

Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law

(Published in the Official Gazette ref 25692, 2005-01-06)

PART ONE

General Provisions

Purpose

Article 1- The purpose of this Ordinance is to define the procedures and principles for the legal, technical aspects and implementation of electronic signatures.

Scope

Article 2- covers procedures and principles regarding notification and certification processes, secure electronic signature creation and verification data and devices, obligations of electronic certificate service providers, the Authority and third parties, inspection, termination of operations, time-stamps, foreign electronic certificates, security, technical and financial aspects.

Legal Basis

Article 3- This Ordinance is prepared on the basis of Electronic Signature Law No.5070 of 15 January 2004.

Definitions

Article 4 - The definitions and abbreviations used in this Ordinance have the following meanings;

Law: Electronic Signature Law No.5070 of 15 January 2004,

Board: Telecommunications Board,

Authority: Telecommunications Authority,

ECSP: Electronic Certificate Service Provider,

Archive: Documents and electronic data described in paragraph 2 of Article 14 of this Ordinance and which shall be kept by ECSP,

Notification Requirements: Requirements described in paragraph 2 of Article 8 of the Law,

Inspection: All actions in order to detect potential faults, imperfections, unlawfulness and/or abuses and to apply sanctions prescribed in related legislation, by assessment of compliance of electronic certificate service provider's activities and operations with related legislation,

Directory: Repository in which valid certificates are kept,

Activation Data: Data like biometrical value, password used for activation of secure electronic signature creation devices.

Assessment: All actions for determination of whether notification submitted to the Authority satisfies all requirements or not,

Revocation Status Record: Record that includes the revocation information data of certificates which are not expired, ensures to determine revocation time precisely and can be easily accessed by third parties secure and promptly,

Organisational Application: Application of qualified electronic certificate which is submitted by a legal person on behalf of its employees or customers or members or shareholders,

Qualified Electronic Certificate: Electronic certificate which satisfies the requirements laid down in Article 9 of the Law,

Hash Algorithm: Algorithm that is used to produce a fixed-length hash value of the data to be signed,

Fingerprint: Hash value calculated over certificate,

Certificate Policy: Document containing general rules regarding operations of ECSP,

Certification Practice Statement: Document describing implementation of the issues laid down in the certificate policy in detail,

Certificate Financial Liability Insurance: Insurance that ECSP shall take out to compensate any damages arising from infringement of the obligations laid down in the Law,

Time-stamp Policy: Document containing general rules regarding time-stamp and time-stamping services,

Time-stamp Practice Statement: Document describing implementation of the issues laid down in the time-stamp policy in detail,

For the terms not defined in this Ordinance, the definitions in the Law shall apply.

Principles

Article 5- The following basic principles shall be observed in enforcement of this Ordinance;

a) Unless objective reasons require the opposite, qualitative and quantitative continuity, reliability, non-discrimination, orderliness, efficiency, openness, transparency and effective use of resources,

b) Protecting consumer rights,

c) Assuring quality of service,

d) Setting effective and sustainable competition environment and encouraging applications for its continuity,

e) Considering international standards,

f) Encouraging new investments and implementations to make wide use of electronic signature,

g) Avoiding the possibility that the electronic certificate holders are forced to buy services or products they do not demand,

h) Avoiding the possibility of financing the cost of a service or a product by the price of another service or a product.

PART TWO

Notification Process

Notification

Article 6 – The public entities and establishments or natural persons or private law legal entities, who request to be an ECSP, shall notify to the Authority all the information and documents listed in Annex-1. ECSP shall indicate compliance of its notification with the requirements in detail.

Assessment and Results of the Notification

Article 7 – The Authority shall assess the notification promptly and complete it within two months. ECSP, that satisfies the notification requirements, shall commence its operations after a period of two months from the date of notification.

In case the Authority determines the incompleteness or infringement of any of the notification requirement, the Authority shall grant a period utmost for a month to the ECSP in order to remedy this incompleteness. ECSP shall not go into operation until the end of this period. ECSP shall submit the documents proving that it has remedied the incompleteness in the notification requirements within the period granted by the Authority. ECSP who has met those requirements, as determined by the Authority, shall commence its operations in case the period of two months has ended from the date of notification. The Authority shall determine that ECSP has lost its status of being ECSP in case the ECSP has not remedied the incompleteness in the notification requirements until the end of period given.

Changes in the Notification

Article 8 – After commencing its operations, in case of any change in the notification, ECSP shall inform the Authority about those changes within a period of seven days.

