J. Appl. Environ. Biol. Sci., 5(4)150-155, 2015
© 2015, TextRoad Publication

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

E-signature and its legal place

Reza Nikkhah[1], Ali Ariana[2]

[1]Department of Jurisprudence and Law, Faculty of Literature, Urmia University, Urmia, Iran.
P.O. Box: 57153-1177
[2]Department of Jurisprudence and Law, Faculty of Literature, Urmia University, Urmia, Iran.

Received: November 23, 2014
Accepted: February 9, 2015

ABSTRACT

Development of commercial transactions and necessity for facilitation of commercial transactions has made use of electronic instruments unavoidable. Virtual identity is the first condition of an electronic buyer or seller. This is especially true when the business is developed. Management of e-documents and sending and receiving electronic information composes a large portion of executive activities and advertisement in today's world. One of the technologies which increases trust in transactions is digital signature. This technology is based upon decryption and adds formality to electronic information. It makes it possible to control and revise the identity of the creator of a document. Consequently, it seems necessary to investigate the legal place and competency of electronic signature in the law. The present research tries to deal with the technical aspect of digital signature and review it.

KEYWORDS: electronic commerce, electronic signature, digital signature, decryption, certification authorities, global commerce

INTRODUCTION

Electronic commerce refers to conclusion of a contract for product, service, money and commercial documents transfer via advanced electronic instruments. This phenomenon is very important due to its role in global markets. Absence of use of electronic commerce means losing many opportunities in global commerce and endangering competitive situation and isolation from international commerce. This directs countries towards e-commerce. Growth in commerce has been accompanied with legal issues. Different countries and international and regional organizations try to impose and predict laws and regulations on electronic commerce issues. Iranian legal system can also use the experiences and models of international institutes and other countries. Development of electronic commerce involves creation of public trust with respect to this kind of commerce. This kind of trust is created via security guarantee and electronic data transfer reliability. One of the factors which bring reliability for a contract or any other kind of document is the accuracy of attribution of the document to its issuer. This is done via stamp or signature and it I is a valid reason for implementation of accuracy of issuer attribution. In electronic contracts, in addition, documents and information must be signed by the issuer person so that their validities can be identified. Therefore, it is necessary to define an electronic signature for validating electronic contracts documents and replace hand signatures by electronic signature. It seems necessary to specify exactly the features of an electronic signature. Furthermore, limits of the validity of methods and software of electronic software must be determined. Since signing a document is a legal action, electronic signature technology must be legally investigated as a legal issue in electronic commerce.

The present research tries to investigate technical and legal aspects of electronic signature in addition to defining e-signature.

THEORETICAL LITERATURE

Definition of signature and its legal place

A signature is writing the name or family name (or both of them) or drawing a special sign which indicates the identity of the owner of the sign in the end of formal or ordinary documents which are signed in a contract or transaction or as testifying or below documents on which transactions or commitments will be written (without signature) (Mohammad Jafar Jafari Langroudi, 1991, p 18). The important impact of a signature is becoming committed to all aspects of a document or contract which has been signed. In general, writing can be attributed to a person as long as it has been signed by that person. Signature indicates verification of items of a contract or document and acceptance of its commitments. Before signing, a document has not been finalized and it is going to be decided (Naser Katouziyan, 2001, p 278). Therefore, any document which is signed by a person is valid and the commitments are accepted and must be fulfilled by the person.

***Corresponding Author:** Ali Arian, Department of Jurisprudence and Law, Faculty of Literature, Urmia University, Urmia, Iran. Email: Aliariana1344@gmail

Differences between a written and a digital signature

Although the word "sign" is used for both of them, digital and written signatures are naturally different. If a digitally-signed document is manipulated, the digital signature is not verified; however, a written signature cannot prevent from manipulation of the document. A written signature is certification of a person which is expressed on a document but a digital signature is a certificationwhich is expressed on a document by a private key. Furthermore, a digital signatureindicates that the document has not been changed since signature date (Brian Gladman, 1999).

