

**NB: Unofficial translation;
legally binding texts are those in Finnish and Swedish**

Act

on Strong Electronic Identification and Electronic Signatures

(617/2009)

Chapter 1 General provisions

Section 1

Scope of application

(1) This Act lays down provisions on strong electronic identification and electronic signatures, as well as on the offering of these services to service providers using them and to the general public.

(2) This Act does not apply to strong electronic identification within an organization or the offering of services for electronic signatures.

(3) Neither does this Act apply to services where an organization uses its own identification methods for the identification of its own customers in its own services.

(4) This Act does not apply to the manufacture, import and sales of devices for strong electronic identification or electronic signatures.

Section 2

Definitions

For the purposes of this Act:

1) *strong electronic identification* means the identification of a person and the verification of the authenticity and validity of the identification by an electronic method based on at least two of the following three alternatives:

- a) password or something similar that the identification device holder knows;
- b) chip card or something similar that the identification device holder has in his possession; or
- c) fingerprint or some other characteristic identifying the device holder;

2) *identification device* means objects or identifying data or characteristics that together form the identifiers, identification devices and verification devices required for strong electronic identification;

3) *identification method* means the entirety of the identification device and system required to create an individual strong electronic identification event;

4) *identification service provider* means a provider offering services for strong electronic identification to service providers using them or issuing identification devices to the general public or both;

5) *identification device holder* means a natural person to whom the identification service provider has issued an identification device based on an agreement;

6) *initial identification* means the verification of the identity of the applicant for an identification device in connection with the acquisition of the device;

7) *certificate* means an electronic verification that confirms the identity or confirms the identity and links the data for verifying a signature to the signatory, and that can be used for strong electronic identification and electronic signatures;

8) *certification service provider* means a natural person or legal person who offers certificates to the general public;

9) *electronic signature* means data in an electronic form that is linked or logically connected to some other electronic data and used as a device for verifying the identity of the signatory;

10) *advanced electronic signature* means an electronic signature:

- a) that is unambiguously linked to the signatory;
- b) that can be used to identify the signatory;
- c) that has been created by using a method which the signatory is able to keep under his exclusive control; and
- d) that is linked to some other electronic data in such a way that any alterations made in the data can be detected;

11) *data for creating a signature* means the unique set of data, such as codes or private keys, used by the signatory for the creation of an electronic signature;

12) *means of creating a signature* means software and hardware which, together with the data for creating a signature, are used to create an electronic signature; and

13) *data for verifying a signature* means a set of data, such as codes or public keys, used for verifying an electronic signature.

Chapter 2 **Legal effects and processing of personal data**

Section 3

Imperative nature of the provisions

Any contractual terms that differ from the provisions of this Act to the detriment of the consumer are deemed void unless otherwise provided below.

Section 4

Electronic signatures to be created with an identification device

Electronic signatures and advanced electronic signatures may be created with identification devices depending on their characteristics, unless otherwise provided by law or section 18.

Section 5

Legal transactions

(1) Identification devices may be used in the execution of legal transactions, unless otherwise provided by law or section 18.

(2) If a signature is required for a legal transaction, an advanced electronic signature based on a qualified certificate and created with a secure signature creation device will satisfy this requirement. However, the legal validity of an electronic signature cannot

be denied solely on the grounds that it was created using another method than the one referred to above.

(3) Separate provisions shall be issued regarding the use of electronic signatures in the public administration sector.

Section 6

Processing of personal data

(1) An identification service provider may process necessary personal data on the grounds referred to in section 8(1)(1 and 2) of the Personal Data Act within the course of issuing and maintaining the identification devices and performing the identification event. On the same grounds, a certification service provider may process personal data for issuing and maintaining certificates. Besides for the purpose specified above, identification service providers and certification service providers may collect personal data from the persons directly.

(2) For any other purposes than those referred to in subsection 1, personal data may only be processed on the grounds referred to in section 8(1)(1) of the Personal Data Act.

(3) When verifying the identity of an applicant, identification and certification service providers may request the personal ID code of the applicant. Identification and certification service providers may process personal ID codes in their registers for purposes set out in subsection 1. The personal ID code may be included in the identification device or certificate only if the data content of the devices or certificate is accessible exclusively to those persons who absolutely require them in the performance of their services. A personal ID code must not be available in a public directory.

(4) Other provisions on the processing of personal data are issued in sections 19, 24, 30, 37 and 38 and in the Personal Data Act.

Section 7

Use of data stored in the population data system

(1) Identification service providers and certification service providers offering electronic signatures may collect personal data and verify personal information provided by an applicant or holder in the population data system by virtue of section 8(1)(1)(2) of the Personal Data Act and for the purposes of section 6(1) of this Act.

(2) Data from the population data system is released as a service under public law in accordance with the provisions of the Act (150/1992) on Criteria for Charges Payable to the State.

