Issuer:	Riigikogu
Type:	act
In force from:	26.10.2016
In force until:	In force
Translation published:	27.10.2016

Electronic Identification and Trust Services for Electronic Transactions Act

Passed 12.10.2016

Chapter 1
General Provisions

§ 1. Scope of regulation and application of Act

(1) This Act regulates electronic identification and trust services for electronic transactions, and organisation of state supervision to the extent that these are not regulated by 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 (OJ L 257, 28.08.2014, pp. 73–114).

(2) This Act and other national legislation apply to electronic identification and trust services for electronic transactions if pursuant to Regulation (EU) No. 910/2014 of the European Parliament and of the Council, national law is to apply or if the Regulation permits the governing of national law in certain areas.

(3) The Administrative Procedure Act applies to administrative procedures provided for in this Act, taking account of the specifications provided for in this Act.

(4) The General Part of the Economic Activities Code Act applies to the commencement, pursuit and termination of the economic activities of an undertaking regulated by this Act, taking account of the specifications deriving from this Act and in Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

§ 2. Competent authorities

(1) A state authority authorised by the Government of the Republic shall perform the functions of a point of single contact for the purpose of cooperation between the Member States, deriving from Articles 9 and 12 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

(2) A state authority authorised by the Government of the Republic shall organise that availability of cross-border authentication of person identification data shall be ensured pursuant to Article 7 point (f) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

(3) The Technical Regulatory Authority (hereinafter competent authority) shall perform the functions of a supervisory body provided for in Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

(4) The Information System Authority (hereinafter competent information security authority) shall perform the functions of a supervisory body provided for in Article 19 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

Chapter 2
Trust Service and Trust Service Provider

§ 3. Trusted list and trust infrastructure

(1) The competent authority shall maintain a trusted list in accordance with Article 22 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council (hereinafter trusted list).

(2) The competent authority or the competent information security authority may organise the establishing, maintaining and updating of a trust infrastructure in accordance with Article 17 (5) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

(3) The requirements and procedure for establishing, maintaining and updating of a trust infrastructure may be established by a regulation of the minister responsible for the area.

§ 4. Obligation of notifying of security incidents

Trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the competent information security authority of any security incident in accordance with Article 19 (2) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

§ 5. Requirements for qualified trust service providers and for provision of trust services

(1) Qualified trust service providers and trust services shall comply with the requirements provided for in Regulation (EU) No. 910/2014 of the European Parliament and of the Council and in this Act, and the publicly approved and available specifications describing the trust service.

(2) To ensure compensation for damage as provided for in Article 13 (1) and (2) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council, qualified trust service providers shall enter into a liability insurance contract, with the sum insured at least in the amount of one million euros annually per each single insured event, and at least one million euros per all events in total. Qualified trust service provider shall make information on the existence of liability insurance and insurance coverage available to the public.

(3) Qualified trust service providers shall record the procedures performed upon provision of trust services, and shall maintain the respective activity record for ten years after creating the records.

(4) Qualified trust service providers shall have an up-to-date termination plan to ensure continuity of service, and the plan shall contain at least the following:
1) procedure for notification of clients, contractual partners and other interested parties, and for termination of contracts related to provision of trust services;
2) procedure for storage of the data set out in subsections (3) and (7) of this section;
3) procedure for destruction of private keys, backup copies or keys withdrawn from use in such a manner that these cannot be retrieved;
4) procedure for destruction or reinitialization of hardware depending on the security regulations.

(5) Before issuing a qualified certificate, a qualified trust service provider shall identify, verify identification on the basis of the document provided for in subsection 2 (2) of the Identity Documents Act, a valid travel document issued abroad or another document conforming to the requirements provided in subsection 4 (1) of the Identity Documents Act, and verify the reliability of the submitted data. A qualified trust service provider shall verify also the existence of the right of representation when issuing a certificate to a legal person.

(6) Qualified trust service providers shall refuse to provide services if there is doubt in respect of the accuracy of submitted data or authenticity of a submitted document upon verification of information submitted for identification or establishment of the right of representation.

