable. With regard to Articles 1287-1294 of Civil Law providing Deed of Attorney is not official; Article 1 of 22.6.27 Law is not apparently applicable. Second; by the same reasoning, Article 99 of the Registration Law is not applicable as well and if a writ of enforcement has been issued by virtue of a normal document it must be abandoned... (Bazgir, 2009, p. 145)

In Registration Law Reforms, an authority must be explicitly given so as to void documents that are evidently (without judicial comment) informal". (Jafari Langrudi, 2003, pp. 258-259)

Multiple verdicts indicate that non-certified copy of official documents is not considered official and their forgery is not deemed as distortion in official documents. For instance, a verdict has provided that, "with respect to Article 20 of Discretionary Punishments Law and its legal definition, forgery of official documents copy and normal documents and using that is not considered criminal; yet if copy of documents whether normal or official has been certified, its forgery is deemed as a crime". Precedent Verdict No. 1342.9.27-6339 states that forgery of the copy of documents is not regarded as an example of forgery of legal documents (Model Notary Act 2002, p. 77). So recognizing the legal effects of official documents for any electronic document, record or signature or their copy by Legislator of Electronic Commerce Law – without necessity of "data message" certification by the competent authorities – is surprising and stems from negligence about the nature and formalities required for an official document.

4. Comparison of Internal Regulations with Electronic Registration Law

Compliance of electronic registration with existing principles and rules for registration in general, involves considering its comparison with some articles of registration laws that may be challenging. Here articles will be mentioned and compared with modern registration system.

4.1 Jurisdiction of Electronic Notary Public

As per Article 2 of Registration of Documents and Properties Law, ratified in 1931, "Managers and representatives of registration and owners of Notary Public may not act except in their jurisdiction outside which their measures do not have a legal effect". The latter part is regarded as a heavy executive guarantee for violation and document registration outside the jurisdiction. More importantly, this guarantee embraces Notary Public as well as document owner, and it seems that legislator has preferred protection of general rights to any other priority including ignorance of the client and thus his goodwill. An issue raised regarding electronic registration is whether general principle of Article (2) is enforced in this method of registration or whether legislator must confine that by considering modern global advancements.

It is evident that cases in which presence of registration applicant in Notary Public is necessary, is off-topic. Yet there are affairs in an electronic notary public that do not require presence of the applicant, and there will be no justification for enforcing limitation provided by Article 2. Particularly when owner of electronic document needs to receive information from Notary Public while he is outside that area and it is possible to provide the information electronically, Article 2 may not be enforced. The Article indicates that in all affairs that during or after document issuance, the Notary Public or registration authority must be accountable for the related matters geographical constraints may not be exerted in the electronic registration system. This exception to the traditional general principle that itself is regarded as a principle in electronic registration is confined to such conditions as "necessity of registration ", "lack of necessity of applicant physical presence by virtue of law", and "possibility of doing it electronically". In case of predicting particular law for electronic registration, this matter must be taken into account.

Giving an unlimited jurisdiction to the Notary Public has two important legal effects in terms of electronic registration: first, the matter of documents electronic registration is automatically eliminated in the international level, and by presence of applicants in any Notary Public, it is bound to register and albeit it is accountable for technical needs of applicant after registration. As per Article 83 of Registration of Documents and Properties Law, "jurisdiction of Notary Public is specified by virtue of the constitutions of the Ministry of Justice".

Second, Notary Public that undertakes electronic registration may present a certified copy of documents whose presentation are not prohibited, electronically, to the transaction parties even beyond its jurisdiction. It does not seem that law is in conflict with these kinds of services that merely result in speed and decrease costs and formalities.

Article 12 of the UNCITRAL Model Law on Electronic Signatures underscores this matter in the form of "recognizing electronic certificates and signatures". As per paragraph 2 of this Article, a certificate issued in abroad, if meets the requirements for citation, has a legal effect identical to the

domestic certificates. To recognize validity, paragraph 4 underlines considering international standards so as to prevent probable misuses and discriminations by the governments (UNCITRAL Model Law on Electronic Signatures with guide to enactment 2001. p. 71, n. 158).

Attention to the electronic documents issued in abroad, in judicial forums, and bureaus such as Registration Enforcement when document is considered official is among new issues that must be supported; because as per Article 969 of Civil Law that has been completed explicitly by Article 1295 of the same law, "documents, in terms of regulation, comply with the law of the regulation place" (Glad man, Brian, Ellison, 1999, p. 10).

