Unofficial translation

Act

on Electronic Signatures

(14/2003)

Chapter 1

General provisions

Section 1

Purpose of the Act

The purpose of this Act is to promote the use of electronic signatures and the provision of products and services related to them as well as to promote data protection and data security of electronic commerce and electronic communication.

Section 2

Definitions

For the purposes of this Act:

1) *electronic signature* means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authenticating the identity of the signatory;

2) *advanced electronic signature* means an electronic signature

a) which is uniquely linked to the signatory;

b) which is capable of identifying the signatory;

c) which is created using means that the signatory can maintain under his sole control; and

d) which is linked to other electronic data in such a manner that any subsequent change of the data is detectable.

3) *signatory* means a natural person who lawfully holds the signature-creation data and who acts either on his own behalf or on behalf of the natural or legal person he represents;

4) *signature-creation data* means unique data, such as codes or private keys, which are used by the signatory to create an electronic signature;

5) *signature-creation device* means software or hardware used together with signature-creation data to implement an electronic signature;

6) *signature-verification data* means data, such as codes or public keys, which are used for the purpose of verifying an electronic signature;

7) *certificate* means electronic data which links signature-verification data to the signatory and confirms the identity of the signatory;

8) *certification-service-provider* means a natural or legal person who provides certificates;

9) *electronic-signature product* means hardware or software, or relevant parts thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or

to be used in the creation or verification of electronic signatures; as well as

10) *electronic-signature service* means the provision of certificates as well as that of other products or services related to electronic signatures.

Section 3

Scope of application

This Act shall apply to electronic signatures as well as to service providers who offer products or services related to electronic signatures to the public.

The use of electronic signatures in administration shall further be governed by provisions to be issued separately.

Section 4

Free circulation of services and products

Electronic-signature products and services complying with this Act are permitted to circulate freely in the internal market.

Section 5

Secure signature-creation device

A secure signature-creation device must with sufficient reliability ensure that

1) the signature-creation data can practically occur only once and that their secrecy is assured;

2) the signature-creation data cannot be derived from other data;

3) the signature is protected against forgery;

4) the signatory can protect the signature-creation data against the use of others; as well as that

5) the creation device does not alter the data to be signed and that it does not prevent such data from being presented to the signatory prior to the signature process.

The signature-creation device shall always be deemed to meet the requirements laid down in paragraph 1 if

1) it complies with the generally accepted standards confirmed by the Commission of the European Communities and published in the Official Journal of the European Communities; or if

2) the secure signature-creation device has been approved by an inspection body designated for the assessment of conformity and located in Finland or in another State belonging to the European Economic Area.

Section 6

The inspection body

The Finnish Communications Regulatory Authority may designate inspection bodies to assess whether a signature-creation device meets the requirements laid down in section 5, paragraph 1. The inspection bodies may be private or public bodies.

The designation of an inspection body shall require that

1) the inspection body is functionally and financially independent;

2) its operations are reliable, appropriate and non-discriminatory;

3) it has sufficient financial resources to arrange its operations appropriately and to cover any liability for damages;

4) it has a sufficient professional and unbiased personnel; and that

5) it has the facilities and equipment necessary for its operations.

The Finnish Communications Regulatory Authority shall designate the inspection bodies upon an application. In addition to the contact information and the Trade Register extract of the applicant, the application shall contain an account of the fulfilment of the requirements referred to in paragraph 2 with respect to the operations of the applicant. Where necessary, the Finnish Communications Regulatory Authority shall issue instructions on the information to be included in the application and on its delivery to the Finnish Communications Regulatory Authority.

The Finnish Communications Regulatory Authority shall supervise the operations of

the inspection body. If the inspection body does not meet the requirements laid down or if it violates the provisions, the Finnish Communications Regulatory Authority shall withdraw its designation decision. The inspection body shall notify the Finnish Communications Regulatory Authority of any changes relating to the criteria for designation.

In its assessment work the inspection body may be assisted by outside parties. The inspection body shall be liable also for the work of outside parties assisting it.

Chapter 2

Provision of qualified certificates

Section 7

Qualified certificate

A qualified certificate shall mean a certificate meeting the requirements laid down in paragraph 2 and issued by a certification-service-provider meeting the requirements laid down in sections 10 - 15.

A qualified certificate shall contain:

1) an indication that the certificate is a qualified certificate;

2) the identification of the certification-service-provider and the State in which it is established;

3) the name of the signatory or a pseudonym, which shall be identified as such;

4) signature-verification data which correspond to the signature-creation data under control of the signatory;

5) the period of validity of the qualified certificate;

6) the identity code of the qualified certificate;

7) the advanced electronic signature of the certification-service-provider;

8) any limitations on the scope of use of the qualified certificate; and

9) specific data relating to the signatory if relevant for the purpose of use of the qualified certificate.

