ARTICLE:

ELECTRONIC SIGNATURES IN IRAN

By **Dr Parviz Savrai**

Introduction

In 2004, the Parliament of Iran passed the Electronic Commerce Law of the Islamic Republic of Iran. The Act commenced operation on 22 January 2004 by virtue of articles 1 and 2 of the Civil Code of Iran, providing for the general conditions of an Act entering into force:

> Article 1 – The Islamic Consultative Assembly's enactments and the results of the referendum, having gone through legal procedures will be notified to the president of the Republic. The President shall within five days sign them and notify them to executors, and issue instruction to have them published, and the Official Gazette shall be required to publish them within 72 hours after notification thereof.
>
> Note: In case of the President's refusal to sign or notify an enactment within the time period referred to in this Article, the Official Gazette shall be required to publish it within 72 hours on the order of the Chairman of the Islamic Consultative Assembly.
>
> Article 2 – The legislative enactments come into force throughout the country fifteen days after their publication, unless a specific arrangement has been prescribed in the given legislation itself to the timing of its enforcement.
>
> Article 3 – The text of laws must be published in the Official Gazette.

The Act was passed to remove concerns about uncertainties over e-commerce and to clarify some of the ambiguities in the Iranian legal system. There are a number of issues raised by the Act, but it is not intended to consider all of them in this article. The purpose here is to concentrate on one particular issue relating to a particular subject of the Act, namely, the electronic signature.

Admissibility and evidential value of electronic documents

Article 2(a) defines 'Data Message' as follows:

> 'Any representation of facts, information, and concepts generated, sent, received, stored, or processed by use of electronic, optical or other information technology means'.

According to the definition, an electronic document can be any document that is generated or stored on a computer. In essence, this means any digital data, although the data will be categorized such as a letter, a contract, an agreement, a will, an image, a drawing, a sound or even a photograph. An electronic signature can be used to sign these documents. In Iranian jurisprudence, the evidential value of an electronic document has two distinct aspects: the first is the validity and binding force of the electronic document; and the second is the admissibility of the electronic document as evidence in legal proceedings.

The provisions of article 6 permit a data message to be used as a replacement document, with the exception of the following cases:

1. Ownership documents of immovable property.
2. Sale of medical materials to the final consumer.
3. 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.

Other forms of document in electronic format are legally binding in the same way as paper documents.

In this regard, articles 12 and 13 provide that evidence and any supporting document may be in the form of a data message. The evidential value of a data message can by no means be rejected solely due to its form and framework at any court or governmental office, and generally the evidential value of a data message depends on the methods used to guarantee its security, such as selecting a security measure that corresponds to the subject and purpose of the data message.

In respect of private agreements, article 9 specifies that under circumstance where the distribution of a data message is terminated from a certain point in time and is replaced with a paper document, this shall be expressly stated in the paper document. Such a replacement does not affect the previous rights and obligations between the parties. It should be added that under the provisions of article 8, where the law requires that the information be presented or retained in its original form, it is also possible to retain it as a data message if the following requirements are met:

1. The information is accessible so as to be usable for subsequent reference.

2. The data message is retained in the same format it was generated, sent or received or in a format that can exactly represent the information generated, sent or received.

3. The information, if any, enabling the identification of the origin and destination of a data message and the date and time when it was sent or received is also retained.

4. Other provisions that an institution, organization, and governmental agency or ministry has set down within the scope of their functions are retained.

Secure method of generating electronic documents

A secure method of generating electronic documents means a method under which a data message is stored by the observance of the requirements of a secure information system and which is accessible and can be viewed when needed (article 11). Paragraph (l) of article 2 'Secure Method' provides as follows:

> 'A method to authenticate the correctness, the origin and the destination of a "data message", along with its date and to detect any error or modification, in communication, content, or storage of a "data message" from a certain point. A secure message is generated using algorithms or codes, identification words or numbers, encryption, acknowledgement call-back procedures or similar secure techniques'.

Article 15 provides that the validity of a secure electronic record and a signature may not be questioned or denied; only a claim of forgery or a proof of its invalidity on a legal basis may be considered. The provisions of article 15 do not preclude a challenge to the validity of an insecure electronic record and signature. It may be questioned or denied, and a claim of forgery or a proof of its invalidity can be asserted on a legal basis.