Written signature and its features

A signer specifies his or her identity, verifies the terms of the document and states that he or she is committed to the contents of the document by putting a signature below a document. Some important features of written signatures are as follows:

A person's signature is the same for all documents; it is generated easilly; it can be differentiated easily; it must be in a way that it cannot be forged; it is produced physically. In general, a written signature is unique and it can be re-generated only by the person who has signed a document. When a document is signed, the document's contents must not be changed without the signer's notice. Consequently, a written signature is considered as the lock of paper document contents and specifies that the signer knows about the contents and agrees to the contents of the paper document.

digital signature and its features

A digital signature is an electronic username for digital world and facilitates secret and sensitive informationsecure transfer. A digital signature guarantees the originality of a file or message or document and is an electrical validation instrument. Determination technique is used for proving the identity of a user. When a user's identity is identified, the user accesses to his or her digital identity. A digital certification is a collection of validations used in a signature process which is issued by internal or external certification issuance centers after thorough verification personal identity. Special software is used for implementation of a signature process. These software combine unique information of the signed file and digital certification in order to put a digital signature inside a file. This signature can be investigated and verified by special software which are usually free of charge.

Common wrong beliefs about digital signature

Many people have different wrong beliefs about digital signature concept. One of the commonest beliefs about digital signature is that it is a graphical drawing of a written signature which is considered as the image of the signature on the document. This belief views a personal digital signature the same as a written signature because a graphical drawing of a signature can be regenerated by any other person. This is possible by simply scanning the signature and putting it on the document. Furthermore, the contents can be changed easily and the signature can be added afterwards. Consequently, a graphical drawing does not guarantee that the signer agrees to the contents of the signed document. Furthermore, a written scanned signature or entering a person's name in an email account should not be accepted as a substitute for a written signature because they will not have all applications of a written signature.

Differences between a digital and electronic signature

The terms "electronic signature" and "digital signature" have been used widely over the past few years and these two are used mistakenly. An electronic signature is usually used for attributing a signature to a text via one or several electronic instruments or decryption instruments for agreeing to a document. In fact, an electronic signature is any symbol or sign which indicates the satisfaction and intention of a person in an electronic form. It may come in the following forms: writing a name, clicking on a verification button, inserting a username or password, biometric signature and digital signature (Lorna Brazil, 2004, pp: 38-39).

Definition of a digital signature

USA center of lawyers first started working on legal aspects of signatures in electronic contracts in 1992 and prepared the draft of a guideline for using signatures in electronic contracts and its infrastructures. The first law on digital signature was approved at that year. It dealt with adding certainty and validity to electronic contracts and technologies which were related to decryption and identification and certification authorities of electronic signature. In 1996, Uncitral prepared a law on electronic commerce which included regulations on electronic signature. In 1997, international chamber of commerce issued a "public guideline for secure digital international commerce". EU (1999) approved "electronic signature guideline". In the end, Uncitral committee approved " sample law ofUncitral on electronic signature" and it was used as a standard reference for national law-making on digital signature in many countries.

Many countries passed laws on digital signature using international regulations on electronic signature during 1996-2001. We can dare say that electronic signature is currently used in all legal systems (Lorna Brazil, 2004, p4). In Law, no document is valid unless it has a particular sign indicating the issuance of the document by a person. A signature below a document has the following purposes: adding formality to the document, verification and adding certainty to a document. However, it must be noted that a signature indicates necessarily the intention of the signer for conclusion of a contract. In other words, if a document is not signed, the individual did not want to conclude the contract and the contract is null and void. Commerce on internet must have a legal framework in order to eliminate legal issues so that all individuals can use this kind of commerce and their rights are reserved. Therefore, it can be said that absence of legal infrastructure is a main barrier ahead of development of e-commerce.

Standard digital signatures

The following sentences introduce three standard methods for adding a digital signature for short:

a. RSA-based digital signature: this signature method is based upon RSA public key code and was accepted by ANSI as a standard (Chalamaih, Avadhani, 2006, p 224).

b. DSS digital signature standard: DSS method is based onAljamal public key encryption system. DSS was proposed in 1991 by national American standard and technology institute and was accepted in 1993 as a standard for processing information in American Federal Government. DSS was the first digital signature method which was recognized as formal. In order to reduce the size of signatures, this method uses small subgroups in Zp.

c. Digital signature based on elliptical curves

Elliptical curves digital signature algorithm is similar to DSS. This means that we work on Zp instead of working on a subgroup with rank q (Tuan-Yuan Shen, Hung-Zih Liao, 2006, p 109).