5. A Comparative Study on the Electronic Signature Position

This study is necessary as it indicates acceptance of electronic signature in most countries and tendency towards development, security and reliability. For brevity, international documents and rules, United States, Canada, France, and Iran laws are studied respectively and the laws of other countries are not discussed.

5.1 International Documents and Rules

In the international level, electronic signature issue was firstly addressed in Article 7 of the UNCITRAL Model Law on Electronic Commerce in 1996. In this Article, a valid electronic signature has positive values and effects identical to the traditional signature. According to the report of UNCITRAL Electronic Commerce Workgroup, document authenticity and its assignment to the signatory are proved by electronic signature and the signatory will be committed to the document content. The importance of signature in the electronic commerce made UNCITRAL (op.cit, p. 19) to enact a separate Model Law on Electronic Signatures with 12 Articles in 2001.

As per Article 3 of the Model Law (2001), there is no distinction among various technologies of creating signature if they meet security requirements, and all of them are valid and have identical legal effects. Recognition of "identical function" principle in this article is important because it remains no doubt that there is no discrimination between written and electronic signatures. In Article 6, conditions for validity of electronic signature have been mentioned, and Articles 8 and 9 provide obligation for the signatory and certification service provider (Greenwood, Daniel, J., 2008, p. 45). Article 12 states an interesting point and that is "recognition of electronic signatures and certificates issued in abroad" (Op. cit, p. 61). As per this Article, geographical location of signature place or the signatory business center must not be considered when determining the legal effects of electronic signature or certificate, and any signature is substantially valid in case of meeting the requirements.

In the UN Report on the electronic commerce and development (Katuzian, 2001, p. 170), enactment of proper rules has been regarded as a requisite for electronic transactions validity. Acceptance of electronic signature will have two important advantages namely merchants inclination towards electronic commerce and increase in the confidence as a pre-requisite for concluding electronic transactions (the same, p. 171). These advantages made UNCITRAL to enact the Model Law on Electronic Signature.

In the European Union, Electronic Signatures Guideline (Leff, Laurence Leff Laurence, 2002, p. 76) and Electronic Commerce Guideline must be considered as the legal foundation of electronic signatures validity. These rules are imperative and the European Union member states are bound to join it. Article 2 of Electronic Signatures Guideline mentions four conditions namely certain assignment to the signatory, possibility of recognizing signatory identity based on his signature, signatory control, and consistency of signatory and text (data message), and recognizes "advanced electronic signature". In Electronic Commerce Guideline, Article 19 does not fully elaborate words "written" and "signature". By virtue of this article, "member states must guarantee that electronic contract conclusion is permissible in their legal system. They must guarantee that the rules governing contracts permit using electronic contracts and do not lead to the lack of legal effect of these contracts due to their formation by electronic means (Op cit, p. 81).

It is inferred from Article 9 that member states may not make using paper and pencil mandatory for contracts formation. Albeit as mentioned earlier, there are some exceptions. Article 9 is not right as it does not prohibit member states from imposing special technical requirements as formal conditions (Katuzian, 2001, p. 213). So it is not unlikely that some member states accept just specific kinds of electronic signatures; while other countries, following UETA and UNCITRAL Model Law, will have a broad perspective in this regard (the same, p. 221). Adopting various measures in the European countries will be probable and thus it will impede consistency among these countries laws as the ultimate objective.

5.2 The United States Law

Recently in the United States, electronic signature is binding similar to the traditional signature. However, the law has not referred to how it is realized or has not investigated the minimum precautions for validity and security of signature process. (Thaw, Deborah M. 2000, p. 411) From historical viewpoint, the first law on digital signature was ratified in Utah in 1996 (The Model Notary Act, September 1, 2002, p. 93). In federal level, Electronic Signatures Law in Local and International Trade was ratified in 30 June 2000 and was enforced from 1 October 2000 (Idem). This strategic law validates electronic signature. This law has moderated rules and judicial procedures of 50 states in the USA from acceptance of written signature as an imperative principle to the acceptance of electronic signature and its recognition in all actions and forums.

Article 101 (a) (1) provides that signature, contract, or any other document related to electronic transactions may not be considered invalid by virtue of any law, legal procedure or principle merely for the sake of its electronic form. The Uniform Electronic Transactions Act (UETA) enacted in 1999 provides that if signing a contract is mandatory based on law, it can be realized by electronic means equipped with technology of signature creation; providing that signing intent is confirmed. Albeit UETA has excluded will and trust agreements by virtue of Article 3 (b) (1). As regards validity of electronic signatures created outside the United States, E-Sign gives a positive answer to this matter in Article 101 (h).

