The electronic signature law in Turkey

PEKIN & PEKIN

As a result of recent technological developments, parties resident at different places and jurisdictions may enter into contracts through communication via their computer. As a result, the requirement of execution and exchange of such contracts by the use of valid and binding signatures has emerged as an important legal problem. With a view to harmonizing our national law with the legal practices in various countries and satisfying the needs of the new method of communicating, an Electronic Signature Law was passed and published in the Official Gazette on 23 January 2004. This Law, no. 5070, will enter into force as of 22 July 2004.

Purpose and scope of the law

The law sets down legal and technical aspects of electronic signature and principles on use of electronic signature and deals with:

- The legal definition of an electronic signature.
- The activities of electronic certificate service providers.
- Rules on the use of electronic signature in all aspects.

■ Concept of the electronic signature

Article 3 defines an electronic signature as:

electronic data which is added to or has a logic link with another electronic data and is used for identity verification purposes	baska bir veriye eklenen veya elektronik veriyle mantıksal baglantisi bulunan ve kimlik dogrulama amacıyla kullanılan elektronik veri

"Electronic data" is defined as all records and data that are generated, carried or stored by electronic, optic or similar other ways.

Provision has been made for a "secure electronic signature", which, in accordance with article 4, is an electronic signature which:

- belongs solely and only to the signing party; and
- is created by using "secure electronic signature tool" that is only at the disposal and under control of the signing party; and
- is used for verification of identity of the signing party in reliance upon a "qualified electronic certificate" and
- can be used for detection of any subsequent change or modification in a signed "electronic data".

Activities of Certificate Service Providers:

■ Who may offer these services:

An "electronic certificate service provider", as provided for in article 8, is a new concept used in Turkish law and refers to providers of the services relating to:

- electronic certificate,
- time stamp and
- electronic signature.

A certificate service provider may include public entities and organizations, private law legal entities or natural persons.

If certificates are generated by the service provider, it has a responsibility to provide for the confidentiality and security of the certificate

■ Start of activities

Electronic certificate service providers may start their business activities two months after sending a notice to the Telecommunication Authority certifying that they satisfy the required conditions and qualifications.[1]

Pursuant to article 8, these service providers start their activities two months after the date of notice delivered to the Telecommunication Authority, and if, during performance of their activities, it is at any time determined that the service provider fails to "use secure products and systems" or "perform and render the services securely" or "take all kinds of measures for prevention of imitation and alteration of certificates", first, a certain period of time not exceeding one month is granted to the service provider to correct and remedy any default, and its activities are immediately stopped and suspended. If the default is not corrected or remedied by the end of this period of time, its activities are terminated.

■ Information on and contents of a "Qualified Electronic Certificate"

According to article 9, a certificate service provider is required to clearly write on a "qualified electronic certificate" issued and provided to its client that the certificate is a "qualified electronic certificate". Article 9 further provides as follows:

- The certificate is required to include the identity data of the service provider and name of its home country.
- Identity data for "identification" of the signing party is also given in this certificate.
- The certificate contains signature verification data corresponding to the signature formation date. Signature verification data refers to cryptographic keys and codes used for verification of an electronic signature.
- 'Validity term' and 'serial number' of the certificate, and if the certificate holder is an agent, information about the principal, and if requested by the certificate holder, professional or personal data and information of the certificate holder must also be given in the certificate.
- Conditions of use of the certificate, and restrictions on transactions where the certificate may be used, if any, will also be inserted in the certificate.
- The certificate must also contain the secure electronic signature of the service provider, verifying the accuracy of the information in the certificate.

■ Liabilities of certificate Service Provider

In accordance with the provisions of article 10, the service provider is required to securely determine and verify the identity of the client, and the identity of both the certificate holder authorized to act for and on behalf of another person and the person in whose name the certificate holder acts, in reliance upon and according to official identity documents. If certificates are generated by the service provider, it has a responsibility to provide for the confidentiality and security of the certificate.

Under article 9, the service provider is required to inform its clients in writing before the delivery of the certificate about the conditions of use of certificate; and

- the methods by which disputes can be resolved; and
- that an electronic signature is equivalent to a manual signature; and
- that the client must not let third parties use the signature formation data corresponding to signature verification data.

The service provider is required to keep all relevant records for a period of time to be specified in the Regulation, which has not yet been issued. Where the service provider ceases its activities, it is required to inform the relevant bodies and authorities, mainly the Telecommunications Authority no later than three months before ceasing its activities.

■ Prohibitions on a Service Provider

Electronic certificate service providers are not allowed to take and keep copies of the "signature formation" data or to store any such data, pursuant to article 16.

■ Protection of information by a Service Provider

In accordance with article 12, a service provider:

- may not request or receive information, other than the information requisite for issuance of a certificate, from its clients; and
- may not keep the certificates within reach of third parties; and
- may not disclose to third parties or use the collected information without a prior consent of the certificate holder.

[1] Telekomünikasyon Kurumu, http://www.tk.gov.tr.

