February 2004

The Turkish Electronic Signature Law

By Mehtap Yildirim-Öztürk, Member of Ankara and New York Bars, and Çagdas Evrim Ergün, Member of Ankara Bar, lawyers with Cakmak Law Office. The authors may be contacted by e-mail at: c.ergun@cakmak.gen.tr.

Introduction

Recent years have witnessed an increasing interest in ensuring the authenticity and confidentiality of electronic communication and electronic commerce. As a result of such interest, as well as Turkey's efforts to harmonise its laws with E.U. legislation, Turkey has recently enacted its first statute dealing directly with electronic signatures, namely E-Signature Law No. 5070 (the "Law").[1]

The term e-signature[2] is very broad: it would even encompass a scanned image of a hand-written signature in a word processed document. For the purpose of this article, however, the term "e-signature" refers to an advanced form of signature which requires the use of some form of encryption, *i.e.*, making data meaningless for all parties other than the intended parties by using certain codes and ciphers,[3] and which provides a considerable degree of assurance that the signature is that of a particular person. In other words, the e-signature, in terms of this article, may be defined as a string of electronic data used to identify the sender of an electronic message; in much the same way as a hand-written signature identifies an individual.[4]

Both the Law and the E.U. E-Signature Directive No. 99/93 (the "E.U. Directive") similarly define the e-signature as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

The term "signatory" is defined under the Law as an individual, i.e. real person, who utilises a signature-creation device to create an e-signature. The E.U. Directive, however, defines the signatory as a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. Hence, the definition of signatory under the E.U. Directive also includes the legal entities, whereas the Law does not consider legal entities as signatories.

The competent Authority provided by the Law is the Telecommunications Authority (the "Authority") which is empowered to issue the relevant secondary legislation and to regulate and supervise the activities of the electronic certification service providers ("CSPs").

Basic Features of the Law

Purpose and Scope

The purpose of the Law is to facilitate the use of e-signatures by determining the principles concerning their legal and technical aspects. Similarly, the E.U. Directive aims to facilitate the use of e-signatures and to contribute to their legal recognition.

Both the Law and the E.U. Directive cover the legal nature of e-signatures, the activities of the CSPs and the principles concerning the utilisation of e-signatures. In addition, the Law also covers the conditions for the cancellation of qualified electronic certificates and the criminal and administrative sanctions envisaged for violation of the Law.

The E.U. Directive explicitly provides that it does not cover aspects related to the conclusion and validity of contracts. Although the Law does not explicitly provide such a provision, it does not deal with the aspects relating to the conclusion and validity of contracts either, since the objectives of both the Law and the E.U. Directive are limited to give legal effectiveness to the e-signatures.

E-Signature

Differences Between E-Signatures and Secured Electronic Signature

The Law makes a distinction between e-signatures and the secured e-signatures. An identical distinction is made between the e-signatures and the advanced e-signatures under the E.U. Directive. Despite their terminological difference, both the concepts of secured e-signatures under the Law and the advanced e-signatures under the E.U. Directive refer to the same concept.

In order to qualify as a secured e-signature under the Law, or as an advanced e-signature under the E.U. Directive, an e-signature must be:

- uniquely linked to the signatory;
- capable of identifying the signatory;

- created using means that the signatory can maintain under his sole control; and
- linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Legal Effects of Secured Electronic Signatures

Article 5(1) of the Law provides that a secured e-signature creates the same legal effects as a handwritten signature. An exception to this is set out in Article 5(2) of the Law, which states that e-signatures have no legal effect in the security contracts and transactions required by law to be performed in an official form or through certain procedures.

Similarly, the E.U. Directive states that an advanced electronic signature satisfies the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data.

Articles 22 and 23 of Law No. 5070 amend the Turkish Code of Obligations No. 818 and the Turkish Civil Procedural Law No. 1086, respectively, so as to ensure that documents duly signed with a secured e-signature qualify as evidence, which in legal proceedings is as binding as a document signed with a hand-written signature.

The E.U. Directive also states that an advanced electronic signature is admissible as evidence in legal proceedings.

E-Certificates

Both the Law and the E.U. Directive define the term "certificate" as an electronic attestation which links signature-verification data to a person and confirms the identity of that person.

Differences with the Qualified E-Certificate

Both the Law and the E.U. Directive provide that a "qualified e-certificate" must contain certain statements, such as:

- an indication that the certificate is issued as a qualified certificate;
- the identification of the CSP and the name of the country in which it is established;
- the name of the signatory, which shall be identified as such;
- an indication of the beginning and end of the period of validity of the certificate;
- the advanced e-signature of the CSP issuing it;
- limitations on the scope of use of the certificate, if applicable; and
- limits on the value of transactions for which the certificate can be used, if applicable.

In addition to the above-mentioned requirements, the Law stipulates that a qualified e-certificate must also include the professional and other personal information regarding the holder of the qualified e-certificate, if so requested by the holder of that e-certificate.