In terms of nature, by raising the issue of "signing intent" as a requisite for its validity, UETA has taken a great stride compared with Electronic Commerce Guideline, Electronic Signatures Guideline, and UNCITRAL Model Laws. It is due to the broad interpretation of Uniform Commercial Act (report of National Notary Association, an overview of the rules related to digital signature and deeds registration, 2004, p. 193) about signature concept; which embraces typing and marking method that may not be reliable like written signatures (Mansour, 2003, p. 297). Another important point in UETA is that it has permitted companies and institutes to require certification or registration of electronic signatures when circumstances involve so. Bestowing this authority, particularly in terms of decreasing commercial risks, has a remarkable importance.

5.3 Iran Law

In Iran Law, rules of Registration of Documents and Properties Law, Civil Law, and Civil Procedure Law can be applied in inferring provisions related to the "digital signature". However it must be investigated whether these signatures have essentially been accepted by the Iranian legislator or not. An important law from which several principle regarding electronic signature and documents may be inferred is Electronic Commerce Law.

This law – particularly in the section pertaining to electronic signature – has been ratified by imitating two UNCITRAL Model Laws (1996 and 2001). Electronic signature and "reliable electronic signature" have been defined in paragraph (z) and paragraph (v) of Article 2, respectively. As digital signature – like written signature – confirms existence of a document without which it does not have a legal effect, and since digital signature may only be found in electronic – not paper – documents, it is necessary to address the concept of "electronic documents".

Electronic Commerce Law does not offer a definition for "electronic document". It provides in paragraph (a) of Article 2, "data message is any symbol of event, information or concept that is generated, sent, saved or processed by electronic means or a new information technology". It must be added that this law continuously talks about security and safety of computer and informational systems. This emphasis is per se important; because without security, data message and electronic signature will be invalid from all prospects. So, acceptance of electronic documents and consequently digital signature requires the existence of "confidence and security". Thus Electronic Commerce Law defines "Secure Information Systems" and "Safety procedures"; though it was better to consider these important concepts in a substantive manner, rather than offering definitions merely.

"Reliable electronic record and signature" mentioned in Articles 10 and 11 of Electronic Commerce Law require all above-mentioned conditions. As regards electronic signature requirements, it provides that

a. It is specific to the signatory.
b. It determines the identity of data message signatory.
c. It has been issued by signatory or under his exclusive intention.
d. It is connected to a data message in a way that any change in data message is identifiable.

As we will see in the next section, in stating "acceptance of positive value and effects pertaining to a reliable electronic record and signature, Electronic Commerce Law in Articles 12-16 goes far beyond what must be really, and was caught in the same mistake that, according to the United States National Notary Association, are seen frequently in

the laws of digital signature in most states (Katuzian, 2001, p. 317).

6. Legal and Practical Problems resulted from Emergence of Digital Signature System

Most countries of the world have incorporated the concept of digital signature into their internal laws and have ratified special laws in this regard. It must be noted that unfortunately the most essential legal and practical problem of using digital signature for approving electronic documents related to the different types of transactions stems from these rules and regulations. The legislators has forgotten this important principle that issuance of any kind of "certificate" and "confirmation" of a signature requires consultation with entities specialized in document registration and signature certification.

Intractable legislation and attention to scientific and technical aspects of electronic commerce without considering formal and substantive rules of positive evidences are faced with this matter that predicting all scientific criteria and immunizing computer and informational systems will not warrant inviolability of electronic signature and documents: every day a novel technology emerges in the electronic knowledge which may be gained by hackers, professional thieves, and internet hustlers and set the stage of "distrust" that is the main obstacle in the way of electronic commerce development.

Another important problem of non-specialized legislation – at least in the field of electronic record and signature – is that it is not clear who is responsible for presenting the proof regarding various problems resulted from generating, sending, receiving, disclosing, using, and misusing electronic signature and record. In this respect, Electronic Commerce Law is the best existing law in the countries. Impossibility of denial and doubt regarding reliable data message and reliable electronic records in Article 15 and providing a unique solution of "forgery claim" or "legal invalidity", comparing these documents with official documents and replication of Article 1292 content of Civil Law – specific to official documents – is regarded as the violation of all principles and rules regarding official documents; as no official authority has undertaken the responsibility of providing, inspecting and controlling this kind of services.

Article 31 of Electronic Commerce Law on certification service provider may not be a ground for justification of this big mistake; because, first: the Article indicate that these service providers have only been established to provide services of electronic signature issuance, and second: not using services of these providers, due to the lack of law emphasis and that the above mentioned Article has been written after Articles 12-16 of Electronic Commerce Law in a separate section, will not impede acceptance of electronic signature and documents as broad as the latter Articles provide.

