Text consolidated by Valsts valodas centrs (State Language Centre) with amending laws of:

6 May 2004 [shall come into force from 27 May 2004];

28 October 2004 [shall come into force from 24 November 2004];

22 June 2006 [shall come into force from 21 July 2006];

24 May 2007 [shall come into force from 26 June 2007];

24 September 2009 [shall come into force from 22 October 2009];

5 March 2015 [shall come into force from 2 April 2015];

11 May 2017 [shall come into force from 22 May 2017];

7 June 2018 [shall come into force from 30 June 2018];

5 December 2019 [shall come into force from 31 December 2019].

If a whole or part of a section has been amended, the date of the amending law appears in square brackets at the end of the section. If a whole section, paragraph or clause has been deleted, the date of the deletion appears in square brackets beside the deleted section, paragraph or clause.

The *Saeima* 1 has adopted and

the President has proclaimed the following Law:

**Electronic Documents Law**

**Chapter I**

**General Provisions**

**Section 1. Terms Used in this Law**

The following terms are used in this Law:

1) [11 May 2017];

2) **secure electronic signature** – a qualified electronic signature within the meaning of Article 3(12) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter – Regulation No 910/2014/EU);

3) **electronic** **document** – an electronic document within the meaning of Article 3(35) of Regulation No 910/2014/EU;

4) **electronic** **signature** – an electronic signature within the meaning of Article 3(10) of Regulation No 910/2014/EU;

5) **electronic signature verification data** – validation data within the meaning of Article 3(40) of Regulation No 910/2014/EU;

6) **electronic signature creation data** – electronic signature creation data within the meaning of Article 3(13) of Regulation No 910/2014/EU;

7) **qualified certificate** – a qualified certificate for electronic signature within the meaning of Article 3(15) of Regulation No 910/2014/EU;

8) **time** **stamp** – a qualified electronic time stamp within the meaning of Article 3(34) of Regulation No 910/2014/EU;

9) **signatory** – a signatory within the meaning of Article 3(9) of Regulation No 910/2014/EU;

10) **certification** **services** – a trust service within the meaning of Article 3(16) of Regulation No 910/2014/EU;

11) **certificate** – a certificate for electronic signature within the meaning of Article 3(14) of Regulation No 910/2014/EU;

12) **certification service provider** – a trust service provider within the meaning of Article 3(19) of Regulation No 910/2014/EU;

13) **trusted certification service provider**– a qualified trust service provider within the meaning of Article 3(20) of Regulation No 910/2014/EU.

[*24 May 2007; 11 May 2017*]

**Section 2. Application of this Law**

(1) This Law determines the legal status of an electronic document and an electronic signature and it applies to the provision of certification services in accordance with the requirements laid down in Regulation No 910/2014/EU.

(2) The provisions of this Law for the circulation of electronic documents among State and local government institutions shall be applicable also to other public persons and their institutions, courts, persons and institutions belonging to the judicial system, and also public service providers within the meaning of the law On Regulators of Public Utilities.

[*11 May 2017*]

**Chapter II**

**Electronic Documents and the Derivation thereof**

**Section 3. Electronic Documents**

(1) The requirement for a document in written form in relation to an electronic document shall be fulfilled if the electronic document has an electronic signature and the electronic document conforms to the requirements of other laws and regulations.

(2) An electronic document shall be considered to have been signed by hand if it has a secure electronic signature. An electronic document shall be considered to have been signed by hand also in such cases where it has an electronic signature and the parties have agreed in writing regarding the signing of electronic documents with an electronic signature. In such case, the written agreement shall be drawn up and signed on paper or electronically with a secure electronic signature.

(3) If laws and regulations provide that, in addition to other requisites for a document to acquire legal effect, it also requires the imprint of a seal, then this requirement in relation to an electronic document shall be fulfilled if the electronic document has a secure electronic signature and a time stamp or electronic signature if the parties in accordance with the procedures laid down in Paragraph two of this Section have agreed in writing regarding the signing of electronic documents with an electronic signature.

(4) [11 May 2017]

(5) In the circulation of electronic documents between State and local government institutions or between these institutions and natural persons and legal persons, the electronic document shall be considered to be signed if it has a secure electronic signature and time stamp or electronic signature if the parties in accordance with the procedures laid down in Paragraph two of this Section have agreed in writing regarding the signing of electronic documents with an electronic signature.