Chapter 3 **Strong electronic identification**

Section 8

Requirements posed on the identification method

- (1) The identification method must meet the following requirements:
- 1) The method shall be based on initial identification according to section 17, where the relevant data can be verified afterwards as set out in section 24;
 - 2) the method shall unambiguously identify the identification device holder;
 - 3) the method is sufficiently secure to ensure that only the identification device holder can use the device; and
 - 4) the method is sufficiently secure and reliable, taking into consideration the relevant technical threats to data security.
- (2) The provisions of subsection 1 do not prohibit offering a specific service in a way that the identification service provider discloses to the service provider using the identification service the pseudonym of the identification device holder or only a limited amount of personal data.
- (3) The Finnish Communications Regulatory Authority may issue further technical regulations regarding the requirements set out in subsection 1.

Section 9

Requirements posed on the identification service provider

- (1) Any natural persons operating as or for an identification service provider, members and deputy members of the management board or board of directors, chief executives, general partners or persons in equivalent positions in an identification service organization shall meet the following requirements:
- 1) they must be of age;
 - 2) they must not have declared bankruptcy; and
 - 3) their operating capacity must not be restricted.
- (2) An identification service provider shall be trustworthy. An identification service provider is not deemed trustworthy if a person referred to in subsection 1 has been convicted of a crime by a court of law during the past five years, or has been fined during the past three years for a felony that would make such person obviously unfit to act as an identification service provider.
- (3) An identification service provider is not deemed trustworthy if a person referred to in subsection 1 has previously acted in a way that would make such person an obviously unfit identification service provider.

Section 10

An identification service provider's obligation to notify commencement of operations

- (1) An identification service provider based in Finland who intends to offer services shall, prior to commencement of such services, submit a written notification to the Finnish Communications Regulatory Authority. Such notification may also be

submitted by an association of service providers, if such services provided can be deemed as such by an identification service.

(2) The notification shall include:

- 1) name of the service provider;
- 2) complete contact information of the service provider;
- 3) information about the services to be provided;
- 4) information about facts referred to in sections 8, 9, 13 and 14; and
- 5) other information relevant to monitoring.

(3) The identification service provider shall notify the Finnish Communications Regulatory Authority in writing and without delay of any changes to information referred to in subsection 2. A notification shall also be submitted if business operations are discontinued or transferred to a different service provider.

(4) The Finnish Communications Regulatory Authority may issue technical regulations relevant to monitoring and regarding details of aforementioned information to be submitted and their submission to the Finnish Communications Regulatory Authority.

Section 11

An identification service provider based in another member state of the European Economic Area

The provisions of section 10 will not prevent an identification service provider based in the EEA from submitting a notification referred to in the subsection.

Section 12

Register related to an identification service provider

(1) The Finnish Communications Regulatory Authority maintains a public register of identification service providers, who have submitted a notification according to section 10, and their services.

(2) Upon receipt of notice referred to in section 10, the Finnish Communications Regulatory Authority shall forbid the identification service provider from offering its services as strong electronic identification if the services or the provider do not meet the requirements of this Chapter. If the shortcomings are minor, the Finnish Communications Regulatory Authority may ask the service provider to correct them within a specified period.

Section 13

General obligations of an identification service provider

(1) The identification service provider shall ensure that its personnel have adequate expertise, experience and competence.

(2) The identification service provider shall have sufficient financial resources for its operation and for covering possible liabilities for damages. The service provider may also take other necessary measures regarding possible liabilities for damages.

(3) The identification service provider shall also protect personal data referred to in section 32 of the Personal Data Act and ensure adequate information security.

(4) The identification service provider is responsible for the reliability and functionality of services and products provided by people working for it.

Section 14

Identification principles

(1) The identification service provider shall have identification principles in place that define how the provider will perform its obligations set out in this Act. In particular, they should specify how the service provider will perform the initial identification referred to in section 17.

(2) The identification principles shall also provide the following central information about:

- 1) the service provider;
- 2) services to be provided and their prices;
- 3) the most important cooperation partners of the service provider;
- 4) audits performed by external auditors; and
- 5) other relevant information on the basis of which the operation and trustworthiness of the service provider can be assessed.

(3) If the identification device may also be used for electronic signatures or advanced electronic signatures, the identification service provider shall also inform of their implementation method, level, and security factors.

(4) The identification service provider shall keep the identification principles updated and in a generally accessible location.

Section 15

The identification service provider's duty of disclosure prior to entering into an agreement

(1) Prior to entering into an agreement with an applicant for an identification device, the service provider shall disclose to the applicant information about:

- 1) the service provider;
- 2) the services offered and their prices;
- 3) the identification principles referred to in section 14;
- 4) the rights and responsibilities of the parties;
- 5) potential limits of liability;
- 6) complaint and dispute settlement procedures;
- 7) potential restraints and restrictions on use referred to in section 18; and
- 8) other potential terms of use related to the identification device.

