

Electronic Documents Law

Tulkošanas un terminoloģijas centra tulkojums.

The Saeima 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) **secure electronic signature-creation devices** – software packages, hardware and electronic signature-creation data that conform to the following requirements:
 - a) the electronic signature-creation data shall be created only once, and the secrecy thereof is ensured,
 - b) the electronic signature-creation data cannot be derived and, utilising technologies, the electronic signature is secured against forgery,
 - c) the electronic signature-creation data are securely protected against being used unlawfully by third persons, and
 - d) the secure electronic signature-creation devices do not alter the electronic document to be signed and do not prevent becoming acquainted with such a document before its signing;
- 2) **secure electronic signature** – an electronic signature that conforms to all of the following requirements:
 - a) it is linked only to the signatory,
 - b) it ensures the personal identification of the signatory,
 - c) it is created with secure electronic signature-creation devices, which may be controlled only by the signatory,
 - d) it is linked to a signed electronic document so that later changes in the electronic document are detectable, and
 - e) it is certified by a qualified certificate;

3) **electronic document** – any data which is created, stored, sent or received electronically, which ensures the possibility of utilising such data for the performance of some activity, realisation of a right and protection;

4) **electronic signature** – electronic data that is attached to or logically associated with an electronic document, and ensures the authenticity of the electronic document and confirms the identity of the signatory;

5) **electronic signature-verification data** – data that is utilised in order to verify an electronic signature;

6) **electronic signature-creation data** – data created only once, which are utilised by the signatory in order to create an electronic signature;

7) **qualified certificate** – a certificate which contains the information specified in this Law and which has been issued by a trusted certification service provider;

8) **time-stamp** – an electronically signed confirmation of the fact that at a specified date and time the electronic document has been signed at the certification service provider;

9) **signatory** – a person who has electronic signature-creation devices and who acts either in his or her own name or the name of the natural person or legal person or institution that he or she represents;

10) **certification services** – the issuance and cancellation of certificates, the suspension and renewal of the validity of certificates, registration of certificates, the maintenance of a electronic signature-verification data register, the stamping of electronic documents with time-stamps, as well as the provision of consultancy services in relation to electronic signatures; and

12) **certificate** – an electronic confirmation that links the electronic signature-verification data with a signatory and serves to specify the identity of the signatory.

Section 2. Application of this Law

(1) This Law determines the legal status of electronic documents and electronic signatures.

(2) The provisions of this Law are not applicable if a natural person or legal person who is not a certification service provider performs the stamping of electronic documents with a time-stamp.

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 regulatory enactments.

(2) An electronic document shall be considered to have been signed by hand if it has a secure electronic signature.

(3) If regulatory enactments 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.

(4) An electronic signature is legal evidence and the submission of an electronic document as evidence to competent institutions has no restrictions, based only upon the fact that:

a) the document is in electronic form; or

b) it does not have a secure electronic signature.

(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.

(6) The provisions of this Law are not applicable to:

1) contracts with which rights are created or transferred to immovable property, except for rental rights;

2) contracts which, in accordance with law, are not in effect if they have not been certified according to special procedures by law;

3) guarantee contracts if the guarantee grants, and security for pledges if such is provided by persons who engage in purposes, which are not related to the trade of such person, entrepreneurial activity or occupation; and

4) transactions in the field of family law and inheritance law.

Section 4. Original Electronic Documents

(1) If regulatory enactments 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 regulatory enactments 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 regulatory enactments 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 specified by 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 regulatory enactments, has the right to certify document original copies, true copies or extracts has certified its correctness with a secure electronic signature and time-stamp, and it conforms to the requirements of regulatory enactments.

(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 regulatory enactments.

(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.

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 regulatory enactments determine requirements for the preparation, drawing up and storage of documents 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 regulated by Cabinet regulations.

(3) The Latvian State Archive Directorate shall be responsible for the evaluation and selection of electronic documents for long-term and permanent storage, and it shall also monitor that State and local government archives 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, and time periods for the transfer of such documents to State archives for storage shall be regulated by Cabinet regulations.

Section 7. Special Provisions for the Storage of Electronic Documents

(1) If regulatory enactments 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 utilisation;
- 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; and
- 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 utilising the services of another person if the provisions of this Law are complied with.

Chapter IV

Certificate 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) Accreditation of a certification service provider is voluntary.

(3) A certification service provider shall be considered to be trustworthy if he or she conforms to all the requirements of Section 9 of this Law.