(6) This Law shall apply insofar as other procedures and conditions for the drawing up of documents have not been determined in other laws and regulations.

[*28 October 2004; 5 March 2015; 11 May 2017*]

**Section 4. Original of Electronic Documents**

(1) If laws and regulations require the storage or presentation of the original of a document, this requirement in relation to electronic documents shall be fulfilled if it conforms to the requirements of Section 3, Paragraphs two and three of this Law.

(2) Paragraph one of this Section applies to a requirement expressed in the form of a duty or in a case, where the laws and regulations provide for a legal effect regarding the non-storage of documents or the non-presentation of document originals.

**Section 5. Derivation of Electronic Documents**

(1) A copy, true copy or extract in paper form of an electronic document shall have the same legal effect as the original if the correctness of the copy, true copy or extract is certified in accordance with the requirements of laws and regulations and if the issuer of the copies, true copies or extracts in paper form can, on the basis of a request, present the document original in electronic form, and it conforms to the requirements laid down in this Law.

(2) A copy, true copy or extract in electronic form of a paper document shall have the same legal effect as the original if the person who, in accordance with the requirements of laws and regulations, has the right to certify document original copies, true copies or extracts has certified its correctness with a secure electronic signature and time stamp or electronic signature if the parties in accordance with the procedures laid down in Section 3, Paragraph two of this Law have agreed in writing regarding the signing of electronic documents with an electronic signature, and it conforms to the requirements of laws and regulations.

(3) A duplicate of a paper document in electronic form shall have the same legal effect as the original if the duplicate has been issued and drawn up in conformity with the requirements of this Law and other laws and regulations.

(4) The making of derivations of electronic documents in paper form shall be only from such electronic documents as is possible to present in a readable or graphic form.

[*28 October 2004*]

**Chapter III**

**Provisions for the Circulation and Storage of Electronic Documents**

**Section 6. General Provisions for the Circulation and Storage of Electronic Documents**

(1) If laws and regulations determine requirements for the preparation, drawing up and storage of a paper document in a separate way, these same provisions shall be applicable also to electronic documents.

(2) The procedures for the preparation, drawing up, storage and circulation of electronic documents in State and local government institutions, and the circulation procedures between State and local government institutions, or between these institutions and natural persons and legal persons shall be governed by Cabinet regulations.

(3) The National Archives of Latvia shall be responsible for the evaluation and selection of electronic documents for long-term and permanent storage, and it shall also monitor that the archives of State and local government institutions ensure the storage and accessibility of electronic documents.

(4) State and local government institutions shall develop internal circulation instructions for electronic documents which comply with this Law and the regulations of the Cabinet referred to in Paragraph two of this Section, as well as the work specifics of the institution, and shall ensure the possibility of natural persons and legal persons to submit and receive State and local government institution documents, their copies, true copies, extracts and duplicates electronically or in another form according to the choice of the person.

(5) The type of evaluation of electronic documents, procedures for storage, and time limits for the transfer of such documents to the National Archives of Latvia for storage shall be regulated by Cabinet regulations.

[*6 May 2004; 5 December 2019*]

**Section 7. Special Provisions for the Storage of Electronic Documents**

(1) If laws and regulations provide for the storage of specific documents, records or data, this requirement in relation to electronic documents is fulfilled if:

1) the data contained therein is accessible for use;

2) the electronic document is preserved in such a form as it was initially created, sent or received, or in such a form as the initially created, sent or received data can be shown;

3) the preserved data allows the origin or final destination of the electronic document to be specified, and the time of sending or receipt.

(2) The provisions of Paragraph one, Clause 3 of this Section shall not apply to data that is automatically created in the process of receiving or sending an electronic document.

(3) A person may fulfil the provisions of Paragraph one of this Section by using the services of another person if the provisions of this Law are complied with.

**Chapter IV**

**Certification Service Providers and Trusted Certification Service Providers**

**Section 8. Certification Service Providers**

(1) A certification service provider is a natural or legal person, who provides certification services without the receipt of a special permit.

(2) The approval of a certification service provider is voluntary.