■ Legal liability of a Service Provider

The liabilities of a certificate service provider to electronic certificate holders are subject to the provisions of the general law. Under article 13, a service provider is liable to indemnify and hold third parties harmless from all kinds of damages and losses attributable to a breach of laws by the service provider, and is further held liable for all acts of its employees. All kinds of limitations or disclaimers of liability of the service provider are invalid, pursuant to Article 13. The service provider is under an obligation to take out and buy a "certificate financial liability insurance" in accordance with the provisions of article 13.

Legal consequences of a secure electronic signature

■ The principle

Pursuant to provisions of article 5 of the Law, a secure electronic signature is the equivalent of a manual signature with respect to its legal results *(guvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu dogurur).*

■ Where electronic signature is not accepted

Article 5 of the law provides that:

(i) legal transactions and deals that are subject to an 'official form' pursuant to laws, or
(ii) legal transactions and deals that are subject to a 'special procedure' pursuant to laws, and
(iii) 'warranty and guarantee contracts' cannot be signed by a secure electronic signature".

■ Details on exclusions

Requirements on form of contracts are as described below. Turkish law generally deals with the form of a contract in two separate categories, namely:

■ legal form requirements and
■ voluntary form requirements.

Legal form stands for the form of contract stipulated by the relevant laws. If the form of a contract is envisaged in a mandatory law provision, that form constitutes a basic condition of 'validity' of the contract. Examples include a surety for bail or a bond referred to in article 484 of the Code of Obligations; the assignment of receivables (article 163/1 of the Code of Obligations); contract of maintenance for life (article 512 of the Code of Obligations) and marriage contract (article 134 of the Turkish Civil Code).

Voluntary form refers to the form agreed upon between the parties of a contract that is not subject to any form requirements for validity.

On the other hand, in 'written form', the declarations of will of the parties to a contract are written and then signed by the party or parties who assume obligations. For instance, donation promise (article 238/1 of the Code of Obligations) and real estate brokerage contract (article 404/IV of the Code of Obligations).

'Official form' refers to the signature of a contract by or before an official authority, such as a notary public or title deed registry. A notary public is required to sign an official testament such as a will and in the case of a land registry, for the purchase and sale of a real estate. Transactions conducted in official form are considered and treated as valid and true unless and until proven otherwise, in that the official form is, in itself, evidence of the underlying transaction.

This is to say that the Turkish law has substantially restricted the freedom of form in contracts both in terms of validity of contract and for the sake of facilitating the proof of contract. The Turkish Law no. 5070 restricts the freedom of form by restricting the use of secure electronic signature in contracts such as those relating to warranty and guarantee because they are subject to a special procedure or an official form pursuant to the applicable laws.

■ Foreign Electronic Certificates

This issue can be discussed under two headings according to the laws:

■ Certificates accepted by a Turkish Provider

Article 14 of the law stipulates that an electronic certificate service provider established in Turkey may be 'accepted' by an electronic certificate service provider resident in a foreign country. In this case, in accordance with article 14 the law, the foreign electronic certificates are considered and treated as "qualified electronic certificates". If and when the use of this type of electronic certificates causes damage and loss, the service provider in Turkey will be held liable for such damage and loss pursuant to article 14.

■ Certificates received directly from a foreign provider

A foreign 'electronic certificate service provider' founded and active in a foreign country may issue

In this case, in accordance with article 14 the law, the foreign electronic certificates are considered and treated as "qualified electronic certificates"

and provide electronic certificates; provided, however, that the legal results of these certificates are subject to and governed by the relevant international agreements, pursuant to article 14. Provisions of the relevant international agreements, if any, will be applicable for indemnification of the damages and losses that may arise out of use of this type of certificates.

■ Audit

Pursuant to article 15 of the Electronic Signature Law, the activities and transactions of electronic certificate service providers will be audited by the Telecommunication Authority, if and when deemed necessary.

■ Sanctions

According to article 18, one who: collects or obtains signature formation data; or acquires or obtains signature formation tools; or gives these tools; or copies these tools; or recreates these tools; or creates an 'unauthorized electronic signature' by using signature formation tools acquired or obtained without authority without and beyond the consent of the relevant person will be sentenced to imprisonment from one year to three years and can be subject to various fines.

In addition, one who:

- issues and creates fully or partially false electronic certificates; or
- imitates or alters a valid electronic certificate; or
- issues and creates electronic certificates 'without authority'; or
- knowingly uses electronic certificates that are false, imitation, altered or unauthorized

will be sentenced to imprisonment from two years to five years and various fines.

Furthermore, various administrative fines are imposed on service providers that violate the laws.

■ Regulations

The details of implementation will be regulated by various regulations required to be adapted and enacted until 23 July 2004. This is to say that the provisions of the Regulations to be enacted are also required to be complied with. These regulations have not yet been issued by the Telecommunications Authority. ■

The Pekin & Pekin law firm was established in 1971, and has a reputation for its legal services to international and multi-national companies all over the world. Pekin & Pekin is located in the center of Istanbul at 10 Lamartine Caddesi, Taksim 34437, Istanbul

http://www.pekin-pekin.com