So, an unexpected crisis, i.e. negative effects resulted from perception of lack of necessity of referring to the Notary Public or any other competent authority for certifying electronic documents - as it was considered by the U.S. National Notary Association – is occurring in our country as well, that must be resolved as soon as possible. In the following, problems and challenges caused by electronic signature emergence will be explained and some solutions will be presented.

6.1 Scientific and Technical Problems

Digital signature as one of the modern electronic achievements pursues particular scientific principles. Although this aspect of digital signature has been taken into account in the scientific works, its legal effects have not yet analyzed accurately. Importance of such problems is so that other aspects may be examined based on them.

Digital signatures are secured by an encryption known as "public key encryption". Public key encryption is based on an algorithm that is created by two different codes known as "key" and these keys are used for encryption and decryption of data message. Encryption key is called "private key", and the key owner as the signatory is bound to maintain and not disclose it. But since all people must be assured about the accuracy of the signature, public key is availed for all. Any digital signature created is unique to its owner, and using different algorithms for encryption of different signatures will distinct the signatures from each other (Valera, Milton, 2000, p. 211).

7. Legal Problems of Digital Signature

Counting these problems due to their multiplicity is very difficult. Lack of registration authority for digital signature causes legal problems as following.

7.1 Anonymity

Due to the fact that in internal laws (on electronic signature) the presence of signatory in the Notary Public has not been provided, there is no need to the formalities provided in the registration Law for recognizing signatory identity and this increases the probability of signing by people that do not exist (imaginary individuals). The result is clear: signatory may create rights and obligation for himself in contract with others, while the obligations are escapable due to the lack of natural personality. Although this status is changing in the United States

by ratifying Model Law of Public Notary, Electronic Commerce Law has not foreseen involvement of Public Notary and this is an essential problem.

To compare internal laws and the United States law, it must be noted that by virtue of Article 86 of the Registration Law, "if someone requests registration of a document, the Notary Public must be assured about the identity of the parties or the committed party, and if he does not know them personally he must treat according to this article; otherwise he will be liable to Article 102 of this Law. Article 102 refers to Article 101 in which administrative penalty from one to three year dismissal has been determined for the violator. Also, as per Article 50 of Registration Law, "whenever Notary Public doubts about the identity of the parties or the committed party, two popular and trusted persons must confirm their identity personally and Notary Public must register it and stipulate it in his documents and witnesses must sign it.

Article 10 of Electronic Commerce Law do not clarify that what authority must meet these requirements: although signature may per se be unique to its signatory and may be created by signatory or under his exclusive will (paragraph a and f of Article 10), there is no guarantee that the identity that digital signature shows is the real identity of signatory, and its recognition must be assigned to a competent authority.

In the United States law, lack of emphasis in UETA regarding the role of Notary Public in electronic registration and thus ratification of particular laws in the United States by virtue of which there is no need to the presence of signatory in the Notary Public, were highly criticized by lawyers and registers (Ares, C. Paz, 2001, p. 319). So the US National Notary Association regarded it as a kind of informal robbery to its jurisdiction (and Samuelson K, Bea.tty N. 2000, 225). Multiple seminars and meetings were held on explaining the matter prospects and finding a solution (Op cit, p. 229). The opponents believe that E-Sign as the Federal Law and the internal law of some states, permits individuals – explicitly or implicitly – to obtain digital certificates from a competent authority and apply it to create digital signatures without any constraints which provides the stage of misuse through applying the identity of others (identity robbery) and anonymity.

8. Conclusions

Attention to the foundations is the first requisite of entering into the world of electronic commerce and progress in this arena. Electronic Commerce Law – in spite of some defects – must be regarded as a starting point for this trend. The experiences of other countries demonstrate that if the electronic commerce is actualized, the issues of security on the one hand and proving the claims on the other hand will be raised. In the first part, creation and registration of digital signature and in the second part electronic registration of electronic documents will solve many problems in this arena. As regards electronic registration of signature and documents, the important point is "trust" to the Notary Public and endeavor to achieve the updated standards of development. The latter point is so important that without which a principled efficient electronic registration is not feasible. Any measure in assigning registration to a new organization or individuals not specialized in the registration affairs will be doomed to failure due to their unfamiliarity with registration principles. Registration of electronic signature and documents comply with the same principles and rules as paper documents and signatures do. Contrary to some opinions, technology developments may not be a justification for violating existing principles and rules. First, "electronic registration" must be recognized through ratifying a proper law, and a number of Notary Public must be devoted to this affair after being trained. Possibility of registration by both electronic and paper methods is the best evidence for not violating the existing principles and rules. While an electronic notary public may register digital signature and prepare an electronic record of the registered document, it will be able to undertake routine affairs including registration of properties. The claim that creation of electronic registration centers separately will lead to more formalities and sophistication in electronic transaction is doomed to be invalid. It is not rational to cause main problems including forgery and misuse in virtual space so as to reach speed and low costs in transactions. By legislating accurate rules, it is feasible to issue and register electronic signature in a single notary public within the least possible time. Creating balance between electronic commerce development philosophy and its security is the best choice which is achievable by electronic registration of signature and documents.

