Unofficial Translation of Turkish Electronic Signature Ordinance by Telecommunications Authority

Important Notice: In case of divergent interpretation, the original Turkish text shall prevail.

ELECTRONIC SIGNATURE LAW

(Published in the Official Gazette ref 25355, 2004-01-23)

SECTION ONE

Purpose, Scope and Definitions

Purpose

Article 1 – The purpose of this Law is to define the principles for the legal and technical aspects and application of electronic signatures.

Scope

Article 2 – This Law covers the legal status of electronic signatures, operations concerning electronic signatures and the activities of Electronic Certificate Service Providers (ECSPs).

Definitions

Article 3 – The definitions and abbreviations used in this Regulation have the following meanings:

a) Electronic Data: Information which are generated, transferred or stored in electronic, optical or similar methods,

b) Electronic Signature: Data in electronic form that are attached to other electronic data or linked logically to that electronic data and used for authentication,

c) Signature Owner: A natural person, who uses an electronic signature creation device in order to generate electronic signatures,

d) Signature Creation Data: Unique data such as password and cryptographic keys belonging to a signature owner and being used by the signature owner in order to create electronic signatures,

e) Signature Creation Device: Software or hardware products using the signature creation data in order to generate electronic signatures,

f) Signature Verification Data: Data such as passwords and cryptographic public keys used for the verification of electronic signatures,

g) Signature Verification Device: Software or hardware products using the signature verification data for verification of electronic signatures,

h) Time-Stamping: An record signed electronically by the ECSP for the purpose of verification of the exact time of creation, alteration, sending, receiving and/or recording of an electronic data,

i) Electronic Certificate: Electronic data binding the signature verification data of the signature owner to identity data of that person,

j) Authority: Telecommunications Authority.

SECTION TWO

Secure Electronic Signature and Certification Services

PART ONE

Secure Electronic Signature, Secure Electronic Signature Creation and Verification Devices

Secure Electronic Signature

Article 4- A Secure Electronic Signature shall be a signature that;

a) is exclusively assigned to the Signature Owner,

b) is generated with the Secure Electronic Signature Creation Device which is kept under the sole control of the signature owner,

c) enables the identification of the Signature Owner based on the Qualified Electronic Certificate,

d) enables detection as to whether signed electronic data has or has not been altered or not subsequent to the signature being applied.

Legal Effect and Area of Application of Secure Electronic Signature

Article 5- A secure electronic signature shall have the same legal effect as that of a handwritten signature.

A secure electronic signature shall not be applicable to legal proceedings subject to a special procedure or an official form pursuant to laws and warranty contracts.

Secure Electronic Signature Creation Devices

Article 6- Secure Electronic Signature Creation Devices are Signature Creation Devices which ensure that;

a) Electronic Signature Creation Data produced by those devices are unique,

b) Electronic Signature Creation Data recorded in those devices cannot be derived in any means and that their secrecy is assured,

c) Electronic Signature Creation Data recorded in those devices cannot be obtained or used by third parties and that electronic signatures are protected against forgery,

d) The data to be signed cannot be altered by anyone except the signature owner and can be seen by the signature owner before the generation of a signature.

Secure Electronic Signature Verification Device

Article 7- Secure Electronic Signature Verification Devices are Signature Verification Devices which;

a) display without any alteration the data used for verification of the signature to the person who makes verification,

b) manage the signature verification process in a reliable and accurate way, and display the results of verification without any alteration to the person who makes verification,

c) ensure that signed data is displayed in reliable manner when necessary,

d) display without any alteration its results to the person who makes verification establishing in a reliable manner the authenticity and validity of the electronic certificate used for the verification of the signature,

e) display without any alteration the identity of the signature owner to the person who makes verification,

f) ensure the detection of any alterations that effect the conditions relevant to the verification of the signature.