Section 8

Qualified certificate provided by a certification-service-provider established outside Finland

A certificate provided as a qualified certificate by a certification-service-provider not established in Finland shall be deemed to meet the requirements concerning qualified certificates laid down in this Act if

1) the certification-service-provider is established in a State belonging to the European Economic Area and the certificate meets the requirements laid down for a qualified certificate in the State of establishment; or if

2) the certification-service-provider belongs to a voluntary accreditation scheme in a State belonging to the European Economic Area and meets the national requirements laid down in that State for the implementation of Directive 1999/93/EC; or if

3) the certificate is guaranteed by a certification-service-provider that is established in a State belonging to the European Economic Area and who meets the national requirements laid down in that State for the implementation of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, hereafter Directive on electronic signatures; or if

4) the certificate or certification-service-provider is recognised under a bilateral or multilateral agreement between the European Community and third countries or international organisations.

Section 9

Notification on the start of operations

A certification-service-provider that intends to provide qualified certificates to the public shall, prior to the start of the provision of qualified certificates, submit a written notification to the Finnish Communications Regulatory Authority. The notification shall contain the name and contact information of the certification-service-provider as well as information on the basis of which it is

possible to ensure that the requirements laid down in section 7 and sections 10-15 are fulfilled. The Finnish Communications Regulatory Authority may issue orders and recommendations necessary for supervision on the further contents of the information to be provided to the Finnish Communications Regulatory Authority and on the procedure for its notification.

If a certificate does not fulfil the requirements laid down in section 7, paragraph 2, or if the certification-service-provider does not fulfil the requirements laid down in sections 10 - 15, the Finnish Communications Regulatory Authority shall without delay after learning of the matter forbid the certification-service-provider from providing its certificates as qualified certificates.

If the information referred to in paragraph 1 has changed, the certification-service-provider shall without delay inform the Finnish Communications Regulatory Authority of the changes in writing.

The Finnish Communications Regulatory Authority shall maintain a public register of certification-service-providers providing qualified certificates.

Section 10

General obligations of a certification-service-provider providing qualified certificates to the public

The operations of a certification-service-provider providing qualified certificates to the public shall be careful, reliable and appropriate and non-discriminatory towards its customers. The certification-service-provider shall have technical expertise and financial resources sufficient vis-á-vis the scope of operations. The certification-service-provider shall be liable for all the aspects of the certification operations, including the reliability and functionality of any services and products produced by parties assisting the certification-service-provider.

The certification-service-provider shall:

1) ensure that its personnel has sufficient expertise, experience and qualifications;

2) ensure that it has sufficient financial resources to arrange its operations and to cover any liability for damages;

3) have generally available all relevant information on the certificate and certification operations for the assessment of the operations and reliability of the certification-service-provider; and

4) ensure the confidentiality of the certificate-creation data when these data are produced by the certification-service-provider.

The certification-service-provider may not store or copy the signature-creation data submitted to the signatory.

Section 11

Trustworthy hardware and software

A certification-service-provider providing qualified certificates to the public shall ensure that the systems, hardware and software it uses are sufficiently trustworthy as well as protected against alterations and forgery.

Hardware or software relating to electronic signatures is deemed to fulfil the requirements laid down in paragraph 1, if it complies with the generally accepted standards confirmed by the Commission of the European Communities and published in the Official Journal of the European Communities.

Section 12

Issuing a qualified certificate

A certification-service-provider providing qualified certificates to the public shall, in a careful and reliable manner, verify the identity of the person applying a qualified certificate as well as any other data relating to the person applying for the certificate necessary for the issuing and maintenance of the qualified certificate.

A certification-service-provider providing qualified certificates to the public shall, before entering into a contract, inform the person applying for a qualified certificate of the terms regarding the use of the qualified certificate, including any limitations on its

use, the existence of voluntary accreditation schemes, the supervision of certification operations by the authorities as well as of the procedure for complaints and dispute settlement. The person applying for a qualified certificate shall be given the information in an easily comprehensible form. The information shall be given at least in Finnish or Swedish according to the applicant's choice.

Section 13

Revocation of a qualified certificate

The signatory shall without delay request the certification-service-provider that has issued the qualified certificate to revoke it if it has justified reason to suspect unlawful use of the signature-creation data.

