ELECTRONIC SIGNATURE LAW

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.

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 electronical, optical or similar methods,

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

c) Signature Owner: 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 signature owners and being used by 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: The record that is confirmed by certification service provider with electronic siganture for the purpose of verification of the exact time for 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- Secure Electronic Signature shall be signature that;

a) is exclusively assigned to the owner of signature,

b) is generated with the secure electronic signature creation device which is kept under sole control of the signature owner,

c) enables the identification of the signature owner based on the qualified electronic certificate,

d) enables to detect whether signed electronic data is altered or not subsequently.

Legal Effect and Area of Application of Secure Electronic Signature

Article 5- Secure electronic signature shall have the same legal effect with that of handwritten signature.

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 their secrecy is assured,

c) Electronic signature creation data recorded in those devices can not be obtained or used by third parties and electronic signatures are protected against forgery,

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

Secure Electronic Signature Verification Device

Article 7- Secure electronic signature verification devices are signature verification devices which;

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

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

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

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

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

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 – Electronic certificate service providers shall be public entities and establisments and natural persons or private law legal entities that provide electronic certificates, time-stamping and other services related to 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 infringment of any of the above terms, the Authority shall grant a period utmost for a month to the electronic certificate service provider in order to straighten out this incompleteness; during this period the Authority shall cease the operations of electronic certificate service provider. At the end of the period, in the event that incompleteness is not straightened out, the operations of the electronic certificate service providershall be terminated. Any objection may be raised against those decisions of the Authority pursuant to the provisions in paragraph 2 of Article 19.

In case 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 too.

Electronic certificate service providers shall comply with the lower and upper limits for fees to be determined by the Authority.

Qualified Electronic Certificate

Article 9 – It is required that qualified electronic certificates shall include the followings;

a) an indication that the certificate is “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 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 certificate holder if the holder acts on behalf of another person,

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

i) information related to conditions of the usage of 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 provider 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 qualified electronic certificate is issued,

c) Determining reliably, based on official documents too, the information in case qualified electronic certificate holder's authorization of acting on behalf of anyone, occupational or other personal information is to be contained in the certificate,

d) Providing confidentiality of operation in cases the electronic certificate service provider generates signature creation data or applicant generates it in premises of electronic certificate service provider or provide confidentiality of process in case the signature creation data is generated by tools provided by electronic certificate service provider,

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

f) Warning and informing the certificate holder in written form not allowing 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 provider shall not keep a copy of generated signature creation data or store it.

Revocation of Qualified Electronic Certificates

Article 11 – Electronic certificate service provider shall immediately revoke the qualified electronic certificates upon;

a) the request of certificate holder,

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

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

Electronic certificate service provider shall ensure to create a record including the date and time when a certificate revoked can be determined precisely and available by third parties in a secure and prompt way. In the event that qualified electronic certificates can not be

transfered before the date of terminating operations or the usage of certificates can not be available by any operating electronic certificate service provider.

Electronic certificate service provider shall immediately revoke the qualified certificates in case of terminating its 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 provider shall not revoke qualified electronic certificate retroactively.

Protection of Personal Data

Article 12 – Electronic certificate service provider;

a) shall not request any information from the applicant except for necessary information to issue an electronic certificate and shall not get 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 the third parties to obtain the personal data without the written consent of the applicant. electronic certificate service provider shall not pass the related information to the third parties and use them for any other purposes without the consent of the certificate holder.

Legal Liability

Article 13- Liability of electronic certificate service provider for certificate holders shall be subject to the general provisions.

Electronic certificate service provider 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 electronic certificate service provider proves the absence of negligence.

Electronic certificate service provider shall be liable for such damages arising from infringements made by the employees of electronic certificate service provider too. Electronic certificate service provider shall not redeem from this liability by submitting any proof of evidence as described in Article 55 of Turkish Code of Obligations.

All types of requirements limiting or removing the liability of electronic certificate service provider against certificate holders and third parties are invalid excluding the limitations of the usage and value of the qualified electronic certificates.

Electronic certificate service provider 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 Undersecretariat of 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 are fined for eight billion TRL by Undersecretariat of Treasury. The provisions of Article 18 are implemented in procedures of collection and objection of this fine.

Electronic certificate service provider shall be obliged to deliver electronic certificate to signature owner by taking out its 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 also be liable for the damages arised from using those electronic certificates.

SECTION THREE
Supervision and Penalty Provisions

Supervision

Article 15 – The supervision of electronic certificate service provider's operations and transactions regarding the implementation of this Law shall be fulfilled by the Authority.

The Authority, when considers as necessary, may supervise electronic certificate service providers. During supervision, electronic certificate service providers and relevant individuals shall present all notebooks, documents and records and provide samples, written and oral information to supervisors, permit the supervisors to enter their premises and enable them to supervise the accounts and transactions.

Use of Signature Creation Data Without Consent

Article 16 – A person who obtains, delivers, copies and 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 heavily fined for not less than 500 million TRL(Turkish Lira).

In case the crimes mentioned above paragraph are committed by the employees of 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 seperately.

Forgery in Electronic Certificates

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

If the crimes mentioned above paragraph are committed by the employees of 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 seperately.

Administrative Fines

Article 18 –

a) An electronic certificate service provider who breaches the Article 10 of this Law shall be fined for 10 billion TRL,

b) An electronic certificate service provider who breaches the Article 11 of this Law shall be fined for 8 billion TRL,

c) A person who breaches the Article 12 of this Law shall be fined for 10 billion TRL,

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

e) An electronic certificate service provider who breaches the Art.15 of this Law shall be fined for 20 billion TRL

The administrative fines in this Law are determined by the Authority. The decisions about the fines shall be notified to persons concerned pursuant to The Notification Law numbered 7201. The objections to these decisions may be made to the competent administrative court within a period of 7 working days starting from the date of notification. The objections shall not cease the fulfilment of the decision. The objections shall not cease the fulfilment of the decision regarding the closure. The objections, when it is not necessary, shall be concluded by making analysis over the documents as soon as possible. It may be applied to Regional Administrative Court against the decisions that are taken regarding the objection. The decisions of Regional Administrative Court are 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 – In case, the crimes described in Article 18 of this Law are repeated second time within a period of 3 years starting from the date of that crime committed for the first time, administrative fines are doubled, in case, the same crimes are commited for a third time, the Authority shall decide to the closure of electronic certificate service provider.

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

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 conclusiveness with 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.

In case any party denies the data generated by secure electronic signatures and alleged against himself, 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.