(3) In addition to the requirements of this Law laid down for a certified service provider, the provisions of Regulation No 910/2014/EU shall be applicable in respect of a trusted certification service provider.

[*11 May 2017*]

**Section 9. Trusted Certification Service Providers**

[11 May 2017]

**Section 10. Approval of the Activities of Trusted Certification Service Providers**

(1) [5 December 2019]

(2) A State fee shall be paid for the approval of the activities of a trusted certification service provider and the amount and the procedures for the payment thereof shall be determined by the Cabinet.

[*11 May 2017; 5 December 2019*]

**Section 11. Certification Service Provision Regulations**

[11 May 2017]

**Section 12. Description of the Certification Service Provision Information System, Equipment and Procedure Security**

[11 May 2017]

**Section 13. Examination of the Certification Service Provision Information System, Equipment and Procedure Security**

[11 May 2017]

**Section 14. Third Party Liability Insurance**

(1) It is mandatory to insure against the possible risk of losses associated with the activities of a trusted certification service provider.

(2) The insurance of the risk of the activities of a trusted certification service provider shall secure claims, which may arise in relation to his or her activities.

(3) The trusted certification service provider shall enter into an insurance contract prior to receipt of the approval of the activities, and the insurance contract shall be maintained in effect throughout the entire period of the provision of certification services.

(4) If as a result of the actions or inaction of the trusted certification service provider, losses are incurred, the insurance company on the basis of the insurance contract shall cover such losses from the insurance compensation of the trusted certification service provider.

(5) The Cabinet shall determine the minimum amount of insurance.

[*28 October 2004; 11 May 2017; 5 December 2019*]

**Section 14.1 Technical and Organisational Requirements**

[11 May 2017]

**Section 15. Personal Data Protection**

(1) A certification service provider may only acquire personal data directly from the natural person or from a third person if the natural person has consented in writing that his or her data shall be acquired by the concrete certification service provider from the third person.

(2) A certification service provider may process the personal data only for the provision of certification services.

(3) A certification service provider may not process the personal data, which are acquired for provision of certification services, for other purposes.

[*24 May 2007*]

**Chapter V**

**Qualified Certificates**

**Section 16. Information to be included in Qualified Certificates**

(1) Information in accordance with Annex I to Regulation No 910/2014/EU shall be included in a qualified certificate.

(2) In addition to the information referred to in Paragraph one of this Section, also the following information may be included in a qualified certificate upon written request of the signatory:

1) restrictions on the scope of operation of the certificate or other certificate operation restrictions;

2) specific legal facts in relation to the signatory (if such is necessary) depending upon the purpose for which the certificate is intended;

3) [24 May 2007];

4) [05 March 2015];

5) limitations of transaction amounts which may be performed using the qualified certificate.

(3) [11 May 2017]

(4) [11 May 2017]

[*22 June 2006; 24 May 2007; 5 March 2015; 11 May 2017*]

**Section 17. Issuance of Qualified Certificates**

(1) In order to receive a qualified certificate, the signatory shall submit a personally signed written application.

(2) Prior to the issue of a qualified certificate for electronic signature, a trusted certification service provider shall ascertain the identity of the signatory in person on the basis of a personal identification document presented by the signatory or electronically on the basis of the application of the signatory that has been signed with a qualified electronic signature of the signatory, or in accordance with the Law on Electronic Identification of Natural Persons.

(3) A trusted certification service provider shall, on the basis of a written application of the signatory, include in the qualified certificate information regarding the powers of the signatory or other important information, which is referred to in Section 16, Paragraph two of this Law.

(4) A trusted certification service provider on the basis of a written application of the signatory in place of the given name and surname of the signatory in the qualified certificate may record a pseudonym, in respect of which making a relevant indication in the certificate.

(5) The trusted certification service provider shall issue the qualified certificate to the signatory.

(6) A signatory may be issued several qualified certificates.

(7) The trusted certification service provider, preserving the liability laid down in this Law, on the basis of a contract may entrust another person to perform the activities laid down in Paragraphs two, three, four and five of this Section if the supervisory institution has given written consent for this.