A certification-service-provider providing qualified certificates to the public shall, without delay, revoke a qualified certificate when so requested by the signatory. A request for the revocation of a qualified certificate shall be deemed received by the certification-service-provider when it has been available to the certification-service-provider so that the handling of the request has been possible.

A qualified certificate may also be revoked for another special reason. The signatory shall always be informed of the revocation of a qualified certificate and the time of its revocation.

Section 14

Registers maintained by a certification-service-provider providing qualified certificates to the public

A certification-service-provider providing qualified certificates to the public shall maintain a register of qualified certificates issued by it (certificate register). The following shall be entered in the register:

1) the data content of a qualified certificate defined in section 7, paragraph 2;

2) the data relating to the person applying for the certificate and referred to in section 12, paragraph 1, including information on the procedure used to identity the applicant when issuing the qualified certificate, and necessary information of a possible document used in identification; and

3) the information referred to in section 21 on checking the validity of the certificate from the revocation list, if the certification-service-provider providing qualified certificates to the public uses the right to store information as referred to in section 21.

A certification-service-provider providing qualified certificates to the public shall ensure that the data content of the certificate defined in section 7, paragraph 2 is available to a party relying on an advanced electronic signature certified with a qualified certificate. However, information referred to above in paragraph 1, subparagraph 3 shall not have to be stored in a certificate register, if the certification-service-provider takes other measures to ensure that the party relying on the certificate is able to reliably show that a revocation list is properly checked.

The certification-service-provider shall also maintain a public register of revoked qualified certificates (revocation list) available to parties relying on qualified certificates. Information on the revocation of a qualified certificate and a specific time of revocation shall appropriately and without delay be entered in the revocation list.

The information referred to in paragraphs 2 and 3 shall be available 24 hours a day.

Section 15

Maintenance of the information in the certificate register

A certification-service-provider providing qualified certificates to the public shall maintain the information of the certificate register in a reliable and appropriate manner for 10 years after the end of the validity of the certificate.

Section 16

Liability for damages of a certification-service-provider providing qualified certificates

A certification-service-provider providing qualified certificates to the public shall be liable for damage caused to a party relying on a qualified certificate due to the following:

1) the data entered in the qualified certificate have been wrong when the certificate has been issued;

2) the qualified certificate does not contain the data referred to in section 7, paragraph 2;

3) at the time of the issuance of the certificate, the signatory identified in the qualified certificate did not hold the signature-creation data corresponding to the signature-verification data;

4) the signature-creation data and signature-verification data created by the certification-service-provider or the party assisting it are not compatible; or

5) the certification-service-provider or a party assisting it has not revoked the qualified certificate in the manner provided for in section 13.

The certification-service-provider shall be discharged from the liability laid down in paragraph 1 if it proves that the damage was not due to his own negligence or the negligence of a party assisting it.

A certification-service-provider shall not be liable for damage caused by violating a limitation on use contained in a qualified certificate.

In other respects, the liability for damages of a certification-service-provider providing qualified certificates to the public shall be governed by the Damages Act (412/1974).

The provisions of this section shall also apply to a certification-service-provider, who guarantees to the public that a certificate is a qualified certificate.

Section 17

Liability for unauthorised use of signature-creation data

The signatory shall be liable for damage caused by unauthorised use of the signature-creation data of an advanced electronic signature certified by a qualified certificate until the request to revoke the certificate has been received by the certification-service-provider as provided for in section 13, paragraph 2.

However, a consumer shall be subject to the liability laid down in paragraph 1 only if:

1) he has given the creation data to someone else;

2) the creation data have ended in the possession of a person not authorised to use them due to the negligence of the signatory, which is not slight; or if

3) after losing control of the creation data in a manner other than that referred to in subparagraph 2, he has failed to request the revocation of the qualified certificate as provided for in section 13, paragraph 1.

A contract term derogating from the provisions of paragraph 2 to the detriment of the consumer shall be void.

Chapter 3

Legal effect of an electronic signature and the processing of personal data

Section 18

Legal effect of an electronic signature

If the law requires that a signature be attached to a legal act, this requirement shall be fulfilled at least by an advanced signature based on a qualified certificate and created by means of a secure signature-creation device.

Section 19

Processing of personal data

A certification-service-provider providing certificates to the public may collect personal data necessary for the issuing and

maintenance of the certificate only directly from the signatory. With regard to a certification-service-provider providing qualified certificates to the public, further provisions on the issuing of a qualified certificate, the registers to be maintained and the information to be maintained are contained in chapter 2 of this Act.

When verifying the identity of a person applying for a certificate, the certification-service-provider may require him to provide his personal identity number. The personal identity number of the signatory may not be included in the certificate.