(2) The data in subsection 1 shall be submitted in writing or in electronic form so that the applicant for an identification device can store and reproduce them unaltered. If, upon an applicant's request, an agreement is entered into by distance communication that will not allow submission of data and contract terms in the aforementioned manner, such data shall be submitted in the said manner immediately after the agreement has been executed.

(3) Provisions on the duty of disclosure regarding the processing of personal data are issued in the Personal Data Act.

Section 16

The identification service provider's duty of notification about threats and risks related to data security and protection

(1) The identification service provider shall notify, without any undue delay, service providers using its services, identification device holders and the Finnish Communications Regulatory Authority of severe risks and threats to its data security.

(2) If the risk or threat is aimed at data protection referred to in section 32 of the Personal Data Act, the identification service provider shall notify the Data Protection Ombudsman in addition to the parties mentioned in subsection 1.

(3) The notification must also include information about measures the parties involved have for use to counter such threats and risks, as well as the expenses incurred by these measures.

Section 17

Initial identification of an applicant for an identification device

(1) The initial identification shall be done in person. The identification service provider shall carefully check the identity of the identification device applicant, as evidenced by a valid passport or identity card issued by a government official of an EEA member state, Switzerland, or San Marino. For initial identification purposes, the identification service provider may, if desired, also use a valid driving license issued by an official of an EEA member state after 1 October 1990 or a valid passport issued by a government official of another state.

(2) An exception to the rule of doing the initial identification in person can be made if the identification service providers have entered into a mutual agreement on ways to rely on each other in performing the initial identification. In such cases, the identification device may be applied for electronically. In their agreement, the identification service providers shall define how the liability from potential faulty initial identification will be shared among them. Regarding the party sustaining the damage, the identification service provider relying on another provider performing the initial identification shall be held responsible.

(3) An identification device may also be applied for electronically, if the applicant has a valid identification device from the same identification service provider. In such cases, initial identification will not be necessary.

(4) If the identity of an applicant cannot be reliably established, the police will perform the initial identification for the application. Expenses incurred to the identification device applicant by the initial identification performed by the police are expenses of a service under public law. Provisions regarding charges levied for the service are issued in the Act on Criteria for Charges Payable to the State.

Section 18

Preclusions and restrictions regarding legal transactions

(1) The use of identification device for legal transactions may be precluded by agreements between the identification service provider, the identification service provider using the service and the identification device holder. Restrictions may also

be imposed on legal transactions, either with regard to their purpose or the monetary values involved.

(2) The identification service provider shall ensure that all parties are aware of the preclusions or restrictions or that they are conspicuous. The identification service provider may also implement preclusions and restrictions by technical means. The identification service provider shall not be responsible for transactions performed contrary to preclusions and restrictions, regardless of the fact that the identification service provider acted with due care.

(3) The identification service provider shall provide an opportunity for users of its services to check preclusions and restrictions related to the identification device at all times. However, the provider will not be held responsible if the use contrary to preclusions and restrictions was prevented by technical means.

(4) It is the responsibility of a service provider using identification services to check the systems and registers maintained by the identification service provider for potential preclusions and restrictions related to the use of the identification device. However, a check will not be necessary if the use contrary to preclusions and restrictions was prevented by technical means.

Section 19

Data content of the certificate

(1) If the identification method is based on a certificate, the certificate must include at least:

- 1) information of the certification service provider;
- 2) information of the holder of the certificate;
- 3) the identifier identifying the holder;
- 4) the validity period of the certificate;
- 5) the identifier identifying the certificate;
- 6) potential preclusions or restrictions on the use of the certificate;
- 7) the public key of the certificate holder and its purpose of use; and
- 8) the certification service provider's advanced electronic signature.

(2) The certification service provider shall ensure that the data content of the certificate is available to the service provider using the certificate for electronic identification.

Section 20

Issuance of an identification device

(1) The issuance of an identification device is based on the agreement between the applicant for the identification device and the identification service provider. The agreement must be in writing. The agreement can be in electronic format, provided that its content cannot be changed unilaterally and that it remains available to the parties. The identification service provider shall treat its customers in a non-discriminatory way and the identification device applicants fairly when entering into the agreement.

(2) The agreement can be temporary or for a limited time period. The identification device can have a validity period that is shorter than the term of the agreement.

(3) An identification device is always given to a natural person. The identification device must be person-specific. If needed, data may be linked to the identification device allowing the person to represent another natural or legal person as needed.

Section 21

Delivering the identification device to the applicant

The identification service provider shall deliver the identification device to the applicant as stated in the agreement. The identification service provider shall reasonably ensure that the identification device will not end up in an unauthorized person's possession during delivery.

Section 22

Renewal of the identification device

The identification service provider may provide a new identification device without explicit request to the holder only if a previously delivered identification device needs to be replaced. Delivery should follow the rules in section 21.

Section 23

Obligations of the identification device holder

(1) The identification device holder shall use the device according to the terms and conditions of the agreement. The holder shall store the identification device with care. The holder's duty of care for the identification device starts with its acceptance.