[*24 May 2007; 5 March 2015; 11 May 2017*]

**Section 18. Revocation, Suspension of Operation, and Renewal of a Qualified Certificate**

(1) [11 May 2017]

(2) A trusted certification service provider shall, without delay, revoke a qualified certificate in the following cases:

1) the signatory requests the revocation of the certificate;

2) the trusted certification service provider receives official information regarding the death of the signatory or other information included in the certificate changes;

3) the signatory has provided the trusted certification service provider with false or misleading information in order to receive a qualified certificate;

4) when fulfilling a court ruling on the revocation of the certificate;

5) in the cases stipulated in the contract regarding provision of certification services.

(3) The suspension of operation of a qualified certificate is recognition of the certificate as invalid for a time. The operation of a suspended qualified certificate may be renewed.

(4) The renewal of the operation of a qualified certificate is the recognition of the qualified certificate as valid, the operation of which was suspended.

(5) A trusted certification service provider shall suspend and renew the operation of a qualified certificate in the following cases:

1) when fulfilling a court ruling;

2) on the basis of a written request of the signatory;

3) in the cases stipulated in the contract regarding provision of certification services.

(6) A qualified certificate may not be revoked, and its operation suspended or renewed with a retroactive date.

(7) A secure electronic signature, which has been created after the revocation of a qualified certificate or in the period when the operation of the qualified certificate has been suspended, shall not be valid.

(8) A secure electronic signature, which has been created after the death of the signatory, shall not be valid.

(9) If a trusted certification service provider revokes a qualified certificate, suspends or renews the operation thereof without a legal basis, on wrongful purpose or due to negligence, the trusted certification service provider shall compensate losses caused to persons that have arisen due to the unfounded revocation of the qualified certificate, and the suspension or renewal of the operation thereof.

[*22 June 2006; 24 May 2007; 11 May 2017*]

**Chapter VI**

**Supervision of Trusted Certification Service Providers**

**Section 19. Trusted Certification Service Provider Supervisory Institution**

(1) The supervisory institution shall perform the supervision of trusted certification service providers and services provided thereby, the approval of the activities and revocation of the approval of the activities in accordance with the requirements laid down in Regulation No 910/2014/EU, this Law, and other laws and regulations.

(2) The supervisory institution shall regularly supervise the conformity of the activities of trusted certification service providers with the requirements laid down in Regulation No 910/2014/EU, this Law, and other laws and regulations.

(3) The supervisory institution and the procedures for the organisation of the activities thereof shall be determined by the Cabinet.

[*11 May 2017; 5 December 2019*]

**Section 20. Duties of the Supervisory Institution**

(1) [5 December 2019]

(2) The supervisory institution shall develop, maintain and publish on its website trusted lists, including information on trusted certification service providers whereof it is responsible for, and also information on trusted certification services provided by such service providers and shall provide information to the European Commission in accordance with Regulation No 910/2014/EU.

(3) In accordance with Regulation No 910/2014/EU, the supervisory institution shall publish on its website the numbers of standards which are specified in the referred to Regulation and which have been introduced, and also technical specifications, formats, and procedures which are specified therein and which have been introduced.

[*11 May 2017; 5 December 2019*]

**Section 21. Supervisory Measures**

[11 May 2017]

**Section 22. Termination of the Activities of a Trusted Certification Service Provider and Operation of the Provided Services, Declaration of Insolvency Thereof and Revocation of the Approval of the Activities**

(1) A trusted certification service provider shall, without delay, inform in writing the supervisory institution and on its website shall ensure that signatories, with whom a certification service provision contract has been entered into or to whom an identity card which contains information required for creating a secure electronic signature has been issued, have publicly accessible information that the activities thereof have been terminated, it has been declared insolvent or the approval of the activities of a certification service provider or operation of provided services has been revoked.

(11) If the approval of a trusted certification service provider or operation of provided services is revoked, but the operation thereof is not terminated or it has not been declared insolvent, it shall retain all information on the provided and received data, and shall ensure accessibility of such information.

(12) If the activities of a trusted certification provider are terminated or it has been declared insolvent, the Cabinet shall immediately decide on the transfer of all information thereof containing the data provided and received by a trusted certification service provider to a third person.

(2) [5 December 2019]

(3) [5 December 2019]

(4) [5 December 2019]

(5) [5 December 2019]

(6) The supervisory institution shall, without delay, revoke the approval of the activities of a trusted certification service provider who has terminated the activities thereof or has been declared insolvent, including such information in the trusted certification service provider register.