PART TWO

Electronic Certificate Service Provider, Qualified Electronic Certificate and Foreign Electronic Certificates

Electronic Certificate Service Provider

Article 8 – For the purposes of this act, Electronic Certificate Service Providers shall be public entities or establishments or natural persons or private law legal entities that provide qualified electronic certificates, time-stamping and other services related to qualified electronic signatures. Electronic Certificate Service Providers shall commence its operations within a period of two months from the date of notification.

Electronic certificate service providers shall show in detail in their notification that they ensure the provisions related to;

a) Using secure products and systems,

b) Managing operations in a reliable way,

c) Taking all necessary measures in order to avoid certificates being copied or distorted.

If the Authority determines the incompleteness or infringement of any of the above terms, the Authority shall grant a period of up to a month to the Electronic Certificate Service Provider in order to remedy this incompleteness; during this period the Authority shall suspend the operations of electronic certificate service provider. At the end of the period, in the event that the incompleteness is not remedied, the operations of the electronic certificate service provider shall be terminated. An objection may be raised against such decisions of the Authority pursuant to the provisions in paragraph 2 of Article 19.

Should Electronic Certificate Service Providers fail to comply with the provisions mentioned in this article during their operations, the provisions of above paragraph shall be applied.

Electronic Certificate Service Providers shall comply with such lower and upper fee limits to be determined by the Authority.

Qualified Electronic Certificate

Article 9 – It is required that Qualified Electronic Certificates shall include the following;

a) an indication that the certificate is a "qualified electronic certificate",

b) the identity information of the Electronic Certificate Service Provider and the country in which it is established,

c) the identity information by which the Signature Owner can be identified,

d) Signature-Verification Data which correspond to Signature-Creation Data,

e) the date of the beginning and the end of the validity period of the certificate,

f) serial number of the certificate,

g) the information regarding the authorization of the certificate holder if the holder acts on behalf of another person,

h) when the certificate holder so requests, occupational and other personal information,

i) information related to conditions of the usage of the certificate and limits on the value of transactions, when applicable,

j) the Secure Electronic Signature of the electronic certificate service provider that verifies the information in the certificate.

Electronic Certificate Service Provider Liabilities

Article 10 – Electronic Certificate Service Providers shall be liable for;

a) Employing personnel qualified for the services provided,

b) Determining reliably, based on official documents, the identity of the person to whom a Qualified Electronic Certificate is issued,

c) Determining reliably, based on official documents, any information relating to the Qualified Electronic Certificate holder's authorization of acting on behalf of anyone, or any occupational or other personal information which is to be contained in the certificate,

d) Providing confidentiality of operation in cases where the Electronic Certificate Service Provider generates Signature Creation Data or the applicant generates it on the premises of the Electronic Certificate Service Provider or provide confidentiality of process when the signature creation data are generated by tools provided by the Electronic Certificate Service Provider,

e) Informing the applicant in writing, before delivering the certificate to them, that a qualified electronic signature has the same legal effect in transactions as a handwritten signature unless otherwise specified by laws, and about the limitations concerning the use of certificates and dispute resolution procedures,

f) Warning and informing the certificate holder in written form to not allow third parties to use Signature Creation Data associated with Signature Verification Data in the certificate,

g) Keeping all records regarding the services provided for the period determined in ordinance,

h) Informing the electronic certificate holder and the Authority at least 3 months prior to the termination of operations.

Electronic Certificate Service Providers shall not store or keep a copy of generated signature creation data.

Revocation of Qualified Electronic Certificates

Article 11 –Electronic Certificate Service Providers shall immediately revoke the qualified electronic certificates upon;

a) the request of the certificate holder,

b) the detection of any forgery or falsification of the information existing in the database or changes in such information,

c) the detection of the disability to act, bankruptcy or legally accepted disappearance or death of the certificate holder.

Electronic Certificate Service Providers shall create a record including the date and time when a certificate was revoked and which can be determined precisely and available by third parties in a secure and prompt way.

Electronic Certificate Service Providers shall immediately revoke all qualified certificates they have issued in the case of terminating their operations and in case the usage of certificates can not be available by any operating electronic certificate service provider.