Signature

Before passing the law, it was unclear whether electronic signatures constitute signatures in the sense of the law. It was a common opinion that only a manuscript signature constituted a signature in the legal sense. The law does not define the basic and traditional definition of a signature; but according to the customary law, it is a distinctive mark, characteristic, or symbol placed at the bottom of a document as a guide to the proper sequence of the document in binding as well as a proof of identity.[1] Thus, the function of a signature is evidential: it authenticates a writing by identifying the signer with the signed document and their intention that it has legal effect.[2]

Electronic signature

The traditional definition of a signature is not technology specific, and reliance on the meaning of a signature in the physical world would make it virtually impossible to use technology to provide services and to meet all the legal and evidentiary requirements at

1 *As opposed to the common law system, the Iranian legal system does not rely on previous case reports. Only decisions of the united chambers of the Supreme Court are published and are considered as judicial precedent. For a comprehensive discussion of the case law in a number of common law countries on the meaning of a signature, see Stephen Mason, Electronic Signatures in Law (Tottel, 2nd edn, 2007), Chapter 2.*

2 *There are also a number of other functions of a signature. The reader is directed to a full discussion of this in Stephen Mason, Electronic Signatures in Law, 1.20 – 1.26.*

the same time. To address this problem, article 2 (paragraph J) of the e-commerce law provides a definition of electronic signature which reads as follows: 'Any sign appended or logically affixed to a data message which may be used to identify its signatory'. It appears that the legislator has intentionally defined electronic signature broadly so it does not prevent the use of new potential technologies in the future.

Just as electronic documents can be used as evidence in legal proceedings, so electronic signatures are as legally binding as manuscript signatures. The word 'sign' here could mean any electronic sound, symbol, or process attached to or logically associated with a record adopted by a person with the intent to sign the record This record or signature may not be denied legal effect or enforceability solely because it is in electronic form.[3]

Although the electronic signature is basically a technical issue, it is also a legal issue. The term electronic signature could be divided into the secure and the insecure. For example, a person's initials at the end of an e-mail could be considered an insecure electronic signature; while a secure electronic signature is based on public key technology that uses asymmetric cryptography (a digital signature).

Secure electronic signature

A secure electronic signature should be unique to the signatory. The law provides that an electronic signature is a signature that can be used to authenticate the identity of the sender of a message or the signer of a document. It can also be used to ensure that the original content of the message or document sent is unchanged.

Regarding the secure signature, article 10 provides as follows:

> 'A secure electronic signature must contain the following requirements:
>
> a) Be unique to the signatory.
>
> b) Identify the signatory of 'data message'.
>
> c) Be signed by the signatory or under his or her sole intention.
>
> d) Be affixed to a 'data message' in a way that any change in data message can be detected and identified'.

A secure electronic signature is a digital signature that uses the Public key Infrastructure (PKI) with public and private keys, including a Certification Service Provider to generate and manage secure electronic signatures. Whilst the public key is distributed widely, the corresponding private key, which is specifically assigned and unique to the user, should be kept by its owner in a secure place. The owner is responsible for safeguarding access to the private key.[4]

Concluding comments

Electronic signatures are now recognized by law and thus have great potential. With legal validity, electronic signatures have a prominent role to play in the progress of electronic commerce in Iran. The most important aspect of legal validity of electronic signature is that the law has provided a stable legal platform for the e-commerce market, enabling companies, organizations and individuals to use them in commerce with confidence. Electronic signatures, particularly secure electronic signatures, have the capacity to signify the approval to the terms of a contract or a document that is presented in an electronic format. Any uncertainty about whether transactions made and 'signed' through entirely electronic means has been removed. As a result of the implementation of the Act, Iranian lawyers, legal advisors and judges have started reviewing the methodology, practices, and rules that apply to electronic transactions.

Dr Savrai is an assistant professor of law (Faculty of Law, Shahid Beheshti University, Tehran), a member of the Iranian Bar (First Grade Attorney at Law and Legal Advisor), and was a legal advisor to the Bureau of International Legal Services [Iran-U.S.A. Claims Tribunal] and the Trade Promotion Organisation of Iran.

http://www.iran-attorney.com/

savrai@iran-attorney.com

3 Articles 6, 7, 12, 13, 14 and 15 of Electronic Commerce Law of Iran.

4 Although it is exceedingly difficult to secure the private key of a digital signature, for which see the Russian banking cases that illustrate this problem: Olga I. Kudryavtseva, ' The use of electronic digital signatures in banking relationships in the Russian Federation', (2008) 5 Digital Evidence and Electronic Signature Law Review, 51 – 57; Alex Dolzhich, ' Digital evidence and e-signature in the Russian Federation: A change in trend', (2009) 6 Digital Evidence and Electronic Signature Law Review, 181 – 183.