[*24 May 2007; 5 March 2015; 11 May 2017; 5 December 2019*]

**Chapter VII**

**Duties and Liability of Trusted Certification Service Providers and Signatories**

**Section 23. Duties of Trusted Certification Service Providers**

(1) A trusted certification service provider has the following duties:

1) to use secure certification service provision information systems, equipment and procedures that appropriately guarantee the security of certification services;

2) to take necessary measures in order to guarantee the secrecy of secure electronic signature creation data and protection against illegal processing and use of electronic signature creation data, protection against forgery of qualified certificates and accessibility to such certificates only with the consent of the signatory;

3) to ensure that the certification service provision information system, equipment and procedures conforms to this Law and other laws and regulations;

4) to ensure that personal identification information of the signatory is included in the qualified certificate on the basis of a personal identification document presented in the presence of the signatory or, according to Section 17, Paragraph two of this Law, on the basis of the application of the signatory which has been signed with a secure electronic signature of the signatory;

5) to ensure that the qualified certificate is issued upon entering into a contract with the signatory for the provision of certification services or upon issuing an identity card with information required for creating a secure electronic signature;

6) prior to entering into a contract or prior to issuing an identity card with information required for creating a secure electronic signature, to ensure on its website publicly accessible information on the provisions and conditions which apply to the use of a qualified certificate, including any restrictions on the use of the certificate, the procedures for reviewing complaints and disputes, civil liability of a trusted certification service provider, and also the cases of the suspension, revocation and renewal of the operation of a qualified certificate provided for in the contract or the laws and regulations which apply to personal identification documents;

7) prior to entering into a contract or prior to issuing an identity card with information required for creating a secure electronic signature, to ensure on its website publicly accessible information on the provisions for the provision of certification services and security measures performed by a trusted certification service provider in order to prevent the illegal use of the issued qualified certificates;

8) upon issuing a qualified certificate, to ensure publicly accessible information on its website or to inform the signatory in writing regarding the conditions included in the certificate and the restrictions on use of the certificate;

9) [11 May 2017];

10) [11 May 2017];

11) to ensure, without delay, the revocation of a qualified certificate, the suspension or renewal of the operation thereof in the cases laid down in this Law;

12) [24 May 2007];

13) to inform the signatory, his or her authorised persons or heirs, without delay, regarding the revocation of the qualified certificate or suspension of the operation thereof;

14) to maintain continually in free of charge and freely accessible online regime the registers of full electronic signature-verification data, and issued, revoked, suspended and renewed qualified certificates;

15) [11 May 2017];

16) to preserve information associated with qualified certificates and time stamps for a specified time in accordance with the procedures laid down in this Law and other laws and regulations;

17) to regularly perform the security inspection of information systems, equipment and procedures related to the provision of certification services and to keep inspection records. All measures related to the issue, revocation of a qualified certificate, suspension and renewal of the operation thereof, measures related to marking electronic documents with a time stamp and also any other data changes shall be included in inspection records. The inspection records shall be kept continuously. The audit notes shall be secured by the physical and logical protection laid down in laws and regulations;

18) to perform measures against the possible forgery of qualified certificates and time stamps, and to guarantee the confidentiality of electronic signature creation data during the time period of its creation;

19) not to store and copy secure electronic signature creation data;

20) to ensure that the time stamp indicates an internationally co-ordinated precise time;

21) in accordance with the procedures laid down in laws and regulations, to provide information to a court, the Office of the Prosecutor and inquiry institutions regarding the issued, revoked, suspended and renewed certificates and time stamps;

22) to conform to the Personal Data Protection Law and laws and regulations that govern the security of information systems;

23) to transfer the register of qualified certificates that have been revoked and the operation of which has been terminated to the National Archives of Latvia in accordance with the Cabinet regulations that regulate the procedures by which and time limits in which electronic documents shall be evaluated, collected and transferred to the National Archives of Latvia;

24) to insure for its own civil liability.

(2) If a qualified certificate is included in an identity card, a trusted certification service provider shall enter into a contract with the signatory for the provision of certification services.

(3) A qualified certificate shall be included in an identity card in accordance with the laws and regulations applying to personal identification documents.