(2) The identification device holder may not transfer the device.

Section 24

Storage and use of data regarding the identification event and device

(1) The identification service provider shall store:

1) data required for performing an individual identification event and an electronic signature;

2) data required for initial identification of an applicant referred to in section 17 and the file used for this purpose;

3) data on potential preclusions or restrictions on the use of identification device referred to in section 18; and

4) data content of the certificate as set out in section 19.

(2) Data mentioned in subsection 1(1) above shall be kept for five years from the identification event; and data mentioned in paragraphs 2-4 above for five years from termination of the customer relationship between the identification service provider and the identification device holder.

(3) Personal data generated during the identification event shall be destroyed after the event, unless they are required to be kept to verify an individual identification event.

(4) The identification service provider may process stored data only to perform and maintain the service, for invoicing, to protect its rights in case of disputes, as well as upon request by the service provider using identification service or the holder of the identification device. The identification service provider shall store data on processing the event, the time, reason, and person processing it.

(5) Subsections 1(1) and (3) above do not apply to service providers who only issue identification devices. The five-year record-keeping period referred to in subsection (2) above will then be calculated from the date the identification device validity expires.

Section 25

Cancellation and prevention of use of identification devices

(1) The identification device holder shall notify the identification service provider or a designated party if the identification device has been lost, is in the unauthorized possession of another person or of any unauthorized use immediately upon detection of this fact.

(2) The identification service provider shall provide an opportunity to submit a notification as set out in subsection 1 at any time. Upon receipt of the notification, the identification service provider shall immediately cancel the identification device or prevent its use.

(3) The identification service provider shall properly and without delay enter in its system the information about the time of cancellation or prevention of use. The holder of the identification device has the right to request proof of submitting a notification mentioned in subsection 1. Such request must be made within 18 months from the notification.

(4) The system shall be designed to allow a service provider using identification service to easily verify the information entered at any time. However, such obligation to create an opportunity to verify information does not exist if the use of the identification device can be prevented or blocked by technical means.

(5) A service provider using identification service shall check the systems and registers maintained by the identification service provider for potential cancellations or restrictions to use in connection with the use of the identification device. However, no checking is needed, if the use of the identification device can be prevented or blocked by technical means.

(6) If the identification service is based on certificates and information on cancelled devices is given via Block Lists, the certification service provider may store the data obtained from the Block List for the purpose of verifying the validity of a certificate. Alternatively, the certification service provider may store the Block List.

Section 26

Identification service provider's right to cancel or prevent the use of an identification device

(1) In addition to the provisions of section 25, the identification service provider may cancel or prevent the use of a identification device if:

- 1) the identification service provider has reason to believe that someone other than the person to whom the device was issued is using it;
 - 2) the identification device is obviously defective;
 - 3) the identification service provider has reason to believe that the safe use of the device is at risk;
 - 4) the identification device holder is using the identification device contrary to the agreed terms of use; or
 - 5) the identification device holder has died.
- (2) The identification service provider shall notify the holder as soon as possible about the cancellation or prevention of use of the identification device, as well as the time of and reasons for such action.
- (3) The identification service provider shall restore the ability to use the identification device or give the identification device holder a new device immediately after removal of reasons referred to in subsection 1(2 and 3).

Section 27

Restrictions to the identification device holder's liability for unauthorized use of the identification device

- (1) The identification device holder shall be liable for unauthorized use of the identification device only if:
- 1) he or she has transferred the device to someone else;
 - 2) the loss of the device or unauthorized possession or use is the result of the holder's gross negligence, or
 - 3) the holder has failed to notify the identification service provider or a designated party that the device has been lost, is in the unauthorized possession of another person or of any unauthorized use immediately upon detection of this fact.
- (2) However, the identification device holder shall not be liable for unauthorized use:
- 1) to the extent that the identification device has been used after the holder has reported to the identification service provider of the loss, unauthorized possession or use of the device;
 - 2) if the identification device holder has not been able to report the loss, unauthorized possession or use of the device without undue delay after detecting it, because the identification service provider has failed to perform its obligation referred to in section 25(2) to ensure that the holder can report at any time; or
 - 3) a service provider using identification services has failed to check the restrictions on use or prevention or blocking of the devices as set out in section 18(4) or 25(5).

Chapter 4

Electronic signature

Section 28

Devices for creating safe signatures

- (1) A device for creating safe signatures shall be able to ensure in a sufficiently reliable manner that:

- 1) the data used for the creation of signatures is unique and that it will remain confidential;
 - 2) the data used for the creation of signatures cannot be deduced from any other data;
 - 3) the signatures are protected against forgery;
 - 4) the signatory will be able to protect the data used for the creation of a signature against use by others; and
 - 5) a device for creating safe signatures will not alter the information to be signed nor will it prevent the information from being presented to the signatory prior to signing.
- (2) Devices for creating a signature are deemed to meet the requirements set out in subsection 1, provided that:
- 1) they comply with the generally acknowledged standards confirmed by the European Commission and published in the Official Journal of the European Union; or
 - 2) the notified body that has been appointed to perform the duty of assessing these requirements, which is based in Finland or in another member state of the European Economic Area, has approved them.

