Translation from Finnish
Legally binding only in Finnish and Swedish
Ministry of Transport and Communications, Finland

Act on Strong Electronic Identification and Electronic Trust Services

(617/2009; amendments up to 412/2019 included)

By decision of Parliament, the following is enacted:

Chapter 1
General provisions

Section 1 (533/2016)
Scope of application

This Act lays down provisions on strong electronic identification and on the offering of identification services to service providers, the general public and other providers of identification services.

This Act lays down provisions on the monitoring of the provisions in the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, hereinafter *EU Regulation on Electronic Identification and Trust Services*, and also lays down provisions supplementing the Regulation. Furthermore, this Act lays down provisions on the assessment of conformity of identification and trust services.

This Act is applied to cross-border identification systems notified to the European Commission only unless otherwise provided in the EU Regulation on Electronic Identification and Trust Services.

This Act does not apply to the provision of identification services within an organization. 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.

Section 2 (1009/2018)
Definitions

For the purposes of this Act:

1) *strong electronic identification* means the identification and verification of the authenticity and correctness of the identifying information of a person, legal person or a natural person representing a legal person by electronic means that fulfils the requirements of assurance level substantial referred to in Article 8 (2 b) of the EU Regulation on Electronic Identification and Trust Services or assurance level high in Article 8 (2 c).

2) *identification means* means an electronic identification means referred to in Article 3(2) of the EU Regulation on Electronic Identification and Trust Services.

3) *identification service provider* means a provider of an identification broker service or a provider of an identification means.

4) *provider of an identification means* means a service provider that offers or issues electronic identification means for strong electronic identification to the general public and offers in the trust network their electronic identification means for a provider of an identification broker service to be distributed.

5) *provider of an identification broker service* means a service provider that forwards strong electronic identification events to a party that relies on electronic identification;

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

7) *initial identification* means the verification of the identity of the applicant for an identification means in connection with the issuing of the means;

8) *certificate* means an electronic verification that confirms the identity or confirms the identity and links the data in a trust service to the user of the trust service, and that can be used for strong electronic identification and trust services;

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

10) *trust network* means a network of identification service providers that have submitted a notification to the Finnish Transport and Communications Agency;

11) *conformity assessment body* means a body approved by the Finnish Transport and Communications Agency and referred to in Article 2(13) regulation (EC) No 765/2008 of the European Parliament and of the Council setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, which has been accredited in accordance with the Regulation.

In this Act, electronic signature, trust service, advanced electronic signature, electronic identification scheme and a relying party mean the same as in Article 3 of the EU Regulation on Electronic Identification and Trust Services.

Chapter 2
Binding nature of the Act and processing of personal data (533/2016)

Section 3
Binding 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.

Any contractual terms between identification service providers that differ from the provisions of this Act are deemed void. (412/2019)

Section 4 (533/2016)

Section 4 was repealed by Act 533/2016.

Section 5 (533/2016)

Section 5 was repealed by Act 533/2016.

Section 6 (533/2016)
Processing of personal data

An identification service provider may process necessary personal data on the grounds referred to in section 8 subsection 1 paragraphs 1 and 2 of the Personal Data Act (523/1999) within the course of issuing and maintaining the identification means and performing the authentication event. On the same grounds, a certification service provider offering trust services may process personal data needed for issuing and maintaining certificates and collect personal data from the person himself or herself.

When offering an identification broker service, the provider of an identification broker service has the right to disclose personal data to the party relying on electronic identification, if the relying party has a statutory right to process personal data.

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 subsection 1 paragraph 1 of the Personal Data Act.

When verifying the identity of an applicant, a provider of an identification service and a certification service provider offering trust services shall request the personal ID code of the applicant. An identification service provider and a certification service provider providing trust services 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 means or certificate only if the data content of the means 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.

Further provisions on the processing of personal data are laid down in section 19, section 24 and the Personal Data Act.

Section 7 (139/2015)
Use of data stored in the Population Information System

The provider of an identification means and a certification service provider offering a trust service must use the Population Information System to obtain and update the data they need in order to be able to offer a service for identifying a natural person. The identification service provider shall also ensure that the data it needs for the purpose of offering identification services are up-to-date with the data in the Population Information System. (533/2016)

Data from the Population Information System is released as 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 (150/1992).

Section 7 a (533/2016)
Using the data in the Business Information System

The provider of an identification means and a certification service provider offering a trust service must use the Business Information System to obtain and update the data they need in order to be able to offer a service for identifying a legal person. The identification service provider shall also ensure that the data it needs for the purpose of offering identification services are up-to-date with the data in the Business Information System.

Section 7 b (1009/2018)
Information on the validity of a passport or a personal identity card

An identification service provider has the right to obtain via an interface or other electronic means and without prejudice to secrecy provisions information from the information system of the Police about the validity of a passport or a personal identity card used for initial identification.

Chapter 3
Strong electronic identification

Section 8 (533/2016)
Requirements posed on the electronic identification scheme

An electronic identification scheme must fulfil the following requirements:

1) The identification means shall be based on initial identification according to section 17 and section 17 a, where the relevant data can be verified afterwards as set out in section 24;

2) The identification means can be used for unambiguously identifying the holder of the identification means in a way that, at a minimum, fulfils the requirements on assurance level substantial laid down in sections 2.1.2, 2.1.3 and 2.1.4 of the Annex to the Commission Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, hereinafter *the Act on Level of Assurance in Electronic Identification*.

3) The identification means can be used verify that only the holder of the identification means can use the means in a way that, at a minimum, meets the conditions for assurance level substantial laid down in sections 2.2.1 and 2.3 of the Annex to the Act on Level of Assurance in Electronic Identification.