In the event that the Authority terminates the operations of electronic certificate service provider, the Authority shall decide to transfer the qualified electronic certificates generated by the regarding electronic certificate service provider to another electronic certificate service provider and shall notify it to relevant parties.

Electronic Certificate Service Providers shall not retroactively revoke qualified electronic certificates.

Protection of Personal Data

Article 12 – Electronic Certificate Service Providers;

a) shall not request any information from the applicant except that necessary to issue an electronic certificate and shall not acquire such information without the consent of the applicant,

b) shall not keep the certificates available in public places where third parties may have access without the consent of the electronic certificate holder,

c) shall prevent third parties from obtaining the personal data without the written consent of the applicant. Electronic Certificate Service Providers shall not pass the related information to third parties and use such information for any other purposes without the consent of the certificate holder.

Legal Liability

Article 13- Liabilities of Electronic Certificate Service Providers towards certificate holders shall be subject to general provisions of Turkish law.

Electronic Certificate Service Providers shall be liable for compensation for damages suffered by third parties as a result of infringing the provisions of this Law or the ordinances

published in accordance with this Law. Liability of compensation shall not occur if the Electronic Certificate Service Provider proves the absence of negligence.

Electronic Certificate Service Providers shall be liable for damages arising from infringements made by their employees. Electronic Certificate Service Providers shall not be relieved of this liability by submitting any proof of evidence as described in Article 55 of the Turkish Code of Obligations.

Any requirements limiting or removing the liability of Electronic Certificate Service Provider against certificate holders and third parties are invalid, excluding the stated limitations of the usage and value of the Qualified Electronic Certificates.

Electronic Certificate Service Providers must take out "certificate financial liability insurance" in order to cover the damages incurred upon the failure in fulfilling the liabilities required by this Law. Principles and procedures of this Regulation are determined by the ordinance prepared by the Authority taking advice of the Undersecretary of the Treasury.

Certificate financial liability insurance foreseen in this article is provided by insurance companies authorized in this branch. These insurance companies shall be liable for providing certificate financial liability insurance. The insurance companies that infringe regarding liabilities may be fined up to eight billion TRL by the Undersecretary of the Treasury. The provisions of Article 18 address procedures for the collection of and appeals against this fine.

Electronic Certificate Service Providers shall be obliged to deliver electronic certificates to the signature owners after taking out certificate insurance.

Foreign Electronic Certificates

Article 14 –The legal effects of electronic certificates issued by any Electronic Certificate Service Provider established in a foreign country shall be recognized under international agreements.

In case that electronic certificates issued by any Electronic Certificate Service Provider established in a foreign country are recognized by an Electronic Certificate Service Provider established in Turkey, such electronic certificates are deemed to be Qualified Electronic Certificates. The Electronic Certificate Service Provider established in Turkey shall be liable for any damages arising from use of those electronic certificates.

SECTION THREE

Inspection and Penalty Provisions

Inspection

Article 15 – The inspection of Electronic Certificate Service Providers' operations and transactions regarding the implementation of this Law shall be fulfilled by the Authority.

The Authority, as it considers necessary, may inspect Electronic Certificate Service Providers. During inspection, Electronic Certificate Service Providers and relevant individuals shall present all notebooks, documents and records and provide samples, written and oral information to the Authority's inspectors, permit the inspectors to enter their premises and enable them to access their accounts and transactions.

Use of Signature Creation Data without Consent

Article 16 – A person who obtains, delivers, copies or recreates the signature creation device or data in order to create electronic signatures without the consent of the certificate holder shall be sentenced from 1 year to 3 years and fined a minimum of 500 million TRL (Turkish Lira).

In the case where crimes mentioned in the above paragraph are committed by the employees of an Electronic Certificate Service Provider, these penalties shall be scaled up by 50 percent.

Any damages arising from the crimes mentioned in this article shall be compensated separately.

Forgery in Electronic Certificates

Article 17 – A person who partly or fully generates electronic certificates, or falsify or copies electronic certificates generated as in valid, generates electronic certificates without authorisation or knowingly uses such electronic certificates shall be sentenced from 2 years to 5 years and fined a minimum of one billion TRL (Turkish Lira), even if their deeds become another crime.