Another point is that digital signatures based on elliptical curves have been developed by three institutes: ANSI, IEEE and ISO. Validation algorithms for generation of digital signature are based on encrypting data by private key and decrypting by general key (R.L. Rivest, 1992, 175). This process is exactly the reverse of the process of maintaining data confidential. Consequently, public key encryption systems are proposed usully for signature generation (J. Silverman, D. Lieman, J. Hoffstein, 1999, 149). The main advantage of public key encryption is that it not only provides data comprehensiveness but also it is used for determination of validation (R.L. Rivest and A. Shamir and L.M Adleman, 1978, 109-113). Determination of validity by means of digital signature provides non-denial feature. In other words, it prevents from sender's denial of sending information. These features are essential for encryption and are necessary for any algorithm of encryption. Encryption process is based on short polynomials which are similar to NTRU (Joseph H. Silverman Jill Piphher and Jeffry Hoffstein, 1996, 48) and (J.Hoffstein, J. Pipher, J Silverman, 1998. 267-288).

This has contributed to the solution of large prime numbers generation problems which are necessary in some algorithms (Avadhani. P. S. 2006, 71).

Generation of a digital signature: first, data which must be signed are specified. The information may be a digital object like a text, shape or any other kind of digital data.

A digital signature for a message is built in the following two stages:

1. generation of message abstract: a message abstract is the abstract of a message which must be transferred. In other words, it is a unique number for any message and any small change in the message results in generation of a different abstract. Message abstract is built by means of a series of mixing algorithms. In fact, creation of a mixed amount of information is usually called message abstract.If even one single bit of data is changed, its concerning mixed value undergoes widespread changes.

2. encryption: message abstract is encrypted by means of private key. In fact, the encrypted message abstractof a digital signature which has been generated as above is added to the message and is sent to the receiver. After the receiver received the message, he/she/it acts as follows: 1. The digital signature attached to the document is decrypted by means of the public key of the signer. 2. The message abstract algorithm which has been used in sender's side is also used in receiver's side. 3. The two obtained message abstracts are compared and the message is validated if the two abstracts are equivalent. If the result was the same, the signature is accepted. Otherwise, it is rejected. By this method, we can make sure that the digital signature has been sent by the main sender because only sender's public key can open the digital signature. If the faulty message abstract is returned when decrypting using public key, this means that this is not the main message.Encryption methods aim to make sure of integration of data and validity and originality of the signer besides its application to make sure of data confidentiality. In practice, message abstracts are signed instead of total message in order to increase speed. The abstract validity is the same as that of total text. The total process has been explained in the following figure:

Certification issuance authorities

Signature verification procedure assumes that the public key actually belongs to the signer. However, this may not be true because an individual may build a pair of keys and put the public key below another individual's name in the public directory and therefore sign the electronic messages by other names. Moreover, no pair of keys (private and public) has natural dependence on a specific identity but the pair is only a couple of digits. Therefore, it must be ascertained that the public key belongs actually to the identity of the signer.

Identification issue is dissolved by third part companies. A third party institute guarantees the presence of relationship between identity and public key. This relationship is resulted in electronic verification which relates a public key to an individual. Third part institutes are recognized as certification issuance authorieties and must be accepted by all users as reliable third parties. Key verification procedure must be void of any kind of error and must have the highest security level. After dissemination of a digital verification, a verifier authority verifies the identity of the user and guarantees that the public key belongs to the mentioned user.

Digital signature verification

Digital verifications include: owner's public key, owner's name, verification expiry date, the name of the formal verifying institute which has issued the verification, a serial number and other information.

A verification is made up of four parts: 1. Subject and its features: this section refers to the subject which is going to be verified. For instance, this information may include: name, nationality and address, related organization and its department in that organization. Furthermore, it can embrace a picture of the person, a coded fingerprint and passport number.

2. public key information: this is information about the verified public key. This attaches the public key to the items of the document.

3. signature verifying authority: the verifying formal institute (CA) signs the above two items in any document and attaches it to the verification. Individuals who receive the verification control the signature and if the trust in the CA, they will accept the accuracy of information to which the public key is attached.

4. verification expiry date: any verification has an expiry date. After verification date expired, its contents are not guaranteed by the CA.