Section 29

Notified bodies

- (1) The Finnish Communications Regulatory Authority may appoint, for a fixed period of time, notified bodies that are given the duty to assess whether the devices for creating signatures meet the requirements specified in section 28(1). Notified bodies can be private or public institutions.
- (2) For a notified body to be appointed it is required that:
- 1) the notified body in question is independent, both functionally and financially;
 - 2) its operations are appropriate, reliable and non-discriminating;
 - 3) it has the necessary financial resources for proper operation and for covering possible liabilities;
 - 4) it has at its disposal adequate skilled and unbiased personnel; and
 - 5) it has at its disposal premises and equipment required for the activity in question.
- (3) The Finnish Communications Regulatory Authority appoints the notified bodies based on applications. The application must include the applicant's contact data and trade register excerpt or similar statement, a statement explaining how the applicant's operation meets the requirements set out in subsection 2. If needed, the Finnish Communications Regulatory Authority will provide instructions on information to be included in the application and how to submit them to the Finnish Communications Regulatory Authority.
- (4) The Finnish Communications Regulatory Authority monitors the operations of the notified body. Should the notified body fail to meet the statutory requirements, or act contrary to the regulations, the Finnish Communications Regulatory Authority shall revoke the decision by which the appointment was made. The notified body shall notify the Finnish Communications Regulatory Authority of any changes in its operations that may have an effect on the requirements on the basis of which the notified body has been appointed.
- (5) In its assessment activities the notified body may enlist the assistance of subcontractors. The notified body is also responsible for the work of its subcontractors.

Section 30

Qualified certificates

(1) A qualified certificate means a certificate that meets the requirements set out in subsection 2 and has been issued by a certification service provider that meets the requirements set out in sections 33 to 38.

(2) Qualified certificates must include:

- 1) an indication of the fact that the certificate is a qualified certificate;
- 2) details of the certifier and the state in which the certifier is based;
- 3) the signatory's name, or a pseudonym that makes it clear that it is a pseudonym;
- 4) the signature verification data which corresponds to the data in the signatory's possession used for creating the signature;
- 5) the period of validity of the certificate;
- 6) a symbol identifying the certificate;
- 7) the certification service provider's advanced electronic signature;
- 8) potential limits on use of the qualified certificate: and
- 9) any special information on the signatory, should this be necessary regarding the way the certificate will be used.

(3) If a certification service provider offering qualified certificates also offers identification services referred to in Chapter 3, the requirements of subsection 1 are also deemed to meet the data content requirements of section 19(1).

Section 31

Qualified certificates by certification service providers other than those based in Finland

(1) A qualified certificate by certification service providers other than those based in Finland is deemed to meet the requirements specified in this Act, provided that:

- 1) the certification service provider is based in a member state of the European Economic Area and the certificate meets the requirements applicable to qualified certificates in the country where the certification service provider is based;
- 2) the certification service provider is a member of a voluntary accreditation system in a member state of the European Economic Area and meets the statutory national requirements in the country in question for the entering into force of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, hereinafter the Electronic Signature Directive;
- 3) the certificate is guaranteed by a certifier that is based in a member state of the European Economic Area and meets the statutory national requirements in the country in question for the entering into force of the Electronic Signature Directive; or
- 4) the certificate or certification service provider is acknowledged on the basis of a bilateral or multilateral agreement between the European Community and one or several third countries or international organizations.

Section 32

Notification of commencing operations

(1) A certification service provider offering qualified certificates shall, prior to commencing to offer such qualified certificates, submit a written notification to the

Finnish Communications Regulatory Authority. This notification should include the provider's name and contact information, as well as information used to verify the fulfillment of requirements set out in sections 30 and 33 to 38. The Finnish Communications Regulatory Authority may issue regulations on details of data to be submitted and on their submission to the Finnish Communications Regulatory Authority.

(2) The Finnish Communications Regulatory Authority shall, immediately after receiving the notification, forbid the certification service provider from offering its certificates as qualified certificates if the certificate does not meet the requirements specified in section 30(2) or if the service provider fails to meet the requirements set out in sections 33 to 38.

(3) In the event that the details referred to in subsection 1 have changed, the certifier shall notify in writing the Finnish Communications Regulatory Authority of this without delay.

(4) The Finnish Communications Regulatory Authority keeps a public register of certification service providers who issue qualified certificates.

(5) Certification service providers offering qualified certificates may submit a notification referred to in section 10 if they wish to offer identification services in addition to qualified certificates.

