NB: This is an unofficial translation!

Act on Electronic Service in the Administration (1318/1999)

Chapter 1
General provisions

Section 1 Objective

(1) The objective of this Act is to improve the smoothness and rapidity of the service in the administration, as well as data security, by promoting the use of electronic data interchange.

(2) The Act contains provisions on the rights, duties and responsibilities of the administrative authorities and their customers in the context of electronic service.

(3) In addition, this Act contains provisions on the most significant requirements in the electronic identification of persons.

Section 2 Scope of application

(1) This Act applies to the electronic lodging of an administrative matter with an authority, to its handling and to the service of notice of the decision (electronic service). This Act applies to electronic service also when an administrative matter is being handled by someone else than a public authority. The Act does not apply to administrative judicial procedure, criminal investigations, police inquiries or enforcement.

(2) Separate provisions apply to electronic service in the Evangelical Lutheran Church of Finland.

(3) Unless otherwise provided in this Act, the provisions in other legislation on the lodging of an administrative matter, the service of notice on the decision, the openness of the activities of the authorities, the processing of personal data, the archiving of documents, the language to be used in the matter, and the handling of the matter by the authorities apply also to electronic service.

Section 3 Definitions

For the purposes of this Act:
(1) *electronic data* interchange means telefaxes and teleservice, such as electronic forms or e-mail, and other methods based on electronics, where data is being transferred either wirelessly or via a cable as electromagnetic waves;
(2) *electronic message* means information sent by way of electronic data interchange and easily stored as a written document;
(3) *electronic document* means an electronic message which has an effect on the lodging or handling of a matter or on the service of a decision;
(4) *certificate* means a set of data that confirms the identity of the person in possession of the certificate and the integrity and originality of his/her electronic signature;
(5) *certifier* means a reliable third party who defines and issues certificates;
(6) *electronic signature* means a set of data that confirms the integrity and originality of an electronic message by a method that is open to public inspection;
(7) *public key* means a public set of data that is used in the confirmation of the identity of the person in possession of a certificate and the integrity and originality of an electronic signature.

Chapter 2
Provisions on certifiers' operations

Section 4 Requirements for certifiers

(1) The operations of a certifier shall be based on generally accepted defined methods and best data administration practices.

(2) The certifier shall have the technical, professional and financial resources that can be considered adequate in view of the extent of its operations.

Section 5
Requirements for certificates

(1) A certificate shall contain

(1) the name of the person in possession of the certificate and the other data, albeit not a personal identity code, necessary for the unequivocal identification of that person;
(2) the data identifying the certifier;
(3) the period of validity of the certificate;
(4) the identity code of the certificate;
(5) the electronic signature of the certifier; and
(6) the data on the possible restrictions of the use of the certificate.

(2) The certificate shall be based on adequately strong encryption and on definitions that are open to public inspection. In addition, the certificate shall be based on public key technology or on another method with at least the same standard of security.

Section 6 Access to and contents of the operating principles

The certifier shall keep the documentation on the operating principles applied in the certificate and certification freely available to the public. The documentation shall also contain the data on the technology used in the electronic signature of the certifier and, if public key technology is being used, on the algorithm applied therein.

Section 7 Procedure in the operations of the certifier

(1) The provisions in the following legislation apply to the issuance and maintenance of certificates and the use of the directories relating to them: the Administrative Procedure Act (598/1982), the Languages Act (148/1922), the Act on the Use of the Samí Language before the Authorities (516/1991), the Act on the Openness of Government Activities (621/1999), the Personal Data Act (523/1999) and the Archives Act (831/1994).

(2) A certificate issued to an employee of the certifier and meeting the requirements in this Act may be used when the certifier is deciding a matter under this Act, as well as in the certifier's other own service. In this event, the certificate need not be issued by a third party.

Section 8 Duty of a person requesting a certificate to supply information

A person requesting a certificate shall supply the certifier with his/her name, address and personal identity code for purposes of reliable and unequivocal identification and for the maintenance of contact.

Section 9 The certifier's access to information

(1) The certifier has the right, on the consent of the person requesting a certificate, to obtain and to check the information referred to in section 8 in the Population Register.

(2) The information shall be delivered from the Population Register as a public-law performance, as referred to in the Act on the Charge Criteria of the State (150/1992).

Section 10 Certificate directories

(1) The certifier shall maintain an appropriate and up-to-date directory of the certificates and the public keys in use, so as to allow for the verification of the validity of certificates and the originality of electronic signatures.

(2) The data referred to in section 5(1) and section 8, and the data on the public keys in use, the validity of the certificate and the revocation of the certificate shall be entered into the directory. The data shall be entered into the directory without delay.

(3) A certificate shall upon the request of the person in possession be immediately revoked. No reasons need be supplied for the request.