4) The identification scheme is reliable and safe so that, at a minimum, it meets the conditions for assurance level substantial laid down in sections 2.2.1, 2.3.1 and 2.4.6 of the Annex to the Act on Level of Assurance in Electronic Identification and takes into account the threats to the information security of the technology available at the time, and that the premises used for providing an identification service are safe in compliance with the provisions laid down in section 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification.

5) Information security management is ensured so that, at a minimum, the conditions for assurance level substantial laid down in the introduction to section 2.4 and in sections 2.4.3 and 2.4.7 of the Annex to the Act on Level of Assurance in Electronic Identification are met.

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 means holder or only a limited amount of personal data.

Section 8 a (533/2016)
Authentication factors used in the identification means

The identification means must use at least two of the following authentication factors:

1) a knowledge-based authentication factor that the subject is required to demonstrate knowledge of;

2) a possession-based authentication factor that the subject is required to demonstrate possession of;

3) an inherent authentication factor that is based on a physical attribute of a natural person.

Every identification means must use a dynamic authentication referred to in section 2.3.1 of the Annex to Act on Level of Assurance in Electronic Identification that changes in every new authentication event between the person and the system certifying his or her identity.

Section 9
Requirements posed on the identification service provider

Any legal persons operating as an identification service provider or any natural persons operating for such 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 have reached the age of majority;

2) they must not have declared bankruptcy; and

3) their operating capacity must not be restricted.

(533/2016)

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.

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 (1009/2018)
An identification service provider's obligation to notify commencement of operations

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 Transport and

Communications Agency. Such notification may also be submitted by a consortium of identification service providers, if such services provided can be deemed as one and the same identification service.

The notification shall contain:

1) name of the service provider;

2) complete contact information of the service provider;

3) information about the services to be provided;

4) reports on the fulfilment of the criteria laid down for the applicant and the applicant's operations laid down in section 8, 8 a, 9, 13 and 14.

5) an assessment report on the independent audit drawn up by conformity assessment body, other external assessment body or an internal assessment body pursuant to section 29;

6) other information relevant to supervising.

The identification service provider shall notify the Finnish Transport and Communications Agency 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.

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 section.

Section 12 (1009/2018)
Register related to an identification service provider

The Finnish Transport and Communications Agency maintains a public register of identification service providers who have submitted a notification according to section 10, and their services.

Upon receipt of notice referred to in section 10, the Finnish Transport and Communications Agency 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 Transport and Communications Agency may ask the service provider to correct them within a specified period.

Section 12 a (412/2019)
Trust network of identification service providers

By submitting a notification to the Finnish Transport and Communications Agency in accordance with section 10, an identification service provider becomes a member of a trust network.

An identification means provider shall offer an access right to the providers of identification broker services so that they can forward authentication events to the party relying on electronic identification. The identification means provider shall draw up delivery terms and conditions concerning access right to their identification service and must use them when making agreements with providers of identification broker services. The terms and conditions of access right shall be compliant with this Act, reasonable and non-discriminatory. The provider of an identification means shall accept a request by a provider of an identification broker service concerning the making of an agreement in accordance with the terms and conditions of delivery and shall grant an access right to the identification service immediately, in any case no later than within a month of the submission of the request. The provider of an identification means may refuse to make an agreement only if the provider of an identification broker service acts in violation of this Act or regulations issued pursuant to it or if another important justification for the refusal exists.

Identification service providers must collaborate to ensure that the technical interfaces of the members of a trust network are interoperable and that they enable the provision of interfaces that implement commonly known standards to the relying parties.

An identification service provider shall implement maintenance, alteration and information security measures in a way that causes as little harm as possible to other identification service providers, users and relying parties. In addition to the provision laid down in section 25 and 26, an identification service provider may temporarily suspend the provision of an identification service or restrict access to it without the consent of another identification service provider, if it is necessary for the successful completion of a measure referred to above. The suspension and alteration shall be effectively communicated to the other identification service providers whose services it may affect.

An identification service provider may use data on another identification service provider it has obtained pursuant to an access right transfer or section 16, but only for the purpose for which they were disclosed to the identification service provider. The only people who may process the data are those in the service of the identification service provider or acting on behalf of it who absolutely need the data in their work. Information shall also otherwise be handled in such a way that the business secrets of another identification service provider are not endangered. An identification service provider that causes damage to another identification service provider by acting contrary to this subsection has an obligation to compensate any damage caused by the action.

Further provisions on the administrative procedures, technical interfaces and administrative responsibilities of the trust network are issued by Government Degree.

Section 12 b (412/2019)
Delivery terms and conditions on the access right to the identification service and the duty of disclosure of the provider of an identification means

The provider of an identification means shall publish the delivery terms and conditions of the right to use their identification service and other essential information related to the transfer of an access right and the interoperability of identification services on their website. The provider of an identification means shall publish at least the following information:

1) a description of the identification means, including information on the available data identifying a person pursuant to the Annex of the Commission Implementing Regulation EU 2015/1501 of the on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the

European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market;

2) any restraint or restrictions associated with the identification means referred to in section 18 and information on how such preclusions or restrictions are known to the relying party or can be detected by them, or information about the technical implementation of a restriction.

3) a description of the technical interfaces and testing arrangements of authentication event forwarding to the extent that they do not contain business secrets or information that jeopardises information security;

4) price of an authentication event;

5) service level offered;

6) information on how maintenance and alteration actions are communicated;

7) description of the invoicing procedure;

8) terms and conditions on liability for damages;

9) terms and conditions of using trademarks and other immaterial property rights;

10) principles of the processing of personal data as a controller specified in Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

11) potential grounds for altering the delivery terms and conditions unilaterally;

12) method of dispute resolution;

13) any other terms and conditions critical for the operation of the trust network.

Section 12 c (412/2019)
Charges for the access right to the identification service

The provider of an identification broker service shall pay a fee for the right to use the identification service; the maximum amount of the fee is 3 cents per forwarded authentication event. The fee covers all person identification data associated with an electronic identification means. The Finnish Transport and Communications Agency evaluates the amount of the fee annually.