Section 33

General obligations of certification service providers offering qualified certificates

(1) A certification service provider shall have at its disposal adequate technical skills and financial resources in view of the extent of the activity undertaken. A certifier is responsible for all the sub-areas of the certification activity, including the reliability and functionality of any services and products that may have been produced by subcontractors on behalf of the certification service provider.

(2) A certification service provider should:

- 1) ensure that its personnel have adequate expertise, experience and competence;
- 2) ensure that it has adequate financial resources for proper operation and for covering possible liabilities;
- 3) keep accessible to the general public details of the certificate and certification activities on the basis of which it will be possible to assess the operations and the reliability of the certification service provider; and
- 4) safeguard the confidentiality of the data used for creating signatures in cases where the certification service provider itself produces the data.

(3) The certification service provider shall not store or copy any data used for creating signatures that has been handed over to a signatory.

Section 34

Reliability of hardware and software

(1) The certification service provider offering qualified certificates shall make sure that all the systems and hardware and software it uses are safe, reliable and protected against alterations and forgeries.

(2) A device or software used in connection with electronic signatures is deemed to meet the requirements specified in subsection 1 if the devices or software in question

comply with the confirmed standards of the European Communities as published in the Official Journal of the European Communities.

Section 35

Issuing a qualified certificate

(1) The certification service provider shall carefully check the applicant's identity as well as any other data regarding the identity of the applicant required for issuing and maintaining the qualified certificate. A certification service provider offering qualified certificates shall personally identify the applicant. The certification service provider shall treat its customers in a non-discriminatory manner and the applicants for qualified certificates fairly when concluding an agreement.

(2) Prior to entering into an agreement, the certification service provider offering qualified certificates shall disclose to the applicant for a qualified certificate its terms of use, including potential restrictions on use, information on voluntary accreditation systems, government monitoring of the certification transactions, as well as complaint and dispute settlement procedures. The information must be provided to the applicant for a qualified certificate in writing and in a form that is easy to understand.

Section 36

Cancellation of qualified certificates

(1) A signatory shall without delay request that a certification service provider cancel a qualified certificate if the signatory has a weighty reason to suspect unauthorized use of data for creating a signature.

(2) The certification service provider offering qualified certificates shall immediately cancel a qualified certificate should the signatory so request. A request is deemed to have reached the service provider when it has been at its disposal in such a way that the request can have been dealt with.

(3) A qualified certificate can also be cancelled if there are any special reasons for doing so. The signatory shall always be notified of the cancellation and cancellation time of a qualified certificate.

Section 37

Registers kept by certification service providers offering qualified certificates

(1) A certification service provider offering qualified certificates shall maintain a register of qualified certificates (*certificates register*). The following must be entered in the register:

(2)

1) the data content of the qualified certificate as set out in section 30(2);
2) the applicant's personal data referred to in section 35(1), including information about the applicant's identification method used in issuing the qualified certificate and necessary information on the file possibly used in identification; and

3) data referred to in section 39 relating to checks made using the Block List on the validity of certificates, if the certification service provider issuing qualified certificates uses the right to store pursuant to section 39.

(3) A certification service provider offering qualified certificates should ensure that the party relying on an advanced electronic signature certified by a qualified certificate has access to the data content of the certificate as specified in section 30(2). Data referred to in subsection 1(3) above does not have to be stored in the certificate register if the certification service provider can guarantee in some other way that the party relying on the certificate can provide reliable proof of having checked the Block List properly.

(4) The certification service provider shall also maintain a register of canceled qualified certificates (*Block List*) that is available to parties relying on qualified certificates. Details of all cancellations of qualified certificates, as well as the exact time and date of cancellation must be immediately entered in the Block List.

(5) The information in subsections 2 and 3 above must be available at all times.

Section 38

Storing certificates register data

(1) A certification service provider offering qualified certificates shall store certificates register data properly and reliably for 10 years after expiration of the certificate.

(2) If a certification service provider offering qualified certificates also offers strong electronic identification, it may store data in all respects as referred to in subsection 1, notwithstanding section 24.

Section 39

Storing information related to verifying the validity of certificates

A certification service provider offering qualified certificates may store data received from Block Lists for verifying the validity of a certificate. Stored data may only be used for the purpose of invoicing certificates or verification of legal transactions executed with the help of an electronic signature.

Section 40

Liability for any unauthorized use of data used for creating signatures

(1) The signatory is liable for damages from any unauthorized use of data that is used for creating an advanced electronic signature certified by a qualified certificate until the request for canceling the certificate has been received by the certification service provider, as set out in section 36(2).

(2) The user shall only be responsible pursuant to subsection 1 if:

- 1) he or she user has given out the creation data to others;
- 2) the unauthorized use of the creation data is the result of the user's gross negligence; or
- 3) he or she has lost possession of the data in other ways than set out in paragraph 2, and has failed to request the cancellation of the qualified certificate as provided in section 36(1).