PART THREE

Certificate Management Life

Registration

Article 9 - ECSP shall determine the identity of person, to whom the qualified electronic certificate is to be issued, based on valid and official documents with a photograph such as national identity card, passport and driving license. The person to whom qualified electronic certificate is to be issued shall be physically present during the identity check.

ECSP may dispense with the requirement of being physically present for identification provided that the identity of the person to whom the qualified electronic certificate is to be issued has been determined previously pursuant to the provisions of the first paragraph or when the application is an organisational application. Organisational applicant shall provide the qualified electronic certificate requests of the persons on behalf of whom it applies for in a written form. ECSP shall be liable as regards the accuracy and reliability of identification of the person who qualified electronic certificate is to be issued to during qualified electronic certificate application process.

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, ECSP shall determine those information based on official documents in an accurate, complete and reliable manner. ECSP shall not request any information from the person whom qualified electronic certificate is to be issued to except for those necessary to issue an electronic certificate, and shall not give those to the third parties and shall not use for any other purposes without the consent of the qualified electronic certificate holder.

Qualified Electronic Certificate Generation

Article 10 – After qualified certificate application ECSP shall generate the certificate and deliver the certificate to the certificate holder. The validity period of qualified electronic certificate shall be determined by contract or undertakings.

Qualified Electronic Certificate Dissemination

Article 11 – ECSP shall publish the qualified electronic certificate in a public directory in case for which the certificate holder's consent has been obtained. ECSP shall ensure that directory service is provided without any interruption.

Qualified Electronic Certificate Renewal

Article 12 – Qualified electronic certificate may be renewed by ECSP before expiry of the validity period of the certificate upon a request from certificate holder or from Organisational applicant provided that it has obtained the certificate holder's consent. ECSP shall renew the qualified electronic certificate as it has verified that the information of the certificate owner was still valid.

Qualified Electronic Certificate Revocation

Article 13 –Requests with regard to revocation of qualified electronic certificates shall be submitted by ECSP, certificate holder and persons specified in the contract. ECSP shall ensure that the requests relating to this status can be made at least by telephone and without interruption. ECSP shall inform the qualified electronic certificate holder of the mentioned status. In case of Organisational applications, applicant shall be informed too.

Upon receiving revocation request, the qualified electronic certificate shall be revoked immediately. Revoked qualified electronic certificate shall be included in the revocation status records until it expires. ECSP shall continuously make revocation status records relating to qualified electronic certificates available to public access as free of charge without any need for identification. The next update time of the records shall be displayed clearly in those records. ECSP shall not revoke qualified electronic certificates retroactively.

After such cases that certificate policies change or ECSP's signature generation data is stolen, lost or compromised where certificate holder has no fault renewal activities shall not be charged upon qualified electronic certificate revocation and renewal.

PART FOUR **Obligations**

ECSP Obligations

Article 14 – ECSP shall inform the person to whom qualified electronic certificate is to be issued in written form at least on the following subjects;

- a) Secure electronic signature shall have the same legal effect with that of handwritten signature, without prejudice to the limitations described in the Law,
- b) Not to allow third parties to use signature creation data and device,
- c) Scope of limitations and procedures regarding usage of qualified electronic certificates, d) Revocation status of qualified electronic certificate,
- e) Alternative dispute resolution procedures in case of dispute between ECSP and qualified electronic certificate holder,
- f) Amendments in the provisions and terms of the contract or undertakings.

ECSP shall keep the followings for at least twenty years:

- a) Expired qualified electronic certificates,
- b) Documents, information and electronic data requested in qualified electronic certificate application, c) Certificate policies and certification practice statement,
- d) Time-stamp policy and time-stamp practice statement,
- e) Its own certificate from the date of expiration,
- f) Logs including events regarding qualified electronic certificate life cycle management, information of the operator(s) with date and time.

ECSP shall be liable for;

- a) Publishing the parts of the certification practice statement concerning certificate holder or third parties and its certificate policy in its web site,
- b) Submitting tariffs for services regarding qualified electronic certificate, time-stamping and electronic signature to the Authority within fifteen days after applying them,
- c) Taking out certificate financial liability insurance,
- d) Ensuring the signature creation device is secure signature creation device in case ECSP provides it to qualified electronic signature owner.