Section 9. Trusted Certification Service Provider

A trusted certification service provider shall be considered to be a natural or legal person who conforms to all of the following requirements:

- 1) utilises trustworthy personnel who have the necessary specialised knowledge, experience and qualifications for the provision of certification services, who have become acquainted with the relevant security provisions for the provision of certification services, and have not been convicted for the intentional committing of a criminal offence;

- 2) utilises trustworthy and secure information systems and products which are appropriately protected against unauthorised access and modification;
- 3) maintains sufficient financial resources in order to implement this Law and the regulatory enactment requirements issued on the basis of this Law, and shall insure itself for civil liability in order to be able to compensate losses caused to persons due to wrongful purpose or negligence;
- 4) is accredited with the State Data Inspection (hereinafter also – supervisory institution) in accordance with the procedures specified in this Law;
- 5) ensures the continuous on-line accessibility of the signature-verification data register;
- 6) ensures the possibility of immediate revocation, suspension of operation and renewal of qualified certificates in the cases specified in this Law;
- 7) ensures that at any moment the date and time of the issuance, revocation, suspension of operation and renewal of qualified certificates can be determined;
- 8) utilises a secure system for qualified certificate storage in a verifiable form and shall ensure that:
 - a) only the authorised persons of the trusted certification service provider may make entries or their changes,
 - b) it is possible to check and determine changes in information,
 - c) the qualified certificates issued are not publicly accessible, except in a case where the written consent of the signatory has been obtained,
 - d) any technical changes that affect security requirements are apparent to the systems administrator, and
 - e) such technology is utilised as will ensure that when using electronic signature-creation data they can never be copied;
- 9) in stamping the electronic document with a time stamp, ensures the possibility to specify without doubt the date and time of the received electronic document; and
- 10) ensure that the time-stamp does not alter the signed electronic document.

Section 10. Accreditation of Trusted Certification Service Providers

In order to receive accreditation, the following documents shall be submitted to the supervisory institution:

- 1) a written application;
- 2) the certification service provision regulations;

- 3) a description of the certification service provision information system and procedure security;
- 4) an examination opinion of the certification service provision information system and procedure security; and
- 5) a document that certifies the fulfilment of the requirements of Section 9, Clause 3 of this Law.

Section 11. Certification Service Provision Regulations

(1) The certification service provision regulations shall include:

- 1) the firm name of the trusted certification service provider, registration number or given name, surname, personal identity number, telephone address and electronic mail address;
- 2) information regarding the information system, equipment, technology, computer programmes to be utilised for the provision of certification services and the documents certifying their right of use;
- 3) a model trusted certification service provider and signatory contract;
- 4) information regarding the issuing procedures for qualified certificates and their security;
- 5) information regarding various possibilities of restricting the use of the secure electronic signature by the signatory;
- 6) information regarding the revocation, suspension of operation and renewal procedures for qualified certificates;
- 7) information regarding the technical and technological possibilities which are offered by the certification service provider in order to protect secure electronic signature-creation devices, electronic signature-verification data and qualified certificates from unlawful use;
- 8) information regarding the fact that in the continuous on-line free access regime, free access shall be ensured to the electronic signature-verification data and the issued, revoked, suspended and renewed certificate registers;
- 9) information regarding the stamping of electronic documents with a time-stamp and the security of the procedures thereof; and
- 10) information regarding the fact that in the continuous on-line regime, free access shall be ensured to the time-stamp register.

(2) If the information included in the certification service provision regulation changes, the trusted certification service provider shall, without delay, submit

amendments to the certification service provision regulations to the supervisory institution.

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

(1) Information to be indicated in the description of the certification service provision information system, equipment and procedure security shall be determined by the Cabinet.

(2) If the information indicated in the description of the certification service provision information system, equipment and procedure security changes, the trusted certification service provider shall, without delay, submit amendments to the description of the certification service provision information system, equipment and procedure security to the supervisory institution.

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

(1) The examination of the certification service provision information system, equipment and procedure security and the opinion regarding such shall be provided by an expert who is included in a list approved by the supervisory institution.

(2) The list approved by the supervisory institution shall include persons who conform to all of the following requirements:

1) he or she has the technical possibility to specify the conformity of the certification service provision information system, equipment and procedure security to the requirements of regulatory enactments;

2) he or she is legally and financially independent from trusted certification service providers and supervisory institutions;

3) he or she or his or her employed personnel have the necessary knowledge; and

4) he or she is not engaged in the manufacture and supply of certification service provision information systems and other information technologies.

(3) Procedures for the examination of certification service provision information system, equipment and procedure security and time periods shall be determined by the Cabinet.

Section 14. Civil 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 accreditation, and the insurance contract shall be maintained in effect for the whole of the time 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 and the procedures for calculating insurance compensation.

Section 15. Personal Data Protection

(1) A certification service provider may only acquire the personal data directly from the signatory or from a third person if the signatory has consented to this.

(2) A certification service provider may only process the personal data for the purpose of issuing and maintaining a certificate.

(3) A certification service provider may not process the personal data for other purposes without the consent of the signatory.

Chapter V Qualified Certificates

Section 16. Information to be included in Qualified Certificates

(1) A qualified certificate shall include the following information:

- 1) an indication that it is a qualified certificate;
- 2) the firm name, registration number and the state in which the trusted certification service provider is established or given name, surname and personal identity number;
- 3) the given name and surname of the signatory or a pseudonym (indicating that it is a pseudonym);
- 4) personal identity number of the signatory;
- 5) term of validity of the quality certificate;
- 6) the consecutive number of the certificate granted by the trusted certification service provider; and
- 7) the electronic signature-verification data which correspond to the existing electronic signature-creation data under the control of the signatory.