Personal data may only under the explicit written permission of the signatory:

1) be collected otherwise than directly from the signatory; or

2) be processed for a purpose other than that referred to in paragraph 1.

The processing of personal data shall further be governed by the provisions of the Personal Data Act (523/1999) thereon.

Section 20

Use of the Population Information System

Upon the express consent of the person applying for a certificate, the certification-service-provider may obtain and verify the personal data given by the person from the Population Information System.

The information extracted from the Population Information System shall be delivered as a public-law performance in accordance with the Act on the Charge Criteria of the State (150/1992).

Section 21

Storing the information regarding the validity checking of a certificate

The certification-service-provider may store the information regarding the checking of the validity of a certificate from the revocation list. The information stored may only be used to invoice for the use of certificates or to verify legal acts performed by using an electronic signature certified by a certificate.

Chapter 4

General guidance and supervision

Section 22

General guidance and supervision

The general guidance and development of certification operations shall be the responsibility of the Ministry of Transport and Communications.

The Finnish Communications Regulatory Authority shall be in charge of supervision in compliance with this Act. Where necessary, the Finnish Communications Regulatory Authority shall issue technical orders and recommendations on the requirements of reliability and data security of the operations of certification-service-providers providing qualified certificates relating to electronic signatures.

Provisions of the Act on the Charge Criteria of the State (150/1992) shall apply to charges collected for supervision and other tasks of the Finnish Communications Regulatory Authority.

The Data Protection Ombudsman shall supervise the compliance with the provisions of this Act concerning personal data. When performing his duties, the Data Protection Ombudsman shall have the right to obtain information and to perform inspections referred to in the Personal Data Act. Provisions on appeal regarding the operations of the Data Protection Ombudsman shall be governed by the Personal Data Act.

Section 23

Right to obtain information

Without prejudice to provisions on secrecy, the Finnish Communications Regulatory Authority may obtain information necessary for the tasks laid down in section 22 from certification-service-providers who provide to the public qualified certificates relating to electronic signatures, and from people assisting them.

Section 24

Right of inspection

An inspector appointed to the task by the Finnish Communications Regulatory Authority shall have the right to perform an inspection to supervise compliance with this Act and the orders issued thereunder. The person performing the inspection shall have the right to inspect the hardware and software used by a certification-service-provider providing qualified certificates to the public and of a party assisting it if the hardware or software may be relevant for the supervision of compliance with this Act and with orders issued thereunder.

A certification-service-provider providing qualified certificates to the public or a party assisting it shall provide the inspector referred to in paragraph 1 access to its manufacturing, business and storage premises, if these do not fall within the scope of domestic peace.

The Finnish Communications Regulatory Authority shall be entitled to obtain executive assistance from the police to perform an inspection referred to in paragraphs 1 and 2.

Section 25

Secrecy obligation

Those performing duties under this Act shall be subject to a secrecy obligation as provided for in the Act on Openness of Government Activities (621/1999).

Chapter 5

Miscellaneous provisions

Section 26

Provision on sanctions

Punishment for a personal register crime shall be governed by the provisions of chapter 38, section 9 of the Penal Code (39/1889) and that for a personal register offence by the provisions of section 48, paragraph 2 of the Personal Data Act.

Section 27

Administrative coercive measures

The Finnish Communications Regulatory Authority may order anyone violating this Act or orders issued thereunder to remedy his fault or omission. The decision may be enforced through the imposition of a conditional fine or a threat that either part or all of the operations are suspended or that the omitted measure will be ordered to be performed at the cost of the party in question. The conditional fine, threat of suspension and threat of having a measure performed shall be governed by the provisions of the Act on the Conditional Imposition of a Fine (1113/1990).

The costs of work ordered to be performed shall be paid in advance from State funds and they shall be collected from the neglecting party as provided for in the Act on the Collection of Taxes and Charges through Execution (367/1961).

Section 28

Appeal

Appeal against a decision made by the Finnish Communications Regulatory Authority by virtue of this Act shall be governed by the provisions of the Administrative Judicial Procedure Act

(586/1996).

The Finnish Communications Regulatory Authority may in its decision order that the decision shall be complied with before it becomes final. However, the appeal authority may enjoin the enforcement of the decision until the appeal has been decided.

Section 29

Entry into force

This Act shall enter into force on 1 February 2003.

Measures necessary for the implementation of this Act may be taken prior to its entry into force.

Section 30

Transitional provisions

A certification-service-provider that has started to provide qualified certificates to the public prior to the entry into force of the Act shall make a notification referred to in section 9 no later than within three months from the entry into force of the Act.