(7) Qualified trust service providers shall store the evidence regarding identification for ten years after the end of validity of qualified certificates.

(8) If a qualified trust service provider ceases to provide a trust service but continues economic activities, the qualified trust service provider shall store the data set out in subsections (3) and (7) of this section during the term specified in these subsections, and enable verification of the authenticity of the procedures performed via the trust service on the basis of these data.

(9) Employees of qualified trust service providers who engage in the provision of trust services shall not have a valid criminal record for an intentionally committed criminal offence.

§ 6. Authorisation obligation of qualified trust service providers and entry into trusted list

(1) To provide a qualified trust service, a person and the trust service provided by the person shall have a qualified status pursuant to Article 21 (2) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council, evidenced by a relevant authorisation.

(2) The authorisation is valid for two years.

(3) Qualified trust service providers and trust services are entered in the trusted list for the term of the authorisation.

§ 7. Applying for authorisation

(1) An application for the grant of authorisation shall be decided by a competent authority.

(2) A competent authority shall decide on an application after receipt of required data and documents:
1) within 80 days in case of an application for an initial authorisation;
2) within 50 days in case of an application for a repeated authorisation.

(3) In addition to the data provided in subsection 19 (2) of the General Part of the Code of Economic Activities Act, the application for authorisation shall set out the following:
1) name and description of the trust service, principles of providing the trust service, certificate and conformity assessment report;
2) certificate of the absence of arrears of state taxes and local taxes of the place of residence or seat of the applicant if these data are not available in a database established on the basis of law.

(4) The principles of providing a trusted service set out in subsection (3) of this section shall be described exhaustively. An exhaustive description is presumed if the principles have been laid out in a format that is in compliance with the standards related to principles of providing trust services published by the European Telecommunications Standard Institute, or requirements of any other equivalent publicly approved and available specification.

(5) In the course of processing an application, the competent authority may request that the applicant would submit specifying information in respect of submitted data which is necessary for processing the application, and make inquiries to state authorities and local governments to verify the submitted data.

(6) A state fee in the amount provided in the States Fees Act shall be paid for the review of an application for an initial and repeated authorisation.

§ 8. Subject of review of authorisation

The competent authority grants an authorisation if:
1) the applicant and the trust service comply with the requirements provided in Article 24 (2) points (e), (f), (g) and (k) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council and in subsections 5 (2), 5 (4) and 5 (9) of this Act;
2) the applicant has passed the conformity assessment set out in Article 20 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council;
3) the applicant has no arrears of state taxes or local taxes of the place of residence or seat of the applicant.

§ 9. Refusal to grant authorisation and revocation of authorisation

(1) In addition to the cases set out in subsection 25 (1) of the General Part of the Economic Activities Code Act, the granting of an authorisation may be refused if at least one of the following circumstances exist:
1) on the basis of the submitted application and results of conformity assessment, the applicant for the authorisation for a trust service or the trust service does not comply with the requirements of Regulation (EU) No. 910/2014 of the European Parliament and of the Council or of this Act;
2) the applicant has arrears of state taxes or local taxes of the place or residence or seat of the applicant;
3) the applicant refuses to submit supplementary or significant information requested on the basis of Regulation (EU) No. 910/2014 of the European Parliament and of the Council, and on the basis of this Act.

(2) The competent authority revokes an authorisation if:
1) the trust service provider applies for revocation;
2) it appears after the grant of an authorisation that the trust service provider or the trust service provided by him or her does not comply with the requirements of Regulation (EU) No. 910/2014 of the European Parliament and of the Council or of this Act, and the trust service provider has not brought his or her activities into conformity with the requirements within a term provided by the competent authority;
3) the trust service provider has ceased to provide trust services.

(3) Before ceasing to provide trust services, the provider of the trust services shall inform the competent authority of an intention to cease, and shall apply for revocation of the authorisation.

(4) A trust service provider and trust service shall be deleted from the trusted list upon revocation of the authorisation.

§ 10. Entry of non-qualified trust service providers and trust services in trusted list

(1) Non-qualified trust service providers and trust services may also be entered in the trusted list. To enter them in the trusted list, the competent authority shall make a decision on the entry in the trusted list.