Qualified Electronic Certificate Holder Obligations

Article 15 – Qualified electronic certificate holder is liable for;

- a) Submitting information accurately and completely to the ECSP that's necessary to get qualified electronic certificate,
- b) Informing the ECSP immediately in case of any change in the information submitted to ECSP,

c) Using algorithms and parameters determined by Communiqué on Processes and Technical Criteria Regarding Electronic Signatures, in case the certificate holder generates his/her own signature creation data,

d) Using the signature creation and verification data only for creating and verifying electronic signature and in accordance within the limitations about the usage and value of the qualified electronic certificate,

e) Not allowing third parties to use his/her signature creation data and taking necessary cautions for this purpose,

f) Notifying the ECSP immediately in case the confidentiality or security of the signature creation data is under suspicion,

g) Using secure electronic signature creation device,

h) Assuring the necessary cautions in case the signature creation and verification data are generated out of the premises of ECSP and with devices that do not belong to the ECSP,

i) Informing the ECSP immediately in case the signature creation device or the activation data of the signature creation device is stolen, lost or suspected to be compromised.

Third Parties Obligations

Article 16 – Third parties are liable for;

a) Verifying if the certificate is qualified electronic certificate or not,

b) Verifying the validity and revocation status of the qualified electronic certificate or using secure electronic signature verification device,

c) Verifying if there is any limitation on the usage of the qualified electronic certificate.

The Authority Obligations

Article 17 – The Authority shall publish the information regarding ECPS's notification process and operation status in its web site.

The Authority shall prepare annual report regarding its activities related to electronic signature and status of the electronic signature sector and shall publish that report for this purpose in its web site.

PART FIVE

Technical Issues and Security

Signature Creation and Verification Data

Article 18 – ECSP shall generate its own certificate, signature creation and verification data within the boundaries of the Republic of Turkey and shall not take signature creation data out those boundaries in any means.

The validity period of ECSP's signature creation and verification data shall not exceed ten years.

ECSP, within seven days after commencing operations, shall publish the fingerprint of its own certificate and hash algorithm in its web site, announce to the public by giving out a notice in three nationwide published newspapers of highest circulation and submit each copy of them to the Authority.

Security Criteria

Article 19 – If the ECSP is a private law legal entity, its cofounders and its authorized representative managers and staff employed or employees of its subcontractor(s); if ECSP is a natural person, himself, its authorized representative managers and employees of its subcontractor(s), except the crimes committed by imprudence and indemnified or not indemnified, even if they are granted with an amnesty, shall not be imprisoned for penal servitude or imprisoned for over than six months or shall not be guilty of defamatory offences like simple or qualified debit, malversation, bribery, theft, deceit, forgery, abuse of trust, fraudulent bankruptcy and the crimes of smuggling, excluding the smuggling of employing and consumption, sedition on official public procurement and tenders, money laundering or disclosing the secrets of the government, taking part in tax fraud or participating in tax fraud or cyber crimes in informatics.

ECSP shall employ or subcontract satisfactory number of technical staff in the fields of the information security, electronic signature technologies and database management. Technical staff shall possess enough expertise in their fields or be educated in the above mentioned fields. ECSP shall specify the task definitions and task distributions of its own employees or employees of the subcontractor(s) in organization chart.

ECSP shall use secure systems and equipment and ensure that the buildings or the area where those systems and equipment are installed are protected.

PART SIX

Financial Issues

Fees of Qualified Electronic Certificate, Time-stamp and Related Services

Article 20 – The principles and procedures regarding the upper and lower limits of the fees of qualified electronic certificate, time-stamp and related services which ECSP has to obey shall be determined by the Authority.

Administrative Fee

Article 21 – The Authority shall collect administrative fee from ECSP up to % 0,4 of its net sales of the previous calendar year. All of this fee shall be paid to the Authority until the last working day of April.

PART SEVEN

Principles and Procedures of Inspection

Inspection

Article 22 – ECSP shall be inspected by the Authority when it is necessary and at least biannual at the Authority’s own initiative.

Principles to be Obeyed During Inspection

Article 23 – The Authority shall observe the following principles during the inspection;

- a) Being neutral during assessment of results and preparation of inspection report,
- b) Not allowing any intervention that may affect honesty and neutrality,
- c) Taking necessary pains over all phases of inspection.

Powers of Inspectors

Article 24 – The Authority’s inspectors shall be authorized;

- a) To request and assess all notebooks, documents and records considered as necessary and take original copies and/or samples of these,
- b) To enter into administrative offices and premises and investigate these places,
- c) To request relevant written and/or oral information and keep necessary minutes,
- d) To inspect all accounts and operations.