No other fees may be charged for the right to use the identification service. Invoicing and all access rights to the interfaces, functions, services, software and information systems of the identification means provider that are needed to forward the identification to the relying party shall be included in the charges laid down in subsection 1.

Section 12 d (412/2019)
Liability for damages among the members of a trust network

An identification service provider who intentionally or out of neglect breaches the obligations laid down in section 12 a, subsection 2 or 3 or regulations issued pursuant to subsection 6, section 12 b or 12 c or section 17 subsection 4, shall be liable for compensating the damage they have caused to another identification service provider.

Compensation for damage consists of compensation for costs, the price difference and other direct financial losses caused by the identification service provider's activities referred to in subsection 1.

The compensation can be adjusted if full liability for damages is considered an unreasonable burden with regard to the nature of the offence, the extent of damage, the circumstances of the parties and other factors.

The right to compensation expires if the action for damages is not brought within three years of the date on which the identification service provider received or should have received the information on the damages.

In handling the action for damages referred to in subsection 1, the court may request an opinion on the matter from the Finnish Transport and Communications Agency.

Section 13
General obligations of an identification service provider

The storage of data, the personnel and subcontracted services used by an identification service provider in association with identification shall, at a minimum, meet the requirements laid down for assurance level substantial in sections 2.4.4 and 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification. Moreover, the identification service provider shall have in place an effective plan for terminating the identification service. (533/2016)

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.

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

The identification service provider is responsible for the reliability and functionality of services and products provided by persons contributing to the identification service process.

Section 14 (533/2016)
Identification principles

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, the identification service provider shall define how they implement the identification referred to in section 17 and 17 a when issuing an identification means.

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

1) the service provider;

2) services to be provided and their prices;

3) all terms and conditions that apply;

4) data protection principles associated with the service;

5) the most important cooperation partners of the service provider;

6) conformity assessment pursuant to section 29;

7) other relevant information on the basis of which the operation and trustworthiness of the service provider can be assessed.

If the identification means 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.

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

Section 15
Duty of the provider of an identification means to provide information before making an agreement (533/2016)

Prior to entering into an agreement with an applicant for an identification means, the service provider shall provide the applicant with information about: (533/2016)

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) possible limits of liability;

6) complaint and dispute settlement procedures;

7) possible restraints and restrictions on use referred to in section 18; and

8) other possible terms of use related to the identification means.

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

Provisions on the duty of providing information regarding the processing of personal data are issued in the Personal Data Act.

Section 16 (412/2019)
Notifications of the identification service provider concerning threats or disruptions to their operations and protection of data

Notwithstanding any secrecy provisions, an identification service provider shall inform the parties relying on their identification service, holders of identification means, other agreement parties operating in the trust network and the Finnish Transport and Communications Agency without undue delay of all significant threats or disruptions to the operation of the service, information security or the use of an electronic identity. The notification shall also include information about measures the parties involved have for use to counter such threats and risks, as well as the estimated expenses incurred by these measures.

An identification service provider can, without prejudice to secrecy provisions, notify all members of a trust network of the threats and disruptions referred to in subsection 1 and of service providers of whom there is reason to believe that they are seeking unauthorised financial gain, giving false or misleading information that is significant or processing personal data illegally.

The Finnish Transport and Communications Agency may forward information between the parties of a trust network on behalf of the notifying party by technical means without prejudice to the provisions in the Act on the Openness of Government Activities (621/1999).

Section 17 (1009/2018)
Identifying a natural person applying for an identification means

The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person's identity may be based on a document issued by an authority showing the person's identity or a strong electronic identification means referred to in this Act. In addition, the proofing of an identity may be based on a procedure used at an earlier date by a public or private entity for a purpose other than the issuing of a strong electronic identification means, which the Finnish Transport and Communications Agency approves pursuant to regulations and regulatory control on the procedure, or pursuant to a confirmation by a conformity assessment body referred to in section 28, subsection 1.

In initial identification that is solely based on a document issued by an authority showing the person's identity, the only acceptable documents are a valid passport or a personal identity card issued by an authority of a member state of the European Economic Area, Switzerland or San Marino. If the identification means provider so desires, they may also verify the identity from a valid passport granted by an authority of another state.

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 means 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.

A provider of an identification means shall enable another provider of an identification means to use a strong electronic identification means issued by the first provider for initial identification when the holder is applying for an electronic means on the same assurance level or lower. The provisions in section 12 a and 12 b on the transfer of the access right to an identification means and the publication of the terms and conditions of delivery also apply to the use of an identification means referred to in this subsection for initial identification. (412/2019)

The provider of an identification means relying on a previous initial identification is liable for damages arising from a potential erroneous initial identification in relation to the party that suffered the damage. (412/2019)

If the provider of an identification means that relies on previous initial identification becomes liable for damages under subsection 5, the provider is entitled to receive compensation for the damage they have suffered from the provider of an identification means that made the error in initial identification, unless the latter party can demonstrate that the damage was not caused by their intention or gross negligence. (412/2019)

The provisions in section 12 c on the fee paid for the forwarding of an authentication event also apply to the use of an identification means referred to in subsection 4 for initial identification. (412/2019)

Subsection 7 as added by Act 412/2019 is temporarily in force between 1 April 2019–31 March 2021. Previous form of wording:

Subsection 7 was repealed by Act 412/2019.

Section 17 a (533/2016)
Identifying a legal person applying for an identification means

The reported identity of a legal person must be verified from the Business Information Register or by means that, at a minimum, meet the requirements laid down for the identity proofing and verifying of a legal person at assurance level substantial laid down in section 2.1.3 of the Annex to the Act on Level of Assurance in Electronic Identification.