(2) The provisions of §§ 7 and 9 of this Act shall apply to the application for the entry of non-qualified trust service providers and trust services in the trusted list, refusal to enter them in the trusted list, and their deletion from the trusted list.

(3) Non-qualified trust service providers and trust services are entered in the trusted list for two years.

(4) A state fee in the amount provided for in the States Fees Act shall be paid for the review of an application for the entry of a non-qualified trust service provider and trust service in the trusted list, for the review of an application for a repeated entry, and for an application for amendment of data.

§ 11. Requirements for non-qualified trust service providers and trust services entered in trusted list

(1) To be entered in the trusted list, non-qualified trust service providers and trust services shall comply with the requirements provided for in Regulation (EU) No. 910/2014 of the European Parliament and of the Council and in this Act, and the publicly approved and available specifications describing the trust service.

(2) A non-qualified trust service provider shall have no arrears of state taxes or local taxes of the service provider's place of residence or seat.

(3) For assessment of conformity to the requirements provided in subsection (1) of this section, non-qualified trust service providers shall pass conformity assessment carried out by a conformity assessment authority in compliance with Article 3 (18) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council, before initiating trust services, and at least every two years thereafter.

§ 12. Advisory guidelines and conformity assessment procedure

(1) The minister responsible for the area or the competent authority may issue advisory guidelines for adhering to the requirements provided in §§ 5 and 11 of this Act.

(2) The minister responsible for the area shall establish, by a regulation, the procedure for conformity assessment of trust service providers and trust services.

(3) The minister responsible for the area may, by an order, designate a relevant authority or enter into a contract under public law with a person that certifies the conformity of qualified electronic signature creation devices to the requirements of Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

(4) The Ministry of Economic Affairs and Communications shall exercise administrative supervision over the performance of the duty upon entry into a contract under public law set out in subsection (3) of this section. If a contract under public law is terminated unilaterally or if there is another reason preventing continuance of performance of the duty, the further performance of the duty shall be organised by the Ministry of Economic Affairs and Communications.

§ 13. Notification of changes in circumstances related to provision of trust services

(1) A trust service provider shall immediately notify the competent authority of any changes in the data set out in an application for authorisation and application for entry in the trusted list.

(2) Upon change in the data pertaining to a trust service provider as recorded in the trusted list change, the trust service provider shall submit an application for amending the data, and the competent authority shall amend the trusted list within 14 days without the procedure set out in § 7 of this Act.

(3) If the contents of the trust service change, the competent authority has the right to request resubmission of the application set out in § 7 of this Act.

(4) A state fee in the amount provided for in the States Fees Act shall be paid for the review of an application for amending the data recorded in the trusted list.

§ 14. Time limit for entering trust service providers and trust services in trusted list

The competent authority shall enter a trust service provider and trust service in the trusted list within ten days after the grant of the authorisation pursuant to subsection 6 (1) of this Act or making the decision pursuant to subsection 10 (1) of this Act.

§ 15. Publication and securing of trusted list

(1) The competent authority shall publish a list of trust service providers and trust services on its website.

(2) The competent authority shall secure the trusted list by a public key and the corresponding private key.

(3) The minister responsible for the area shall organise, by an order, the creation of a public key used for certification of the trusted list, and the corresponding private key.

(4) The minister responsible for the area shall establish, by a regulation, the public key used for securing the trusted list, and designate the scope of use of the corresponding private key.

§ 16. Certificate of electronic signature and electronic seal and their period of validity

(1) The requirements for qualified certificates for electronic signatures are provided for in Article 28 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

(2) The requirements for qualified certificates for electronic seals are provided for in Article 38 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

(3) The provisions of this section and §§ 17–21 apply to the certificates of the users of trust services entered in the trusted list.

(4) A certificate is valid from the beginning of the period of validity set out in the certificate but not before the data of the certificate are entered in a certificate database kept by the issuer of the certificate.

(5) The validity of a certificate ends on the validity end date set out in the certificate or upon revocation of the certificate.