[*22 June 2006; 24 May 2007; 5 March 2015; 11 May 2017; 5 December 2019*]

**Section 24. Liability of Trusted Certification Service Providers**

[11 May 2017]

**Section 25. Duties and Liability of Signatories**

(1) A signatory has the following duties:

1) to provide the trusted certification service provider with truthful information;

2) prior to entering into a contract for the provision of certification services or prior to issuing an identity card with information required for creating a secure electronic signature, to confirm in writing that he or she has become acquainted with the security description of the information system for the provision of certification services, equipment and procedures, provisions for the provision of certification services included in the trusted certification service provider register and other security measures performed by a trusted certification service provider to prevent the illegal use of the qualified certificate;

3) after receipt of the qualified certificate to confirm in writing that he or she has become acquainted with the conditions and restriction included in the qualified certificate;

4) to ensure that the electronic signature creation data is not used without the knowledge of the signatory;

5) to request, without delay, that the trusted certification service provider revokes the qualified certificate or suspends the operation thereof if there is a basis to believe that the electronic signature creation data have been used without the knowledge of the signatory;

6) to request, without delay, that the trusted certification service provider revokes the qualified certificate if there are changes to the information indicated therein.

(2) A signatory is liable for losses that are caused to a person who reasonably relied upon the qualified certificate if:

1) the signatory provided the trusted certification service provider with false information;

2) the signatory has not appropriately taken care regarding the protection of the electronic signature creation data against unauthorised use;

3) there has been a basis to believe that the electronic signature creation data have been used without the knowledge of the signatory, but the signatory has not requested the trusted certification service provider to revoke the qualified certificate or to suspend its operation.

[*24 May 2007; 5 March 2015; 11 May 2017; 5 December 2019*]

**Chapter VIII**

**Recognition of Qualified Certificates Issued in a Foreign Country**

**Section 26. Recognition of Qualified Certificates Issued in a Foreign Country**

A certificate issued in a foreign country shall have the legal status and legal effects of a qualified certificate determined in this Law if it conforms to at least one of the following conditions:

1) it has been issued by a trusted certification service provider registered in the supervisory institution of a Member State of the European Union;

2) it has been issued by a trusted certification service provider performing entrepreneurship in a third country in accordance with Article 14 of Regulation No 910/2014/EU.

[*5 December 2019*]

**Transitional Provisions**

1. State and local government institutions have a duty to accept electronic documents from natural persons and legal persons no later than 1 January 2004.

2. The Cabinet shall by 1 January 2005 issue the regulations provided for in Section 14.1 of this Law.

[*28 October 2004*]

3. [11 May 2017]

4. A trusted certification service provider, who has been certified in the supervisory institution in accordance with the requirements referred to in this Law, shall, by 1 July 2017, submit a conformity assessment report to the supervisory institution in accordance with the requirements laid down in Regulation No 910/2014/EU. Until the day when the supervisory institution has examined the abovementioned conformity assessment report, a certification service provider shall be considered as a trusted certification service provider in accordance with this Law.

[*11 May 2017*]

5. The security inspection of the information systems, equipment and procedures for the provision of certification services that has been performed by a trusted certification service provider in the period from 1 January 2016 until 21 May 2017 shall be effective by 31 December 2017.

[*11 May 2017*]

6. The electronic document which has been signed with a qualified certificate for electronic signature issued to the signatory by a trusted certification service provider certified in Latvia in the period from 1 July 2016 until 30 June 2020 shall be considered to have been signed by hand within the meaning of this Law.

[*11 May 2017; 7 June 2018*]

7. The Cabinet shall, by 30 September 2017, issue regulations regarding the State fee for the approval of the activities of a trusted certification service provider and renewal thereof. Until the day of coming into force of new Cabinet regulations, Cabinet Regulation No. 371 of 20 April 2010, Regulations Regarding the State Fee for Accreditation and Renewal of Accreditation of a Certification Service Provider, shall be applicable insofar they are not in contradiction with this Law.

[*11 May 2017*]

**Informative Reference to the Directives of the European Union**

[11 May 2017]

This Law shall come into force on 1 January 2003.

The Law has been adopted by the *Saeima* on 31 October 2002.

Acting for the President, Chairperson of the *Saeima* I. Ūdre

Rīga, 20 November 2002