Section 18 (412/2019)
Preclusions and restrictions regarding legal transactions

The use of an identification means for legal transactions may be precluded by agreements between the identification service provider, the identification service provider using the service and the identification means holder. Restrictions may also be imposed on legal transactions, either with regard to their purpose or the monetary values involved. The preclusions or restrictions may not be targeted at individual service providers nor may they depend on the provider of an identification broker service that forwards an authentication event.

The identification service provider shall ensure that all parties are aware of the preclusions or restrictions or that they are detectable in a clear and easy to understand way. The identification means 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.

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

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 means. 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

If the identification means 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 certificate holder;

4) the validity period of the certificate;

5) the identifier identifying the certificate;

6) possible 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.

The certification service provider shall ensure that the data content of the certificate is available to the service provider using identification services, if it is necessary for performing authentication.

Section 20
Issuing an identification means (533/2016)

The issuance of an identification means is based on the agreement between the applicant for the identification means 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 means applicants fairly when entering into the agreement.

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

An identification means is always issued to a natural person or a legal person. The binding of a natural person and a legal person to an identification means shall be implemented in accordance with section 2.1.4 of the Annex of the Act on Level of Assurance in Electronic Identification. The

identification means must be person-specific. If needed, data may be linked to the identification means allowing the person, on a case-by-case basis, to represent another natural or legal person. (533/2016)

Section 21 (533/2016)
Delivering the identification means to the applicant

The identification service provider shall deliver the identification means to the applicant as stated in the agreement. The identification service provider must ensure that when the identification means is handed over, it does not become subject to unauthorized possession. The method for ensuring this must meet, at a minimum, the requirements laid down for assurance level substantial in section 2.2.2 of the Annex of the Act on Level of Assurance in Electronic Identification.

Section 22 (533/2016)
Renewal of the identification means

The identification service provider may provide a new identification means without explicit request to the holder only if a previously delivered identification means needs to be replaced. The renewal of the identification means must follow, at a minimum, the requirements laid down for assurance level substantial in section 2.2.4 of the Annex of the Act on Level of Assurance in Electronic Identification.

Section 23
Obligations of the identification means holder

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

The identification means holder shall not make the use of the means available to any other person.

Section 24 (533/2016)
Storage and use of data regarding the authentication event and means

The identification service provider shall store:

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

2) data on preclusions or restrictions on the use of identification means referred to in section 18; and

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

The provider of an identification means shall store the necessary data about the initial identification of an applicant referred to in section 17 and 17 a and the document or electronic identification used therein.

The data referred to above in section 1 subsection 1 shall be stored for five years from the authentication event. Other data referred to above in section 1 subsection 2 shall be stored for five years from the termination of a permanent customer relationship.

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

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, to investigate misuse of personal data as well as upon request by the service provider using identification service or the holder of the identification means. The identification service provider shall store data on processing, the time, reason, and person processing it.

If the service provider only issues identification means (devices):

1) subsection 1, paragraph 1 and subsection 4 do not apply to the provider;

2) The five-year record-keeping period referred to in subsection (3) above will then be calculated from the date the identification means validity expires.

Section 25
Cancellation and prevention of use of identification means

The identification means holder shall notify the identification service provider or a designated party if the identification means has been lost, is in the unauthorized possession of another person or of any unauthorized use immediately upon detection of this fact. (533/2016)

The identification means 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 means or prevent its use. (533/2016)

The identification means 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 means 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. (533/2016)

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 means can be prevented or blocked by technical means.

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 means. However, no checking is needed, if the use of the identification means can be prevented or blocked by technical means.

If the identification service is based on certificates and information on cancelled certificates 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 (533/2016)
Identification service provider's right to suspend or revoke the use of an identification means

In addition to the provisions of section 25, the identification service provider may suspend or revoke the use of an identification means if:

1) the identification service provider has reason to believe that someone other than the person to whom the means was issued is using it;

2) the identification means is obviously defective;

3) the identification service provider has reason to believe that the safe use of the means is at risk;

4) the identification means holder is using the identification means contrary to the agreed terms of use; or

5) the identification means holder has died.

The identification service provider shall notify the holder as soon as possible about the revocation or suspension of use of the identification means, as well as the time of and reasons for such action.

The identification service provider shall renew, reactivate or replace the ability to use the identification means or give the identification means holder a new means immediately after removal of reasons referred to in subsection 1(2 and 3).

Section 27

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

The identification means holder shall be liable for unauthorized use of the identification means only if:

1) he or she has made the use of the identification means available to someone else;

2) the loss of the means 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 means has been lost, is in the unauthorized possession of another person or of any unauthorized use immediately upon detection of this fact.

However, the identification means holder shall not be liable for unauthorized use:

1) to the extent that the identification means has been used after the holder has reported to the identification service provider of the loss, unauthorized possession or use of the means;

2) if the identification means holder has not been able to report the loss, unauthorized possession or use of the means without undue delay after detecting it, because the identification service provider has failed to perform its obligation referred to in section 25 subsection 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 means as set out in section 18 subsection 4 or section 25 subsection 5.

Chapter 4
Assessment of conformity (533/2016)

Section 28 (533/2016)
Conformity assessment bodies

The conformity pursuant to this chapter may be assessed by the following assessment bodies as laid down below:

1) a conformity assessment body;

2) other external assessment body operating in accordance with a commonly used procedure (*other external assessment body*); or

3) an independent assessment body operating within the service provider in accordance with a commonly used standard (*internal assessment body*).

Section 29 (1009/2018)
Conformity assessment of an electronic identification service

An identification service provider must regularly subject their service to an assessment by an assessment body referred to in section 28 to evaluate whether the identification service meets the requirements on interoperability, information security, data protection and other reliability laid down in this Act.