§ 17. Suspension of certificates

(1) A trust service provider has the right to suspend a certificate if there is doubt that incorrect data have been entered in the certificate or that it is possible to use the private key corresponding to the public key contained in the certificate without the consent of the certificate holder.

(2) A trust service provider is required to suspend a certificate if this is requested by:
1) the certificate holder;
2) the competent authority, the competent information security authority or the Estonian Data Protection Inspectorate;
3) a court, the Prosecutor's Office or a pre-trial investigation authority in a criminal matter to prevent an offence.

(3) Immediately after suspending a certificate, the trust service provider shall enter the information pertaining to the suspension of the certificate in the certificate database kept by the trust service provider in respect thereof, and shall keep records of the time and bases of suspension of the certificates, and applicants for suspension, and bases for ending the suspension.

(4) The trust service provider shall notify the certificate holder promptly of suspension of the certificate.

(5) E-signatures or e-seals given during the period when a certificate is suspended are invalid.

(6) Trust service provider providing trust services that do not enable suspension of the certificate, shall apply the provisions of §§ 19 and 20 of this Act.

§ 18. Restoration of validity of suspended certificate

(1) A trust service provider shall restore the validity of a suspended certificate at the request of the certificate holder or a person or authority that applied for the suspension, by entering the information on restoration of validity in the certificate database kept by the trust service provider.

(2) While restoring the validity of the certificate suspended on the basis of clause 17 (2) 1) of this Act, the qualified trust service provider that issued the certificate shall verify the identity pursuant to subsection 5 (5) of this Act.

(3) In the cases specified in clauses 17 (2) 2) and 3) of this Act, the person who initiated the suspension may apply for restoration of the validity of the certificate.

(4) A trust service provider shall notify the certificate holder promptly of restoration of the validity of the certificate.

§ 19. Revocation of certificates

(1) A trust service provider revokes a certificate based on an application or on its own initiative.

(2) A trust service provider revokes a certificate if it is requested by:
1) the certificate holder;
2) the competent authority, the competent information security authority or the Estonian Data Protection Inspectorate;
3) a court, the Prosecutor's Office or a pre-trial investigation authority in a criminal matter.

(3) If a certificate holder has a doubt that it is possible to use the private key corresponding to a public key contained in the certificate without his or her consent, the certificate holder shall request revocation of the certificate.

(4) The following are the bases for revocation of a certificate:
1) request of the certificate holder;
2) a possibility of using the private key corresponding to a public key contained in the certificate without the consent of the certificate holder;
3) appointment of a guardian to the certificate holder to an extent that precludes the use of the certificate;
4) death of the certificate holder or declaration of death of the certificate holder;
5) deletion of the certificate holder from the register due to termination of the activities of the certificate holder;
6) release or removal from office of the certificate holder that is a public office holder;
7) submission of false data to a trust service service provider by the certificate holder in order to obtain the certificate;
8) termination of provision of trust services;
9) loss of reliability of such a private key of the trust service provider that was used for issuing the certificate;
10) violation of a material obligation set out in the terms of use of the trust service by the certificate holder;
11) appearance of a circumstance related to revocation of the certificate that is set out in the principles of providing the trust service;
12) appearance of an error in the certificate or in the data entered in the certificate;
13) request of a court, the Prosecutor's Office or a pre-trial investigation authority in a criminal matter;
14) expiry or termination of a contract on the basis whereof the certificate is held;
15) other cases provided by law.

(5) A certificate entered in a document set out in subsection 2 (2) of the Identity Documents Act shall be revoked on the basis of the provisions of the Identity Documents Act.

§ 20. Procedure for revocation of certificates

(1) A trust service provider shall initiate a procedure for revocation of a certificate based on an application or upon appearance of the basis set out in subsection 19 (4) of this Act.

(2) Documents certifying the basis for revocation shall be appended to an application for revocation of a certificate on the basis of subsection 19 (4) of this Act.

(3) A trust service provider shall verify the existence of the legal basis for applying for revocation of a certificate, and enter the revocation promptly in the certificate database kept by the trust service provider.