E-Certification Service Provider

Both the Law and the E.U. Directive define the "e-certification service provider" as an individual or legal entity that issues certificates or provides other services related to electronic signatures.

The Law stipulates that the e-certification service providers must, among other things:

- verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
- in cases where the CSP generates signature-creation data, guarantee security and confidentiality during the process of generating such data;
- record all relevant information concerning a qualified certificate for an appropriate period of time; and
- in the event it terminates its operations, notify the Authority and the e-certificate holders of that fact.

The E.U. Directive, however, does not require all e-certification service providers, but only those which issue qualified e-certificates, to fulfil the above stated conditions.

Foreign E-Certificates

The Law provides that the legal effects of an e-certificate which is issued by an e-certification service provider established in a foreign country shall be determined pursuant to the international agreements. Moreover, in the event that an e-certificate issued by a foreign e-certification service provider is recognized by a Turkish e-certification service provider, such recognized e-certificate shall be considered as a qualified e-certificate in Turkey.

In contrast with the Law, the E.U. Directive only recognises the admissibility of qualified e-certificates, whereas the Law does not make such a distinction between e-certificates and qualified e-certificates in this respect. The E.U. Directive sets forth that certificates which are issued as qualified certificates to the public by an e-certification service provider established in a third country are recognised as legally equivalent to certificates issued by an e-certification service provider established within the European Union, provided that:

- the e-certification service provider fulfils the requirements laid down in the E.U. Directive and has been accredited under a voluntary accreditation scheme established in a E.U. Member State; or
- an e-certification service provider established within the European Union, which fulfils the requirements laid down in the E.U. Directive, guarantees the certificate; or
- the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the European Union and third countries or international organisations.

Supervision and Penalty Clauses

Articles 15 to 19 of the Law set forth the supervision mechanism and the penalty clauses envisaged for non-compliance with its provisions.

Pursuant to Article 15 of the Law, the Authority is empowered to supervise the e-certification service providers. Articles 16 and 17 of the Law envisage certain fines and imprisonment penalties from one year to five years for the unauthorised use of signature creation data and the creation of partially or completely forged e-certificates. Such activities also constitute another crime provided in the Turkish Criminal Code, namely the information crime, which envisages an imprisonment penalty of one to six years. The Law provides that if the actions stated in Articles 16 and 17 of the Law also constitute another crime pursuant to another law, both penalties provided under such different laws shall be applied. Consequently, any person who uses an e-signature creation data without authorization, or who creates, partially or completely, a forged e-certificate, shall be punished by an imprisonment penalty of one to eleven years.

Article 18 of the Law regulates the administrative fines applicable to the violation of certain provisions thereof. Lastly, Article 19 of the Law provides that the operations of the e-certification service providers may be terminated by the Authority in the event that certain provisions of the Law are violated three times within a time period of three years from the first violation.

The E.U. Directive does not regulate the supervision of the compliance, or the penalties for the violation, of its provisions. It merely states that the E.U. Member States may decide how they ensure the supervision of compliance with the provisions laid down in the E.U. Directive.

Conclusion

There seems little doubt that e-commerce will continue its expansion in the coming years despite the concerns regarding the lack of security in online transactions. As Lloyd wrote, “if the Internet creates the problem, it may also provide the solution”.[5] Similarly, if the risks of confidentiality and authenticity of e-communication and e-commerce constitute a problem, e-signature would certainly serve as a solution. Hence, e-communication and e-commerce necessitate the use of legally effective e-signatures and related services allowing data authentication. To this end, the enactment of the Law has been beneficial to meet both business and consumer needs in many respects. Having analysed the multiple aspects of the Law, it appears that the Law has a number of advantages facilitating the performance of e-communication and e-commerce, such as the recognition of legal effects of e-signatures and the regulation of the activities and liabilities of the e-certification service providers.

Much remains, however, to be done regarding the legal framework governing e-commerce in Turkey. The regulation of electronic cash, for instance, is indispensably needed for an efficient and secure operation of e-commerce. Moreover, the provisions regarding the law applicable to international online transactions~~,~~ and the place of jurisdiction for such matters should be specially regulated with respect to e-commerce.

As regards the impact of the Law on e-communication and e-commerce in Turkey, a more accurate assessment can only be made once the necessary secondary legislation is issued by the Authority, pursuant to Article 20 of the Law.

[1] Published in the Official Gazette No. 25355, January 23, 2004.

[2] The term “e-signature” for the purpose of this article is used in a “catch-all” sense for the terms “digital signature” and “soft signature”.

[3] See esp. Lloyd, I. J., *Information Technology Law*, London, 2000, p. 578 *et seq.*

[4] Edwards & Waelde, *Law and the Internet*, 2000, p. 38.

[5] Lloyd, I. J., *op. cit.* p. 591.