Legal references of electronic commerce

IT infrastructure makes it possible to conduct mant commercial transactions on internet. Development of e-commerce has been accompanied by emergence of new legal issues. Recognition of new communicational technologiesin conclusion of contracts, formation and validity of contracts, attribution capability of electronic documents and issues concerning e-signature and trend of e-payments are important issues in this area.

It seems necessary to deal with legal aspects of e-commerce. Many countries have imposed regulations and reformed previous laws to adapt to new conditions. Organizations like Uncitral, EU, organization of economic development and cooperation and international commerce chamber are organizations which are active in this area and have proposed guidelines for preparation of a legal framework for ecommerce. Uncitral ecommerce committee prepared a sample law for ecommerce in 1996 and in 2001, it approved a law on electronic signature. EU has imposed many guidelines for electronic signature and has investigated legal issues like conclusion of electronic contracts and consumers' rights.

Legal acceptance of electronic evidence

Ecommerce is paperless and based on electronic data. Therefore, documents and information which are transacted are also in electronic form. In virtual space, all transactions are done via data transfer and individuals conduct transactions via their information systems. Just like traditional paper space, disagreements are possible in virtual transactions too. Therefore, discussions on evidenceare also used in electronic environment and are considered as one of the aspects of ecommerce law. Electronic documents and evidencecan be presented in a court of law and electronic data can be as valid as paper documents. Therefore, identification of electronic documents and evidence should not be doubted because acceptance of electronic contracts and transactions involves accepting the documents and information based upon electronic data which are traded. Iranian ecommerce law is extracted from Uncitral sample law and has similar regulations. Article 12 of the aforementioned Law states: "documents and evidence proof of claim may come in the form of data message and its value cannot be rejected or ignored in any court of law due to its format." As it can be seen, regulations give validity to data messagesand consider electronic documents as legal reasons. Uncitral sample law on ecommerce (approved in 1996) explains the fact that whether all electronic data have proofing values as "when concluding a contract, requirement and acceptance can be announced via data messageها , the validity and ability to execute the contract cannot be rejected purely and simply for using data messages." As it can be seen, the aforementioned article clearly accepts electronic contract and gives validity and ability to execute to such contracts."

Iranian ecommerce laws

Iranian ecommerce Law was extracted from Uncitral sample law and approved by Iranian Parliament and Guidance Council. The following items concern digital signature: article 7. When the law necessitates a signature, an electronic signature will suffice. Article 10. A definite electronic signature must have the following features: -it must be unique for the signer.-it must clarify the identity of the signer of "data message". –it must be issued from the signer.-it must attach to a data message in a way that any kind of change in that data message can be discovered. Article 11. A confident electronic background means a "data message" which is stored by observing conditions and terms of a secure information system and can be accessed when necessary. article 14. All data messages which are generated and stored safely are valid in courts and legal authorities in terms of contents and signatures, both sides' commitments, execution of the terms and other effects. Article 15. Denial and doubt about definite data message, and secure electronic background and electronic signature and one can only claim about forgery of data message and prove nullity of data message. Article 31. Electronic certification issuance service offices are units which are established for providing electronic signature issuance services nationwide. These services include generation, issuance, storage, sending, verification, nullification and updating certificationsof electronic signatures.

Electronic transactions security

In the traditional method, validity of a document depended on being written, being original, being stamped and closed. In electronic data transaction, confidentiality is provided via encryption and electronic signature. Using asymmetric encryption algorithms and services of a digital certification center we can add security to electronic transactions. In a real system, the relation between origin and destination can be attacked in four manners: disconnection of relation, eavesdropping, change in identity and copying an identity. In addition to such attacks, the sender may deny its work after sending information. By security issues, we mean protection of data and information security against illegal accesses in ecommerce process. Users' actions and activities and tastes are traced and monitored. Their data and information are copied easily and transferred. Internet is a completely open network and individuals' personal information may be accessed illegally. For instance, if a person's credit card number is disclosed to illegal people, they might abuse it. Therefore, protection of financial, credit and personal information is one of the important challenges ahead of ecommerce. This is because information circulation volume and resources are abundant on internet. Therefore, it is not clear where the information goes and who uses it (BidgoliHosein, 2005, 57 and 83).