References

1. A Bill initiated An Act to make provision for, and to regulate the use of, digital signatures and to provide for matters connected therewith Malaysian DIGITAL SIGNATURE BILL ,1997
2. Ares, C.Paz, la formation electronique de contrat, Paris, Bsch, 2001
3. Beatty N. and K. Samuelson, Business law for a new century, London, 2nd, 2000
4. Electronic Commerce Law, ratified in 2003, official newspaper 2003, 59th year, No. 17167.

5. Electronic Signature in Global and National Commerce Act [E-sign]. Effective October. 1, 2000.
6. Fransworth, Sec. 6.1; Restatement (Second) of contracts Sec, 1998
7. Gladman, Brian, Ellison, Carl and Bohm, Nicholas. Digital Signatures, Certificates & Electronic Commerce, Version 1.1, revised 8th June 1999, Digital Signatures
8. Greenwood, Daniel J. Massachusetts Institute of Technology ,Electronic Notarization, Published by the National Notary Association .2007
9. Jafari Langrudi, Mohammad Jafar, Registration Council verdicts, Sherkat-e Sahami Publication, 2003.
10. Katuzian, Naser, Contracts General Rules, Tehran, Sherkat-e Sahami Publication, fifth edition, 2001.
11. Katuzian, Naser, Proof and Evidence, first volume, first edition, Mizan Publication, Tehran, 2001.
12. Leff, Laurence LeffLaurence, Notaries and Electronic Notarization, Western Illinois University 2002
13. Mansour, Jahangir, Notary Public Law and Notary Association, ratified in 1975, first edition, Didar Publication, Tehran, 2003.
14. Mansour, Jahangir, Registration of Documents and Properties Law, ratified in 1931, with subsequent amendments and extensions, first edition, Didar Publication, 2003.
15. Miguel. P.A., Internet, Madrid, Obas, 2000
16. Notwithstanding any written law to the contrary, A document signed with a digital signature in accordance with this Act shall be as legally binding as a document signed with a handwritten signature, an affixed thumb-print or any other mark",2008
17. Report of National Notary Association, an overview on the laws pertaining to digital signature and documents registration, translated by Mostafa Alsan, Jouranl of Notary Association, 47th year, No. 51, 2004.
18. Report of task force on state law exclusions (Sep.21.1998 at www.webcom.com/legaled/ ETAF forum/does/report4
19. Robertson, R. J., Electronic commerce on the internet, London, sweet & Maxwell, 1998
20. Swink Co. V. Carrol, 584 S. W. 2nd 393, 1979; Cljburn V. Allstate Ins. Co., 826 F. Supp. 955, 1993
21. Thaw, Deborah M. the Notary Public and its Impact in 21st Century, A Presentation at the NACO/NACRC Annual Conference, 2000
22. The Model Notary Act, Published As A Public Service by the National Notary Association. September 1, 2002.
23. UNCITRAL Model Law on Electronic Signatures ,with guide to enactment 2001
24. Uniform Electronic Transactions Act [UETA], Approved By National Conference Of Commissioners On Uniform State Laws (NCCUSL) On July 23, 1999.
25. Valera, Milton, G. In Notarization, There is no Substitute for Personal Appearance–Despite Technology, A Presentation to the Property, 2008.
26. Weber, E., commerce law, Madrid, Obas, 2001
27. Widne U. and K. Bhler, electronic commerce monich, 1997
28. Yadollah Bazgir, Problems of check in the courts final awards. Asr-e Hoquq Publication, first edition, 2009, p. 145.
29. http://fwebgate.access.gpo.gov/cgibin/getdoc.cgi ?dbname=106-Cong-bills&docid=f:s761enr.txt.p df
30. www.law.upenn.edu/bll/ulc/ulc.htm
31. www.uncitral.org/pdf/English/texts/electcom/ml-elecsig-e.pdf.
32. www.nationalnotary.org/serImages/Model_Notar y_Act.pdf,p,93

6/10/2013