Provisions on the conformity assessment of an electronic identification scheme that must be notified to the European Commission are laid down in the EU Regulation on Electronic Identification and Trust Services and in the Act on Level of Assurance in Electronic Identification.

Provisions on the right of the Finnish Transport and Communications Agency to issue further provisions on the criteria used for assessing the conformity of an identification service are laid down in section 42. In addition to the regulations referred to above in subsection 1 and 2, the Finnish Transport and Communications Agency may order as criteria for assessment regulations or guidelines issued by the European Union or another international decision-making body, published or commonly or regionally applied instructions on information security and commonly used information security standards or procedures.

Section 30 (1009/2018)
Conformity assessment of a national node for electronic identification

The conformity of a national interface connected to the EU's interoperability framework on electronic identification (*national node*) shall be demonstrated by an assessment by a conformity assessment body or other external assessment body.

Provisions on the requirements for a national node are laid down in the Commission Implementing Regulation EU 2015/1501 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market; Provisions on the right of the Finnish Transport and Communications Agency to issue further provisions on the conformity of the national node are laid down in section 42.

Section 31 (1009/2018)
Assessment report

The identification service provider and the Population Register Centre must obtain an assessment report of the conformity assessment and submit it to the Finnish Transport and Communications Agency.

The assessment report is in force for the period specified in the standard that was used in the assessment, but not longer than two years.

Section 32 (1009/2018)
Verifying the conformity of a trust service

A conformity assessment body inspects the conformity of a qualified trust service provider and a qualified trust service pursuant to the provisions of the EU Regulation on Electronic Identification and Trust Services.

Provisions on the right of the Finnish Transport and Communications Agency to issue further provisions on the criteria used for assessing conformity are laid down in section 42. The Finnish Transport and Communications Agency may order as criteria for assessment regulations or guidelines issued by the European Union or another international decision-making body, published or commonly or regionally applied instructions on information security and commonly used information security standards or procedures.

Section 33 (1009/2018)
General requirements applying to the assessment body

The following qualification requirements apply to the assessment body referred to in section 28 above:

1) it is functionally and financially independent of the targets of the assessment;

2) its staff has good technical and professional training and a sufficiently wide-range of expertise in tasks involved in assessment operations;

3) it has the equipment, premises, devices and systems needed to carry out the assessment;

4) it has appropriate directions for its operations and the monitoring of its operations.

Provisions on the right of the Finnish Transport and Communications Agency to issue further regulations on the requirements stated in subsection 1 are laid down in section 42.

The conformity assessment body must demonstrate that it fulfils the requirements laid down in subsection 1, paragraphs 1–3 by an accreditation of a national accreditation body and by following the pertinent provisions of Regulation (EC) No 765/2008 of the European Parliament and of the Council setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 and the Act on Verifying the Competence of Conformity Assessment Services (920/2005).

In its notification pursuant to section 10, the identification service provider shall present a report that the other external assessment body or internal assessment body that assessed its conformity meets the requirements laid down in subsection 1. The fulfilment of the requirements laid down above in subsection 1 paragraphs 1–3 must be demonstrated by means of an accreditation referred to in subsection 3 or by another independent procedure based on a commonly used standard.

An accreditation granted by a foreign accreditation body is equivalent to an accreditation decision referred to in subsection 3 and 4.

Section 34 (1009/2018)
Approval of a conformity assessment body

A conformity assessment body is approved by the Finnish Transport and Communications Agency. An assessment body may be approved for a for a fixed period, if special reasons exists. In the decision on the approval, the Finnish Transport and Communications Agency may set restrictions and terms and conditions concerning the scope, monitoring and operations of the assessment body.

Section 35 (1009/2018)
An application to become a conformity assessment body

The approval of a conformity assessment body is based on an application. Information about the applicant and its operations must be appended to the application so that the fulfilment of the requirements referred to in section 33 can be assessed.

When processing the application, the Finnish Transport and Communications Agency can obtain statements and let external experts assess the application and the information presented therein.

Section 36 (1009/2018)
Certification of qualified electronic signature and electronic seal creation devices

The Finnish Transport and Communications Agency can, upon application, designate private or public certification bodies referred to in Article 30 and Article 39(2) of the EU Regulation on Electronic Identification and Trust Services, the task of which is to certify qualified electronic signature or qualified electronic seal creation devices. A certification body may be designated for a limited period. The application must include the information necessary for processing the application as requested by the Finnish Transport and Communications Agency.

The certification body shall be functionally and financially independent of manufacturers of electronic signature or electronic seal creation devices. It shall have liability insurance or some other corresponding arrangement that is adequate in view of the extent of its activities, and must have at its disposal a sufficient number of professionally skilled personnel and systems, equipment and tools required for its activities.

Section 37 (1009/2018)
Operations of a conformity assessment body and a certification body

A conformity assessment body and a certification body may use external people to assist them in carrying out their task. A conformity assessment body and a certification body are responsible for the work performed by such assisting people.

When attending to the public administrative duties referred to in this Act, a conformity assessment body and a certification body shall comply with the provisions of the Administrative Procedure Act (434/2003), Act on the Openness of Government Activities, the Act on Electronic Services and Communication in the Public Sector (13/2003), the Language Act (423/2003) and the Sami Language Act (1086/2003). When carrying out their tasks referred to in this section, the personnel of the conformity assessment body, the certification body or a subsidiary or subcontractor used by the bodies are subject to the provisions on criminal liability for acts in office. Provisions on liability for damages are laid down in the Tort Liability Act (412/1974).

A conformity assessment body and a certification body must notify the Finnish Transport and Communications Agency of any changes that have an effect on the fulfilment of the conditions of the approval or designation.

Section 38 (1009/2018)
Revocation of the approval of a conformity assessment body or the designation of a certification body

If the Finnish Transport and Communications Agency concludes that the conformity assessment body or the certification body does not fulfil the conditions set for it or acts materially in breach of the regulations, the Finnish Transport and Communications Agency must set a sufficient deadline for the body to correct the problems.