Obligations of Inspectors

Article 25 – The Authority’s inspectors shall be liable for;

- a) Introducing themselves by showing the document indicating that they are authorized to inspect before starting inspection,
- b) Keeping notebooks, documents and records that are entrusted by relevant individuals to themselves as in original form and give them back at the end of the work,
- c) Not revealing confidential information that is obtained during the inspection to anyone except legally authorized individuals and make use of this information for their benefits directly or indirectly,
- d) Not making any annotation, addition or correction on the notebooks, documents and records except the ones that is necessitated by inspection,
- e) Not intervening administrative and management deeds where the inspection is performed.

Inspection Obligations of ECSP

Article 26 – ECSP shall be liable for meeting inspectors’ requests as soon as possible that are within the framework of their authorization and provide a convenient working place to inspectors.

ECSP shall not refrain from its obligations regarding inspection by alleging reasons like privacy and secrecy.

Submission of Reports

Article 27 –The inspection report prepared by inspectors shall be submitted to the Board within a period of thirty days from the end of inspection.

In case of determination of important points that may affect the activities and operations of ECSP negatively during the inspection, the inspectors shall prepare a report including these issues and submit it to the Board immediately.

Board Decision

Article 28 – Inspection report and the report mentioned in the paragraph 2 of Article 27 shall be put on the agenda preferentially by the Board. The Board shall make a decision by assessing the reports. In case of determination of contradictions to provisions of relevant legislation in the reports and approval of this determination by the Board, it shall be decided to apply the sanctions and penalties described in relevant legislation.

PART EIGHT

Termination of Operations

Termination of Operations by the Authority

Article 29 – In case the Authority determines that ECSP has not complied with one or more notification terms during its operations, as a result of inspection, the Authority shall grant a period to ECSP up to one month in order to straighten out this incompleteness and the Authority shall cease ECSP's operations within this period. The Authority shall cease ECSP's operations in cases ECSP does not straighten out the incompleteness within the period or commits the crimes described in Article 18 of the Law for a third time within a period of three years retroactively starting from the date of that crime for the first time.

An ECSP whose operations are terminated because of any termination cases described in the first paragraph, may agree with any operating ECSP upon transferring the qualified electronic certificates within a period of fifteen days from the notification date of termination decision. In case an agreement is made between the parties, the Authority shall decide to transfer the qualified electronic certificates generated by ECSP whose operations are terminated by the Authority to ECSP agreed. In case no agreement is reached between the parties upon taking over the qualified electronic certificates within a period of fifteen days, the Authority shall decide to transfer the certificates to any ECSP at its own initiative. ECSP who takes over the qualified electronic certificates shall commence the certificate renewal procedures and complete these procedures within a period of one month from the notification date of the transfer decision. The Authority may extend this period utmost for a month if necessary.

ECSP shall not provide the services relating to the electronic certificate, time-stamp and electronic signatures from the notification date of the termination decision. However, ECSP shall continue to provide the service of revocation status record until certificate renewal procedures are completed.

ECSP, whose operations are terminated by the Authority, shall transfer the documents used in identity verification, the directory, the archive and, after certificate renewal procedures are

completed, revocation status record to ECSP which has taken over the qualified electronic certificates and then shall destroy its own signature creation data and its backups.

In the event that any ECSP is not found to transfer the qualified electronic certificates, the Authority shall decide to revoke the qualified electronic certificates generated by ECSP whose operations are terminated by the Authority. That ECSP shall destroy its own signature creation data and its backups after generating the last revocation status record, shall continue to provide the service of revocation status record until the end of validity period of qualified electronic certificate which expires latest and keep the archive at least for a period of twenty years.

The Authority shall publish the decisions regarding transferring the qualified electronic certificates in its web site. ECSP, whose operations are terminated by the Authority, shall announce the related decisions to certificate holders with e-mail and publish them in its web site.

Termination of Operations by ECSP

Article 30 – ECSP shall inform the Authority in written form at least 3 months before terminating its operations. ECSP shall not accept any qualified electronic certificate application from the notification date of related decision and shall not generate a new certificate.

ECSP shall publish its decision in its web site at least three months before terminating its operations, announce it to certificate holders with e-mail and give out a notice in three nationwide published newspapers of highest circulation.

ECSP may transfer the qualified electronic certificates which do not expire till the date of termination to any ECSP operating that can provide usage of those certificates within period of one month prior to the date of terminating operations. ECSP, who terminates its operations, shall announce transfer of the certificates to certificate holders with e-mail. In case of transferring the qualified electronic certificates, ECSP who takes over the certificates shall commence the certificate renewal procedures and complete these procedures within a period of one month. The Authority may extend this period utmost for a month if necessary.

ECSP who transfers the certificates shall transfer the documents used in identification, the directory, the archive and, after certificate renewal procedures, revocation status record to ECSP who has taken over the qualified electronic certificates and then shall destroy its own signature creation data and its backups.