Digital signature and its security

A digital signature security contains public key encryption algorithm security, security of mixedسازي functions, and private key security. In order to validate the signature of any person, his or her public key is used. A digital signature is designed in a way that not only extraction of message from the signature is impossible but also it is not possible to find two messages with similar signatures. A sender gives his or her message and private key to an encryption procedure. The output of this process is an encrypted text of the main text which is called digital signature. Then, this signature is attached to the message text and is sent. A receiver receives the text of a message and signature and decrypts the signature by public key of the sender to acquire the primary text in order to control the identity of the sender. If a text is the same as the main received text, it can be concluded that message text and signature are neither forged nor altered halfway.

Encryption

The main solution for establishment of security in electronic transactions and confrontation with problems is encryption. Using encryption, we can prevent from disconnection attacks as well as other attacks and threats. Key-based encryption (as opposed to algorithm-based encryption) is the most appropriate method and usully encryption means actually key-based encryption. A key is a data value which is used in encryption algorithm. Key-based encryption algorithms are classified in two categories: symmetric and asymmetric encryption. Encryption is a science which can help transfer information securely even if communicational paths (data transfer paths) are not secure. Encryption can be used for security and validity provision of a message. Message security provision: the fact that no one can understand a message text except the licensed receiver. Message validity: the fact that the real sender of a text is obvious.

Conclusion

Development of ecommerce and globalization of economy and increasing growth of internet has turned ecommerce into a comprehensive and widespread way of commerce. Ecommerce is a part of human life in today's world. Global village involves us to prepare necessary infrastructure for ecommerce and ignorance of this issue will be disastrous in future.

Most organizations prefer to eliminate paper work and use electronic forms for receiving and sending information. In this case, the sender and receiver must validate each other. A digital signature has the

applications of a written signature but it has the advantage over written signature: it cannot be forged or copied easily (P. PrapoornaRoga, P.S. Avadhani, 2007, No. 7). Consequently, proof of certification, rules and regulations can be used for facilitation of electronic signature use. Electronic signature is a satisfactory technical instrument and legal element.

REFERENCES

Avadhani. P. S ،Chalamaih. N and Prapoorna Roja. P. "Secure Transit Of Confidential Documents Over Intermet Using High Speed RSA Algorithm ،"Proceedings OF CCCT – O4 ،International Conference held in Texas Austin ،USA ،in Aug-2006.

Brian Gladman ،Carl Ellison and Nicholas Bohm ،"Digital Signatures ،Certificates and Electronic Commerce" ، Version l. l ،revised 8th june1999

Bidgoli ،Hossein ،Electronic Commerce: Principle and Practice ،-Stephen Chen. Strategic Management of e-Business.2005.

Hung-Zih Liao ،Yuan-Yuan Shen ،"On the Elliptic Curve Digital Signature Algorithm" ،Tunghai Science Vol. 8,July ،2006.

Jeffry Hoffstein ،Jill Pipher and Joseph H. Silverman "NTRU: A High Speed Public Key Cryptosystem" ،Pre Print Presented At He Hump Session Of Euro Crypt 96 ،1996.

J .Hoffstein ،J. Pipher ،J. Silverman "NTRU: A Ring Based Public Key Cryptosystem" ،Algorithmic Number Theory (ANTS III) ،J.P. Buhler (ed ،(.Lecture Notes in Computer Science ،Springer-Verlag ،Berlin ،Vol 1423 ،pp , Portland ،OR ،June 1998.

J. Hoffstein ،D. Lieman ،J. Silverman"Polynomial Rings and Efficient Public Key Authentication ،"Proceeding Of the International Workshop on Cryptographic Teehniques and E-Commerce (CrypTEC 99) ،M. Blum and C.H. Lee ،eds. ،City University of Hong Kong Press ،1999.

Loran Brazel ،Electronic Signatures Law and Regulation. ،Sweet & Maxwell ،London ،2004

Mohammad JafarJafariLangroudi, Terminology of Law, fifth printing, Ganj-e-Danesh publications, Tehran, 1991.

NaserKatouziyan, proof and proof evidence, volume 1, Mizan Publications, Tehran, 2001.

P. Prapoorna roga ،and P .S. Avadhani "Digital Signature Development Using Truncated Polynomials ، " IJCSNS International Journal of Computer Science and Network Security ،VOL. 7 , July 2007.

R.L. Rivest. RFC 1321: The MD5 Message-Digest Algorithm. Internet Activities Board ،April 1992.

R.L. Rivest ،A. Shamir ،and L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM ،21(2): ،February ،1978.