Section 11 Delivery of data in a certificate directory

(1) For purposes of verifying the validity of a certificate and the originality of an electronic signature, everyone shall have access to a certificate directory, for data referred to in section 5(1), as well as data on the public keys in use, the validity of the certificate and the revocation of the certificate.

(2) The data not referred to in paragraph (1) shall be delivered from the certificate directory in accordance with the provisions on the delivery of data in the Personal Data Act and the Act on the Openness of Government Activities. When requesting such access, reasons for the request shall be supplied. The data thus delivered shall not be used for purposes not mentioned at the time of the request.

Section 12 Archiving of the data in a certificate directory

(1) The data in a certificate directory shall be retained permanently.

(2) The provisions in section 14 of the Archives Act on the archiving of permanently retained documents apply to a certifier. The provision applies also to the transfer of the certificate directory to an archive at the end of the certifier's operations.

Section 13 Verification of the validity of certificates

The certifier shall not record the verifications of the validity of certificates.

Section 14 Procedure in personal identification

(1) A certificate shall be fetched in person. At this time, the certifier shall verify the identity of the person from current domestic identification documents issued by the police. However, a driver's license issued before 1 October 1990 cannot be accepted as an identification document. In addition, the information shall be double-checked from the Population Register.

(2) If the person does not have documents referred to in paragraph (1) of if there otherwise is a special reason to verify the identification, the identity of the person shall be verified from a specific and current document issued by the police and vouching that the person has been identified.

Section 15 Certifier's liability in damages

(1) The certifier shall be liable in damages for any loss arising from data having been erroneous when it was entered into a certificate or the certificate directory, or from a certificate not having been revoked even though a request or notification for this effect has been received.

(2) However, the certifier shall not be liable for such loss, if it can show that the loss has not arisen from the negligence of the certifier.

(3) If the loss has arisen from the activity of a person employed in the certification operations or in a part of such operations, the certifier shall be released from liability only if also the said person would be released from liability under paragraph (2).

Section 16 Effect of a restriction in the use of a certificate on the obligations of the certifier

The provisions in this Act do not apply to a certifier whose certificates, owing to a restriction in their use, cannot be used in electronic service in the administration.

Section 17 Assignment of a certifier's duties to another person

A certifier may contractually assign a certifier's duty to another person. The provisions in this chapter on the certifier apply correspondingly to the assignee.

Chapter 3
Duties of the authorities

Section 18 Availability of electronic service

(1) An authority in possession of the requisite technical, financial and other resources shall offer to the public the option to send a message to a designated electronic address or other designated device so as to lodge a matter or to have it handled. Furthermore, the authority shall offer to the public the option to deliver electronically the statutory or ordered notifications, the requested accounts and the other comparable documents and messages.

(2) The authority may offer the services referred to in paragraph (1) also on a function-by-function or office-by-office basis.

(3) The authorities shall strive to use equipment and software that is technically as compliant and as user-friendly as possible to the customers of the administration. In addition, the authorities shall ensure an adequate level of data security both in their service and in inter-authority communications.

Section 19 Accessibility of the authorities

The authorities shall see to it that their electronic data interchange equipment is in working order and that their electronic data interchange equipment is accessible, in so far as possible, also outside office hours.

Section 20 Authorities' contact information

The authorities shall make their contact information for electronic data interchange available in an appropriate manner.

Chapter 4
Electronic lodging of matters

Section 21 Risk of delivery of an electronic message

The delivery of electronic messages to the authorities shall take place at the risk of the sender.

Section 22 Lodging a matter by electronic document

(1) If a matter is to be lodged in writing, it can be lodged also by way of a document delivered to the authority as an electronic message.

(2) If a matter is to be lodged by a signed document, an electronic signature shall be accepted as the signature, if the certifier and the certificate of the signature meet the requirements set in sections 4 and 5.

Section 23 Time of delivery

(1) An electronic message shall be deemed to have been delivered to the authority when it is available for the use of the authority in a reception device or data system so that the message can be handled.

(2) If the time of delivery referred to in paragraph (1)cannot be determined, the electronic message shall be deemed to have been delivered at the time it was sent, provided that the sending time can be reliably verified.

Section 24 Notification of receipt

(1) A notification of the receipt of an electronic message shall be given without delay by the authority to the sender. The notification can be given by way of the data system as an automatic receipt or otherwise. The notification of receipt shall not have any effect on the prerequisites for the handling of the matter; separate provisions apply to these prerequisites.

(2) The provisions in paragraph (1) do not apply to a document delivered by telefax or by comparable means.

Section 25 Diary entries and records

(1) Diary entries or other reliable records shall be made on electronic documents that have been received.

(2) A diary entry or record shall indicate the time of delivery of the document and the checks on the integrity and originality of the document.

Section 26 Technical editing of the message

An authority may technically edit a message received by it, if this is necessary in order to render the message into a legible format.

Section 27 Forwarding of an electronic document

The provisions in section 8 of the Administrative Procedure Act apply to the forwarding of an electronic document delivered by mistake to the wrong authority.