(4) The validity of a certificate ends upon entry of the data on revocation of the certificate in the certificate database kept by a trust service provider.

(5) A trust service provider shall inform the certificate holder promptly of revocation of the certificate. In the case specified in clause 19 (4) 4) of this Act, a trust service provider shall inform a successor or the interested person who applied for declaration of death about the revocation of the certificate.

(6) Trust service providers shall preserve the documents evidencing the cause for revocation of certificates during the term set out in subsection 5 (3) of this Act.

§ 21. Consequences of suspension and revocation of certificates without legal basis

A person or authority that without legal basis, intentionally or due to gross negligence, causes suspension or revocation of a certificate is required to compensate for damage caused by the suspension or revocation of the certificate.

Chapter 3
Supervision

§ 22. State supervision

The competent authority and competent information security authority in accordance with their competence shall exercise state supervision over compliance with the requirements of Regulation (EU) No. 910/2014 of the European Parliament and of the Council, this Act, and the legislation established on the basis thereof.

§ 23. Specific measures and specifications of state supervision

(1) A law enforcement authority may, for the purpose of exercising the state supervision provided for in this Act, take special measures of state supervision provided for in §§ 30–32 and 49–52 of the Law Enforcement Act on the grounds and in accordance with the procedure provided for in the Law Enforcement Act.

(2) The measures provided for in §§ 49–50 of the Law Enforcement Act may be applied only upon entry into premises which are used for the provision of services, in the presence of a representative of the trust service provider.

Chapter 4
Implementing Provisions

§ 24. Digital signature and digital seal

(1) A digital signature shall be deemed an electronic signature that conforms to the requirements for a qualified electronic signature set out in Article 3 (12) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

(2) A digital seal shall be deemed an electronic seal that conforms to the requirements for a qualified electronic seal set out in Article 3 (27) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

§ 25. Digital signatures and digital seals given and certification service providers entered in register before entry into force of this Act

(1) A digital signature given on the basis of the Digital Signatures Act before the entry into force of this Act continues to be valid and has an equivalent legal effect with a qualified electronic signature that conforms to the requirements set out in of Regulation (EU) No. 910/2014 of the European Parliament and of the Council and in this Act, if it complies with all the following conditions:
1) it is a data unit, created using a system of technical and organisational means, which is used by a signatory to indicate his or her link to a document;
2) it is created by using a private key contained in a secure signature creation device to which the public key uniquely corresponds;
3) with the system of using the digital signature it enables unique identification of the person in whose name the signature is given, determination of the time when the signature is given, and link the digital signature to data in such a manner as to preclude the possibility of changing the signed data or the meaning thereof undetectably after the signature is given;
4) it has been given by using a trust service certificate entered in the register of certification in compliance with the Digital Signatures Act.

(2) The certificate of a digital seal issued on the basis of the Digital Signatures Act before the entry into force of this Act continues to be valid and the electronic seal given thereby has an equivalent legal effect with a qualified electronic seal that conforms to the requirements set out in Regulation (EU) No. 910/2014 of the European Parliament and of the Council and in this Act, if it complies with all the following conditions:
1) it is a data unit created by a system of technical and organisational means which the certificate holder uses to certify the integrity of a digital document and to link the certificate holder to such document;
2) it is created by a private key contained in a secure signature creation device to which the public key uniquely corresponds;
3) with the system of using the digital seal it enables unique identification of the person in whose name the seal is given, determination of the time when the seal is given, and link the digital seal to data in such a manner as to preclude the possibility of changing the sealed data or the meaning thereof undetectably after the seal is given;
4) it has been given by using a trust service certificate entered in the register of certification in compliance with the Digital Signatures Act.

(3) The certrification service providers entered in the register of certification as at the moment of entry into force of this Act are deemed qualified trust service providers, taking account of the special condition set out in Article 51 (3) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

§ 26. Repeal of Digital Signatures Act

The Digital Signatures Act is repealed.

§ 27. - § 40.Omitted from this translation

§ 41. Entry into force of Act

This Act enters into force on the day following the date of publication in the *Riigi Teataja*.

Eiki Nestor
President of the Riigikogu