If the crimes mentioned above are committed by the employees of an Electronic Certificate Service Provider, these penalties shall be scaled up by 50 percent.

Any damages arising from the crimes mentioned in this article shall be compensated separately.

Administrative Fines

Article 18 – Within this law:

a) An electronic certificate service provider who breaches Article 10 shall be fined 10 billion TRL,

b) An electronic certificate service provider who breaches Article 11 shall be fined 8 billion TRL,

c) A person who breaches Article 12 shall be fined 10 billion TRL,

d) An electronic certificate service provider who breaches the paragraph 5 and paragraph 7 of Article 13 shall be fined for 8 billion TRL,

e) An Electronic Certificate Service Provider who breaches Article 15 shall be fined 20 billion TRL

The administrative fines in this Law are determined by the Authority. Decisions about fines shall be notified to the persons concerned pursuant to The Notification Law number 7201. Any appeals against these decisions may be made to the competent administrative court within a period of 7 working days starting from the date of notification. An appeal shall not nullify the fulfilment of the decision. An appeal shall not nullify the fulfilment of the decision regarding the closure. An appeal, when it is not necessary, shall be concluded by making analysis over the documents as soon as possible. It is possible to apply to the Regional Administrative Court against the decisions that are taken regarding the appeal. The decisions of the Regional Administrative Court will be the final decree. The administrative fines imposed pursuant to this Law by the Authority shall be collected by the Ministry of Finance pursuant to the provisions of the Law about Procedures Collecting Public Receivables.

Repetition of Administrative Crimes and Closure

Article 19 – If any crimes described in Article 18 of this Law are repeated within a period of 3 years from the date of the first instance, administrative fines are doubled, and in should the same crime be committed for a third time, the Authority may decide to close Electronic Certificate Service Provider concerned.

Any decision regarding closure shall be notified to relevant individuals pursuant to Notification Law No. 7201. Any appeal against such a decision may be made to the competent administrative court within a period of 7 working days from the date of notification. An appeal shall not nullify the fulfilment of the decision. An appeal shall not nullify the fulfilment of the decision regarding the closure. An appeal, when it is not necessary, shall be concluded by making analysis over the documents as soon as possible. It may be applied to the Regional Administrative Court against the decisions that are taken regarding the objection. The decisions of the Regional Administrative Court will be the final decree.

SECTION FOUR

Miscellaneous Provisions

Ordinance

Article 20 – The procedures and the rules pertaining to the implementation of the Articles 6, 7, 8, 10, 11 and 14 of this Law shall be described in the ordinances to be published by the Authority within the period of six months from the execution date of this Law with the collaboration of all interested parties.

Exemptions about Public Entities and Establishments

Article 21 – The public entities and establishments providing certification services are exempted from the forth and the fifth paragraphs of Article 8, 15 and 19 of this Law.

Article 22 - The following sentence has been added to the first paragraph of Article 14 of the Turkish Code of Obligations dated 22.04.1926 No. 818:

“Secure electronic signature has the same effect as a handwritten signature”

Article 23 - The following 295/A article has been added to Article 295 of the Turkish Code of Civil Procedure dated 19.6.1927 No. 1086:

“Article 295/A – Electronic data that are generated with secure electronic signatures in accordance with procedures are equivalent to bill. These data are accepted positive evidence until the contrary is proved.

Should any party deny the data generated by secure electronic signatures and alleged against him, Article 308 of this Law shall be imposed through comparison.”

Article 24 - The following Subclause (m) has been added to the first paragraph of Article 7 of the Turkish Radio Law dated 5.4.1983 No.2813 and therefore existing subclause (m) of the current Law has been succeeded as subclause (n):

“m) undertaking the duties assigned by the Electronic Signatures Law”

Entry into Force

Article 25 – This Law shall enter into force six months after the date of its publication.

Execution

Article 26 - The provisions of this Law are executed by the Council of Ministers.