The Finnish Transport and Communications Agency may revoke the approval of an assessment body or the designation of a certification body if the assessment body or the certification body has not corrected their operations by the deadline set pursuant to subsection 1 and the matter involves a material breach or negligence.

Chapter 4 a
Provisions on trust services (533/2016)

Section 39 (533/2016)
Revoking a certificate

If a signatory or a holder of an electronic seal has justified reasons to suspect unauthorised use of the electronic signature or the electronic seal creation data, the signatory or holder of an electronic seal shall, without delay, request the revocation of the certificate from the certification service provider that issued the qualified certificate.

The certification service provider of qualified certificates must revoke the qualified certificate without delay, if requested to do so by the signatory or the holder of an electronic seal. A certificate revocation request is deemed to have reached the certification service provider when it has been at its disposal in such a way that the request can have been dealt with.

Section 40 (533/2016)
Liability for the unauthorised use of a signature or an electronic seal creation data

The signatory and the holder of an electronic seal is liable for the damage caused by unauthorised use of an advanced electronic signature and an electronic seal creation data certified by a qualified electronic certificate, until the certificate revocation request has arrived to the certification service provider as laid down in section 39 subsection 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 control of the creation data in other ways than set out in paragraph 2, and has failed to request the revocation of the qualified certificate as provided in section 39 subsection 1.

Section 41 (533/2016)
Liability of the trust service provider

Provisions on the liability of a trust service provider are laid down in Article 13 of the EU Regulation on Electronic Identification and Trust Services.

The certification service provider offering a qualified certificate is liable for damage caused to the party that trusted the qualified certificate when the damage arises out of the fact that the certification service provider or a person it used to provide assistance has not cancelled the certificate as laid down in section 39. The certification service provider shall be released from the liability if it can show that the damage was not caused by its own negligence or the negligence of a person it used to provide assistance.

Chapter 5
Regulatory supervision

Section 42 (1009/2018)
General guidance and regulations by the Finnish Transport and Communications Agency

General guidance and developing of strong electronic identification and electronic trust services is the responsibility of the Ministry of Transport and Communications.

The Finnish Transport and Communications Agency may issue more detailed regulations on:

1) the requirements for the security and reliability of the identification scheme pursuant to section 8 subsection 1 paragraph 4 and 5;

2) the content of the notification referred to in section 10 and the delivery of the notification to the Finnish Transport and Communications Agency;

3) the properties of the interfaces of the trust network referred to in section 12 a subsection 2;

4) whether a disruption referred to in section 16 is significant and on the content, format and submission of the notification referred to in section 16 subsection 1;

5) the criteria for assessing the conformity of an identification or trust service and the national node referred to in section 29, 30 and 32.

6) the qualification requirements for the conformity assessment body laid down in section 33, taking into account the provisions of the EU Regulation on Electronic Identification and Trust Services;

7) the content of the application referred to in section 35 and the delivery of the application to the Finnish Transport and Communications Agency;

8) the requirements for the certification body referred to in section 36, the procedure to be followed in the certification and the requirements for the creation device for an electronic signature and an electronic seal, taking into account the provisions of the EU Regulation on Electronic Identification and Trust Services;

Section 42 a (1009/2018)
Duties of the Finnish Transport and Communications Agency

Unless otherwise provided in this Act, the task of the Finnish Transport and Communications Agency is to supervise compliance with this Act.

Pursuant to the EU Regulation on Electronic Identification and Trust Services, the task of the Finnish Transport and Communications Agency is to:

1) participate in the cooperation between the Member States of the European Union in the interoperability framework for electronic identification referred to in Article 12 of the Regulation and in the cooperation network established for the purpose;

2) notify the European Commission of electronic identification schemes pursuant to Article 7–10 of the Regulation;

3) act as the supervisory body referred to in Article 17 of the Regulation and perform the tasks laid down for it in the Regulation;

4) maintain and publish lists of qualified trust service providers in Finland and the qualified trust services they offer pursuant to Article 22 of the Regulation.

The Finnish Transport and Communications Agency does not have power of decision over matters concerning the contractual relationship or liability for damages between the parties.

Section 42 b (533/2016)
Duties of the Data Protection Ombudsman

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

Section 42 c (533/2016)
Duties of the Population Register Centre

The task of the Population Register Centre is to maintain the national node referred to in section 30.

Section 43 (1009/2018)
Right of access to information

When performing the duties pursuant to this Act, the Finnish Transport and Communications Agency has, secrecy provisions notwithstanding, the right to obtain information from the parties whose rights and obligations are laid down in this Act and who act on behalf of them.

When performing his or her duties, the Data Protection Ombudsman has the right of access to information referred to in the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter *General Data Protection Regulation*).

Section 44 (1009/2018)
Collaboration between authorities and the right to disclose data

In addition to the provisions in the Act on the Openness of Government Activities, the Finnish Transport and Communications Agency and the Data Protection Ombudsman have the right, without prejudice to secrecy provisions or other restrictions on data disclosure, to disclose such data to the Financial Supervisory Authority and the Finnish Competition and Consumer Authority that is necessary for these bodies to carry out their tasks. Notwithstanding any secrecy provisions, the Financial Supervisory Authority and the Finnish Competition and Consumer Authority have the same right to disclose information to the Finnish Transport and Communications Agency and the Data Protection Ombudsman required for the performance of their tasks provided in this Act.