Section 41

Liability for damages of a certification service provider offering qualified certificates

(1) A certification service provider offering qualified certificates shall be liable for damages to someone relying on the qualified certificate if:

- 1) data marked on the qualified certificate was incorrect at the time of issue of the certificate;
- 2) the qualified certificate does not include the details specified in section 30(2);
- 3) the person identified in the qualified certificate did not, at the time of issue of the certificate, have in his or her possession the data used for creating the signature and corresponding to the signature verifying data as stated or defined in the certificate;
- 4) the creation and verification data created by a certification service provider or its subcontractor are inconsistent; or
- 5) the certification service provider or its subcontractor did not cancel the qualified certificate as provided in section 36.

(2) The certification service provider shall be released from the obligation provided in subsection 1 if it can show that the damage was not caused by its own or its subcontractor's negligence.

(3) The certification service provider shall not be liable for any damages caused by a qualified certificate being used contrary to restrictions related to its use.

(4) Otherwise, provisions regarding a certification service provider's liability to provide indemnity shall be issued in the Indemnity Act (412/1974).

(5) The provisions of this section shall also apply to certification service providers who ensure to the general public that a certificate is a qualified certificate.

Chapter 5

Monitoring by competent authorities

Section 42

General guidance and monitoring

(1) General guidance and monitoring of strong electronic identification and electronic signatures is the responsibility of the Ministry of Transport and Communications.

(2) It is the responsibility of the Finnish Communications Regulatory Authority to monitor compliance with this Act, excluding section 1(3). If needed, the Finnish Communications Regulatory Authority will issue technical orders regarding reliability and data security requirements for identification service providers and certification service providers offering qualified certificates.

(3) It is the responsibility of the Data Protection Ombudsman to monitor compliance with the provisions of this Act regarding personal data.

Section 43

Right to obtain information

(1) Notwithstanding secrecy provisions, the Finnish Communications Regulatory Authority has the right to obtain from identification service providers and certification

service providers offering qualified certificates, notified bodies referred to in section 29 and their subcontractors the necessary information for performing tasks provided in section 42.

(2) In performing his duties, the Data Protection Ombudsman has the right to obtain data as defined in the Personal Data Act.

Section 44

Collaboration between authorities and the right to release data

(1) In addition to the provisions of the Act on the Openness of Government Activities (621/1999), the Finnish Communications Regulatory Authority and the Data Protection Ombudsman have the right to release information to the Financial Supervisory Authority required for the performance of its tasks, notwithstanding any secrecy provisions. Notwithstanding any secrecy provisions the Financial Supervisory Authority has the same right to release information to the Finnish Communications Regulatory Authority and the Data Protection Ombudsman required for the performance of their tasks provided in this Act.

(2) In performing duties according to this Act, the Finnish Communications Regulatory Authority and the Data Protection Ombudsman shall collaborate appropriately with the Financial Supervisory Authority, the Finnish Competition Authority and the Consumer Agency as required.

Section 45

Administrative constraints

(1) Should anyone break this Act or infringe any regulations issued under it, the Finnish Communications Regulatory Authority may order such persons to rectify their failure or neglect. The decision may be reinforced by an imposition of a penalty payment or a threat that the activity may be discontinued either in part or in full, or that the measure which has been failed to carry out may be ordered to be carried out at the person's expense. Provisions on penalty payments, threats of discontinuance and threats of action are issued in the Penalty Payment Act (1113/1990).

(2) The costs of any measures that have been performed by order to carry them out will be paid from government funds and collected from the person guilty of negligence, in the order provided in the Act on implementing taxes and fees (706/2007).

Section 46

Right to inspect

(1) The Finnish Communications Regulatory Authority has the right to perform or commission an inspection of the identification service provider and its services, notified body referred to in section 29 and its services, and certification service provider offering qualified certificates and its services, if it has reason to suspect that they have materially breached this Act or provisions issued under it.

(2) The Finnish Communications Regulatory Authority shall audit the certification service provider offering qualified certificates and its services on a yearly basis.

(3) The Finnish Communications Regulatory Authority shall commission an auditor to perform an audit referred to in subsections 1 or 2 above. The person performing the audit has the right to inspect the hardware and software of the identification service provider and the certification service provider offering qualified certificates and their subcontractors, to the extent relevant to monitoring the compliance with the provisions of this Act or regulations issued under it.

(4) Identification service providers, certification service providers offering qualified certificates and their subcontractors shall, for the purpose of audits, give auditors referred to in subsection 3 above access to production, business and storage areas that are outside the inviolability of home areas.

(5) The Finnish Communications Regulatory Authority has the right to receive help from the police in performing audits under this section.

(6) In performing his or her duties, the Data Protection Ombudsman has the right to audit data as defined in the Personal Data Act.

Section 47

Fees payable to the Finnish Communications Regulatory Authority

(1) The identification service provider or service providers association submitting a notification referred to in section 10 above shall pay the Finnish Communications Regulatory Authority a registration fee of 5,000 euros. In addition, the identification service provider or service providers association shall pay the Finnish Communications Regulatory Authority an annual monitoring fee of 10,000 euros.