In the event that qualified electronic certificates can not be transferred one month prior to the date of terminating operations or the usage of certificates can not be provided by any operating ECSP, ECSP who wants to terminate its operations shall revoke the certificates on the date of termination of operations. ECSP who terminates its operations, shall destroy its own signature creation data and its backups after generating the last revocation status record, continue to provide the service of revocation status record until the end of validity period of qualified electronic certificate which expires latest and keep the archive for a period of twenty years.

PART NINE

Other Provisions

Time-stamp and Time-stamping Services

Article 31- ECSP is obliged to provide time-stamp and its services. Qualified electronic certificate holder can get this service if he/she requests.

Recognition of Foreign Electronic Certificates

Article 32 – The terms regarding the legal effects and recognition of foreign electronic certificates shall be determined under international agreements.

In case that there is no international agreement, in order for electronic certificates issued by an ECSP established in a foreign country to be recognized by an ECSP established within Turkey, the following are required at least;

a) Foreign electronic certificate shall bear the technical criteria of qualified electronic certificate stated in the Law and in this Ordinance.

b) Foreign ECSP shall operate as ECSP in the country it has been established.

An ECSP established in Turkey shall submit the following documents on foreign electronic certificate to be recognized to the Authority within one month before certificates are started to be used;

a) A sample of foreign ESCP's certificate to be recognized,

b) An official document issued by the authorised authority proving that foreign ESCP is an ESCP in the country it has been established,

c) Information and documents indicating that foreign electronic certificate meets the technical criteria of qualified electronic certificate described in the Law and this Ordinance.

The Authority shall publish the information of foreign ESCP in its web site.

The ECSP established in Turkey, who recognized the certificates, shall also be liable for all the damages arising from usage of those recognized foreign electronic certificates.

Activity Report

Article 33 – ECSP shall submit to the Authority the activity report of the previous year until the end of March every year. The report shall cover at least the followings;

a) Types and numbers of certificates generated,

b) Number of certificates revoked for every type of certificates

c) Information and documents indicating the previous year's financial status of ECSP,

d) If applicable, information on certificates transferred to itself,

e) ECSP's market foresights on the next year,

f) Other information and documents to be requested by the Authority.

Communiqué on Technical Issues

Article 34 – Technical criteria to be obeyed regarding ECSP operations including application for qualified electronic certificate generation, dissemination, renewal, revocation of certificate and archiving process, signature creation and verification data, certificate policy and certification practice statement, secure signature creation and verification devices, system, device and physical security used in the operations of ESCP, ESCP's staff, time-stamp and its services shall be determined by the Communiqué. The Authority shall update the Communiqué if required.

Issues not covered in this Ordinance

Article 35 - Any other issues not covered in this Ordinance about electronic signature shall be regulated by decisions of the Board.

Temporary Provisions

Temporary Article – Until the upper and lower limits of qualified electronic certificate, time-stamp and related services' fees are determined by the Authority, ECSP may determine the fees relating to qualified electronic certificate, time-stamp and related services with respect to the principles pursuant to the Article 5.

Entry into Force

Article 36 – This Ordinance and any revisions thereto, shall enter into force on the date of its publication.

Execution

Article 37 – The provisions of this Ordinance are executed by the Chairman of the Board.

ANNEX-1

Information and Documents Requested for Notification

The public entities and establishments or individuals and private law legal entities who apply to serve as an ECSP shall submit the information and documents listed below to the Authority with their notification.

1) Contact Details: Name/title and contact details (address, telephone, fax, e-mail address, internet address) of all units,

2) Documents About Company: If it is a commercial corporation, Trade Record Journal of the company, documents about taxation, signature circular of the company, trade record document and legal records and contact details of the people authorized with representation of company,

3) Personnel: Organization chart, the document taken from social security foundation which indicates that all the employees are ECSP's personnel, the legal records of the employees or employees of the subcontractor(s), resumes of technical personnel and documents that prove expertise of them,

4) Certificate Policy and Certification Practice Statement

5) Time-stamp Policy and Time-stamp Practice Statement;

6) Sample of ECSP's Own Certificate;

7) Certificate Financial Liability Insurance: A copy of policy document proving adequate financial liability insurance;

8) Copy of Certificate Holder Agreement or Undertakings: A copy of undertakings or the agreement which is to be concluded with qualified electronic certificate holders,

9) Service Agreement: A copy of the agreement made with subcontractor, if applicable,

10) Information and Documentation required by the Communiqué