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

Section 45 (1009/2018)
Administrative constraints

The Finnish Transport and Communications Agency may issue a notice to a party that violates this Act and the provisions, regulations or decisions issued pursuant to it, or the EU Regulation on Electronic Identification and Trust Services or the regulations issued pursuant to it, and may obligate the violating party to correct its error or negligence by a reasonable deadline. A notice of a conditional fine may be imposed to enforce the decision, or a notice of suspension of the activities partly or fully, or of having the neglected measure carried out at the expense of the interested party may be issued. Provisions on notices of a conditional fine, notices of enforced suspension and notices of enforced compliance are contained in the Act on Conditional Fines (1113/1990).

The costs of an action performed by enforced compliance are paid from central government funds and recovered from the party who was guilty of the neglect in the order prescribed in the Act on the Enforcement of Taxes and Public Payments (706/2007).

Section 45 a (1009/2018)
Interim decision

If the reliability of an identification and trust service is immediately and materially jeopardised by an error or negligence or information security disruption associated with the EU Regulation on Electronic Identification and Trust Services, this Act or a provision or regulation issued pursuant to them, the Finnish Transport and Communications Agency may decide on the required interim measures without delay and irrespective of the deadline laid down in section 45.

Prior to issuing a decision on an interim measure, the Finnish Transport and Communications Agency shall reserve the party concerned an opportunity to be consulted except if the consultation cannot be arranged as quickly as the urgency of the matter requires.

As an interim measure, the Finnish Transport and Communications Agency may prohibit or suspend:

1) the provision of an identification means as a strong electronic identification;

2) the provision of an qualified trust service referred to in Article 3(17) of the EU Regulation on Electronic Identification and Trust Services;

3) the provision of an electronic identification scheme that has been notified pursuant to Article 9(1) of the EU Regulation on Electronic Identification and Trust Services;

4) the provision of authentication 7(f) of the EU Regulation on Electronic Identification and Trust Services;

Interim measures may be valid for a maximum period of three months. An appeal may be made separately against a decision concerning interim measures in the same manner as against a decision referred to in section 45 subsection 1.

Section 46 (1009/2018)
Right to carry out inspections

The Finnish Transport and Communications Agency has the right to carry out an inspection on an identification service provider and the service it provides, an assessment body referred to in section 28, a certification body referred to in section 36 that certifies the qualified electronic signature and electronic seal creation devices, including their operation, a certification service provider offering qualified certificates and a trust service provider, and the services they provide. The inspection can be made to monitor compliance with the obligations laid down in this Act or in the EU Regulation on Electronic Identification and Trust Services or in provisions, regulations and decisions issued pursuant to them. Provisions on the inspection are laid down in section 39 of the Administrative Procedure Act.

The Finnish Transport and Communications Agency orders a party to carry out the inspection referred to in subsection 1. The person performing the inspection has the right to inspect the hardware and software of the identification service provider, certification service provider offering qualified certificates and a trust service provider and the people they use to provide assistance, to the extent relevant to supervising the compliance with the provisions of this Act or regulations issued under it.

Identification service providers, certification service providers offering qualified certificates and trust service providers or the persons they use to provide assistance shall allow the party referred to in subsection 2 to access premises other than those used for permanent residence.

Section 47 (1009/2018)
Fees to be paid to the Finnish Transport and Communications Agency

When the identification service provider that has submitted a notification referred to in section 10 or a consortium of service providers is registered for the first time, it must pay a registration fee of 5,000 euros to the Finnish Transport and Communications Agency. The identification service provider or consortium shall also pay the Finnish Transport and Communications Agency an annual

supervision fee of a total of 14,000 euros for the supervising of all of the identification services it offers.

A qualified trust service provider that has submitted a notification referred to in Article 21 of the EU Regulation on Electronic Identification and Trust Services and a certification service provider offering a qualified trust service shall pay the Finnish Transport and Communications Agency a registration fee of 5,000 euros for each trust service they provide. In addition, the service providers referred to above shall pay the Finnish Transport and Communications Agency an annual supervision fee of 14,000 euros for the first approved trust service they offer and an annual supervision fee of 9,000 euros for the subsequent approved trust services they offer. If a certification service provider offering qualified trust services also submits a notification referred to in section 10, it shall pay a registration fee referred to in subsection 1.

A conformity assessment body approved in accordance with section 34 above shall pay the Finnish Transport and Communications Agency a designation fee of 10,000 euros. The assessment body shall also pay the Finnish Transport and Communications Agency an annual supervision fee of 15,000 euros.

A certification body designated in accordance with section 36 above shall pay the Finnish Transport and Communications Agency a designation fee of 10,000 euros. The certification body shall also pay the Finnish Transport and Communications Agency an annual supervision fee of 15,000 euros.

The registration fee, designation fee and the supervision fee equal the expenses incurred by the Finnish Transport and Communications Agency in performing its duties under this Act, with the exception of duties mentioned in section 46 subsection 1. The supervision fee is payable in full for the first year of operations, even if operations do not start until mid-year. The supervision fee will not be refunded, even if operations stop mid-year.

The registration fee, designation fee and supervision fee are imposed by the Finnish Transport and Communications Agency and they are directly enforceable. An appeal may be made against a decision of the Finnish Transport and Communications Agency concerning the stipulation of the fee as laid down in section 49 subsection 1. Further provisions on the collection of the fees may be given by Decree of the Ministry of Transport and Communications.

Provisions on the levying of the registration fee, designation fee and supervision fee are laid down in the Act on the Enforcement of Taxes and Public Payments. If the fees are not paid at the latest by the due date, annual interest for late payment will be collected on the amount due in accordance with the interest rate referred to in section 4 of the Interest Act (633/1982). Instead of interest for late payment, the authority may charge a penalty of five euros for late payment if the amount of the interest for late payment is lower than that.

The costs incurred by the audit referred to in section 46 subsection 1 above are charged from the audited party in accordance with the Act on Criteria for Charges Payable to the State.

Chapter 6
Miscellaneous provisions

Section 48
Penal provisions

The penalties for a personal data file offence are provided in Chapter 38 section 9 of the Criminal Code of Finland (39/1889), and for a personal data file violation in section 48 subsection 2 of the Personal Data Act.