Chapter 5
Electronic signature and service of notice of decisions

Section 28 Electronic signature of decisions

A decision may be signed electronically. The electronic signature of an authority shall meet the requirements for an acceptable electronic signature, as provided in section 22(2).

Section 29 Electronic service of notice of a decision

(1) Where an appeal period begins upon service of notice of the decision or where the decision enters into force upon service of notice, the decision may on the consent of the party be served also as an electronic message, but not, however, as a telefax or by comparable means. In this event, the authority shall make a notification to the effect that the decision is available for retrieval by the party or a representative of the party on a server designated by the authority.

(2) The party or the representative of the party shall identify themselves at the time of retrieval of the decision. The identification may be accepted, if the certifier and certificate meet the requirements provided in sections 4 and 5.

(3) The service of notice of the decision shall be deemed effected upon retrieval of the document from the server referred to in paragraph (1). If the decision is not retrieved within seven days of the notification, the provisions in other legislation on service of notice shall be complied with in the service of notice of the decision.

Section 30 Copy of the decision

Once the period of validity of an electronic signature in a decision has ended, the party has the right to receive, upon request, a new copy of the decision free of charge.

Section 31 Contact information for rectification requests and appeals

If a rectification request or an appeal can be electronically lodged with an authority, the relevant contact information shall be supplied in the rectification or appeal instructions. Otherwise, the provisions in section 24a of the Administrative Procedure Act on rectification instructions and section 14 of the Act on Administrative Judicial Procedure (586/1996) on appeal instructions apply in the matter.

Section 32 Electronic service of notice of other documents

A document other than that referred to in section 19 may be served on a party as an electronic message in the manner requested by the party. However, if data security so requires, the provisions in section 29(1) and (2) apply to the service of notice of the document.

Chapter 6
Miscellaneous provisions

Section 33 Electronic identity cards

A certificate referred to in section 3(1) of the Identity Cards Act (829/1999) shall always be acceptable in electronic service.

Section 34 Acceptance of foreign certificates

A certificate issued in another country may be accepted, if the certifier and the certificate meet the requirements laid down in chapters 4-6, if the issuance of the certificate can be deemed appropriate and if the operations of the certifier can be deemed to meet the criteria laid down in section 7(1).

Section 35 Duty of notification of the person in possession of a certificate

The person in possession of a certificate shall notify the certifier immediately if he/she loses possession or if he/she has reason to believe that the certificate is otherwise susceptible to unauthorised use.

Section 36 Consequences of the unauthorised use of a certificate

(1) A person in possession of a certificate shall be liable for the unauthorised use of an instrument of electronic identification or the production of an electronic signature only if he/she has relinquished possession of the instrument to a third person or if he/she has failed in the duty of notification provided in section 35.

(2) A person in possession of a certificate shall not be liable for the unauthorised use of the instrument

(3) if the instrument has been used after the notification on the loss of possession has been received by the certifier, or

(4) if the third party who relied on the certificate has not verified its validity.

Section 37 Penal provisions

(1) Chapter 38, section 9 of the Penal Code (39/1889) contains the penal provision governing personal data file offences and section 48(2) of the Personal Data Act contains the penal provision governing personal data violations.

(2) A person who deliberately or negligently breaches the provisions in section 14 on the procedure for the identification of a person requesting a certificate shall be sentenced for *neglect to identify a person requesting a certificate* to a fine.

Section 38 Archiving

An electronic document shall be archived in a manner allowing for the later verification of its integrity and originality.

Section 39 Charges

Separate provisions apply to the charges payable for administrative decisions.

Section 40 Administrative instructions and guidance

(1) The Ministry of Finance shall publish a list of the certifiers and certificates in electronic service in the administration meeting the requirements of sections 4 and 5; the list shall be as exhaustive and up-to-date as possible; In addition, the Ministry of Finance shall provide instructions and guidance on the arrangement of the data administration required for electronic service. The Ministry of the Interior shall provide instructions and guidance on the arrangement of electronic service.

(2) The Archival Service shall provide instructions and guidance on diary entries, other records and archiving in the context of electronic service.

Section 41 Appeals

(1) A decision on the issuance of a certificate in use in the administration or on the validity of such a certificate shall be subject to appeal before an Administrative Court as provided in the Act on Administrative Judicial Procedure.

(2) A certifier may request that information on itself or on the certificate offered by it be included in the list referred to in section 40 or that information in the list be deleted or altered. A decision of the Government on such a request shall be subject to appeal as provided in the Act on Administrative Judicial Procedure.

Section 42 Further provisions

Where necessary, further provisions on the implementation of this Act shall be issued by Decree.

Section 43 Entry into force

(1) This Act shall enter into force on 1 January 2000.

(2) Measures necessary for the implementation of this Act may be undertaken prior to its entry into force.