(2) A certification service provider offering qualified certificates who has submitted a notification referred to in section 32 above shall pay the Finnish Communications Regulatory Authority a registration fee of 5,000 euros. A certification service provider offering qualified certificates shall also pay the Finnish Communications Regulatory Authority an annual monitoring fee of 40,000 euros. If a certification service provider offering qualified certificates also submits a notification referred to in section 10, it shall pay a registration fee referred to in subsection 1.

(3) A notified body appointed in accordance with section 29 above shall pay the Finnish Communications Regulatory Authority an appointment fee of 10,000 euros. The notified body shall also pay the Finnish Communications Regulatory Authority an annual monitoring fee of 15,000 euros.

(4) The registration fee, appointment fee and the monitoring fee equal the expenses incurred by the Finnish Communications Regulatory Authority in performing its duties under this Act, with the exception of duties mentioned in section 46(1). The monitoring fee is payable in full for the first year of operations, even if operations do not start until mid-year. The monitoring fee will not be refunded, even if operations stop mid-year.

(5) An obligation to pay a registration fee, appointment fee or monitoring fee shall be stipulated by the Finnish Communications Regulatory Authority. Decisions of the Finnish Communications Regulatory Authority regarding the payment obligation may be appealed according to section 49(1). Further provisions on the implementation of the fees may be given by a Ministry of Transport and Communications decree.

(6) Registration fees, appointment fees and monitoring fees may be collected without a judgment or decision in the order specified by the Act on implementing taxes and fees. If payment is not made by the due date, annual interest on delayed payments according to interest rate referred to in section 4(1) of the Interest Act (633/1982) will be levied on the outstanding amount. Instead of interest on delayed

payments the authorities may collect a late payment fee of five euros if the interest on delayed payment is smaller than this.

(7) If an identification service provider's operation needs to be audited based on section 46(1), the identification service provider shall be charged for the expenses incurred as laid down in the Act on Criteria for Charges Payable to the State.

Chapter 6

Miscellaneous provisions

Section 48

Penal provisions

Provisions on penalties for person register related crimes are provided in Chapter 38(9) of the Criminal Code (39/1889), and for person register related offences in section 48(2) of the Personal Data Act.

Section 49

Appeals

(1) Provisions regarding appeals against decisions of the Finnish Communications Regulatory Authority made pursuant to this Act are issued in the Administrative Judicial Procedure Act (586/1996).

(2) In its decision, the Finnish Communications Regulatory Authority may order that the decision must be complied with before it becomes legally valid. However, an appeal authority may forbid the decision to be enforced before the appeal has been heard.

(3) Provisions regarding appeals against the decision of the Data Protection Ombudsman are provided in the Personal Data Act.

Chapter 7

Entry into force

Section 50

Entry into force

(1) This Act will enter into force on 1 September 2009.

(2) This Act repeals the Act of 24 January 2003 on Electronic Signatures (14/2003). The regulations of the Finnish Communications Regulatory Authority pursuant to the repealed act shall be in force until new regulations have been issued under this Act.

(3) Measures necessary for the implementation of this Act may be undertaken before the Act's entry into force.

Section 51

Transitional provisions

(1) Identification service providers shall give the Finnish Communications Regulatory Authority a notification referred to in section 10 no later than six months after the Act's entry into force. During that time, an electronic identification service and electronic identification service provider that falls within the scope of section 1 and meets the requirements of section 2(1 and 4) shall be deemed strong electronic identification service and strong electronic identification service provider.

(2) Identification devices issued prior to the entry into force of this Act or during the transition time referred to in subsection 1 are deemed strong electronic identification devices if the certification service provider submits a notification referred to in section 10 within the timeframe referred to in subsection 1. The identification service and identification service provider must thus meet all requirements set out for them in this Act, with the exception of the requirements of section 17.

(3) If identification service providers have entered into an agreement referred to in section 17(2) on the possibility of relying on each other for initial identification, and the service provider who issued the identification devices used in the initial identification has not made a notification referred to in section 10 within the timeframe referred to in subsection 1, initial identification as regards identification devices issued in such a way shall be made without delay and as referred to in section 17.

(4) A certification service provider offering qualified certificates that has submitted a notification according to section 9(1) of the Act on Electronic Signatures, and continued its business without interruption until this Act's entry into force, does not have to make a new notification pursuant to section 32(1). A certification service provider offering qualified certificates may thus submit to the Finnish Communications Regulatory Authority an informal written notification that it will continue its operations as usual. At the time of the entry into force of this Act, a certification service provider offering qualified certificates shall pay a certification fee referred to in section 12 of the Decree of the Ministry of Transport and Communications on Certain Fees of the Finnish Communications Regulatory Authority until 31 December 2009, regardless of the date of submitting a written notification.