Section 49 (1009/2018)
Appeal against a decision by an authority

A claim for rectification of a decision by the Finnish Transport and Communications Agency that concerns a fee payable to the Finnish Transport and Communications Agency referred to in section 47 may be made as laid down in chapter 7 a of the Administrative Procedure Act.

An appeal against a decision by the Finnish Transport and Communications Agency issued following a claim for rectification and a decision other than the one referred to in subsection 1 made by the Finnish Transport and Communications Agency may be made to an administrative court as laid down in the Administrative Judicial Procedure Act (586/1996).

An appeal against a decision made by an administrative court in a case concerning the cancellation of an approval of a conformity assessment body and the designation of a certification body may be made as laid down in the Administrative Judicial Procedure Act. A decision of an administrative court, other than the above, may be appealed only if the Supreme Administrative Court grants leave to appeal.

In its decision, the Finnish Transport and Communications Agency 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 settled.

Section 49 a (1009/2018)
Appeal against a decision made by a conformity assessment body and a certification **body**

A claim for rectification of a decision made by a conformity assessment body or a certification body pursuant to this Act may be submitted to the Finnish Transport and Communications Agency as laid down in chapter 7 a of the Administrative Procedure Act.

A decision on the claim for rectification may be appealed to an administrative court, as laid down in the Administrative Judicial Procedure Act. A decision of an administrative court may only be appealed if the Supreme Administrative Court grants a leave to appeal.

The decision of the conformity assessment body and a certification body may nevertheless be complied with in spite of the appeal, unless otherwise ordered by the appeal authority.

Chapter 7
Entry into force

Section 50
Entry into force

This Act enters into force on 1 September 2009.

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.

Measures necessary for the implementation of this Act may be undertaken before the entry into force of the Act.

Section 51
Transitional provisions

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.

Identification means 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 means if the identification 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.

If identification service providers have entered into an agreement referred to in section 17 subsection 2 on the possibility of relying on each other for initial identification, and the service provider who issued the identification means 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 means issued in such a way shall be made without delay and as referred to in section 17.

A certification service provider offering qualified certificates that has submitted a notification according to section 9 subsection 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 subsection 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 (1175/2005) until 31 December 2009, regardless of the date of submitting an informal, written notification.

Entry into force and application of the amended provisions:

664/2012:

This «Act» enters into force on 1 January 2013.

139/2015:

This «Act» enters into force on 1 January 2016. However, section 12 a of it shall only be applied from 1 May 2017 onwards.

997/2015:

This «Act» enters into force on 1 January 2016.

The processing of an appeal against an administrative decision issued before this Act entered into force will be subject to the provisions that were in force when this Act entered into force.

533/2016

This «Act» enters into force on 1 July 2016. However, section 7 b of it shall only be applied from 1 May 2017 onwards.

Up until 31 December 2018, the identification means provider may also accept a valid driving licence issued by an authority of a member state of the European Economic Area after 1 October 1990 as an acceptable document referred to in section 17, subsection 2 of this Act.

The regulations of the Finnish Communications Regulatory Authority that were in force at the time of the entry into force of this Act will remain in force.

If an identification service provider entered in a register referred to in section 12 of the Act wishes to continue as a provider of strong electronic identification services, they shall submit a change notification referred to in section 10, subsection 3 of this Act to the Finnish Communications Regulatory Authority within two months of the entry into force of this Act. The information required in section 10 of this Act must be submitted to the Finnish Communications Regulatory Authority no later than 31 January 2017.

The Finnish Communications Regulatory Authority shall process the identification service provider's change notification referred to in subsection 4 and record the information arising out of the notification in the register referred to in section 12 within three months of receiving the change notification and other information laid down in subsection 4.

A strong electronic identification means that was issued under provisions that were in force when this Act came into force shall still be considered a strong electronic identification means on at least assurance level substantial for two months from the entry into force of this Act. Unless section 7 requires otherwise and if the identification service provider submits the change notification referred to in subsection 4 by the set deadline, an identification means issued by the identification service provider before this Act entered into force and after this Act enters into force shall be considered a strong electronic identification means with at least assurance level substantial, until the Finnish Communications Regulatory Authority has entered the information based on the change notification in the register referred to in section 12.

An electronic identification means issued pursuant to section 17 of this Act on the basis of an electronic identification means previously possessed by the holder shall be considered a strong electronic identification means, if:

1) the identification means was issued within two months of the entry into force of this Act; or

2) the identification means was issued after two months had passed from the entry into force of this Act on the basis of another strong electronic identification means issued by an identification means provider who has submitted the change notification referred to in subsection 4.

An electronic identification means shall no longer be considered a strong electronic identification means if the identification service provider fails to submit the change notification referred to in subsection 4 by the deadline. In such a case, the Finnish Communications Regulatory Authority shall delete the identification service provider from the register referred to in section 12 and notify the identification service provider that they have been deleted from the register.

816/2017

This «Act» enters into force on 15 December 2017. Section 17, subsection 5–7 of it shall be in force for five years from the entry into force of the Act.

1009/2018:

The entry into force of this Act shall be laid down separately by law.

Act 1009/2018 entered into force in accordance with Act 937/2018 on 1 January 2019.

412/2019:

This «Act» shall come into force on 1 April 2019. Section 17, subsection 7 of it shall be in force for two years from the entry into force of the Act.

An identification means provider must draw up and publish the delivery terms and conditions of the right to use their identification service within two months of the entry into force of this Act.

The agreements between identification service providers that are in force as this Act enters into force shall be made compliant with the Act within three months of this Act coming into force.

The Government Decree issued pursuant to section 12 a, subsection 5 that is in force at the time this Act enters into force will remain in force.