(2) In addition to the information referred to in Paragraph one of this Section, a qualified certificate may also include the following information:

- 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) restrictions on the amounts of the transactions for the performance of which the qualified certificate may be utilised; and
- 4) the personal identity number of the signatory.

(3) A qualified certificate shall be signed with the secure electronic signature of the trusted certification service provider.

Section 17. Issuance of Qualified Certificates

(1) To receive a qualified certificate, a written application by the signatory shall be submitted.

(2) Before the issuance of a qualified certificate, the trusted certification service provider shall, in the presence of the signatory, be satisfied regarding the identity of the signatory on the basis of the personal identification document presented by the signatory.

(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 specified in this Law, on the basis of a contract may entrust another person to perform the activities specified in Paragraphs two, three and four of this Section if the supervisory institution has given written consent for this.

Section 18. Revocation, Suspension of Operation and Renewal of Qualified Certificates

(1) The revocation of a qualified certificate is the recognising of the certificate as invalid. The operation of a revoked qualified certificate shall not be renewed.

(2) A trusted certification service provider shall revoke without delay 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; or
- 4) fulfilment of a court adjudication regarding the revocation of the certificate.

(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) The suspension of operation and renewal of a qualified certificate shall be performed by a trusted certification service provider on the basis of a court adjudication or a written request of the signatory.

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

(7) A secure electronic signature shall not be valid from the moment of the revocation or suspension of operation of the qualified certificate.

(8) In the event of the death of the signatory, the secure electronic signature shall not be valid from the moment of the death of the signatory.

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

Chapter VI Supervision of Trusted Certification Service Providers

Section 19. Trusted Certification Service Provider Supervisory Institution

(1) The State Data Inspection shall be the supervisory institution for trusted certification service providers.

(2) The supervisory institution shall regularly supervise the conformity of the work of the trusted certification service providers to the requirements of this Law and other regulatory enactments.

Section 20. Duties of the Supervisory Institution

(1) The supervisory institution has the following duties:

- 1) to accredit certification service providers in accordance with the voluntary accreditation principles;
- 2) to check whether the trusted certification service providers comply with the certification service provision regulations;
- 3) to monitor that the security of the trusted certification service provider information system and procedures conform to this Law, other regulatory enactments and the description of the trusted certification service provider information system, equipment and procedure security;
- 4) to monitor that the electronic signature-verification data and time-stamp registers for qualified certificates issued, revoked, suspended and renewed by trusted certification service providers is accessible in a continuous on-line regime; and
- 5) to ensure that the Latvian accredited trusted certification service provider register in which information regarding certification service providers from other states is also included, the issued qualified certificates of which are guaranteed by a Republic of Latvia accredited trusted certification service provider, is freely accessible in a continuous on-line regime.

(3) The supervisory institution shall maintain a continuous on-line freely accessible trusted certification service provider register, in which the following information shall be accessible:

- 1) the firm name of the trusted certification service provider or given name and surname;
- 2) the address, telephone number and electronic mail address of the trusted certification service provider;
- 3) the certification service provision regulations;
- 4) a description of the certification service provision information system, equipment and procedure security;
- 5) an examination opinion of the certification service provision information system, equipment and procedure security;
- 6) the date of accreditation; and

7) information regarding reprimands, warnings or revocation of accreditation by the supervisory institution.

(4) If the documents submitted and the certification service provider conform to the requirements of this Law and other regulatory enactments, the supervisory institution shall issue, within a period of 10 days from receipt of all the documents referred to in Section 10 of this Law, to the certification service provider an accreditation certificate and shall include the information referred to in Paragraph two of this Section in the trusted certification service provider register.

(5) If the documents submitted or the certification service provider do not conform to the requirements of this Law and other regulatory enactments, the supervisory institution shall issue, within a period of 10 days from receipt of all the documents referred to in Section 10 of this Law, a written refusal of accreditation.

Section 21. Supervisory Measures

(1) The supervisory institution has the right to give instructions to trusted certification service providers to rectify non-conformity with this Law, other regulatory enactments, the certification service provision regulations included in the trusted certification service provider register or the description of the certification service provision information system, equipment and procedure security.

(2) The time period for rectification of non-conformity shall be determined by the supervisory institution.

(3) If the supervisory institution's instructions are not carried out within the time period specified by it, the supervisory institution shall warn the trusted certification service provider regarding the possible revocation of accreditation.

(4) If, within 10 days following the supervisory institution's warning regarding the possible revocation of accreditation, the supervisory institution's instructions are not carried out, the accreditation of the trusted certification service provider shall be revoked without delay and the information regarding the revocation of the accreditation shall be included in the trusted certification service provider register.

(5) After the revocation of the accreditation of the trusted certification service provider, the provisions of Section 22, Paragraphs two, three, four and five of this Law shall be applied.

(6) In performing supervision, officials of the supervisory institution shall present a service identification document. The person referred to has the following rights:

1) to freely visit any commercial premises in which the information systems and equipment of the trusted certification service provider is located, and in the presence of the certification service provider to perform the necessary examination or other measures, in order to determine the conformity of the certification service provision process to this Law, other regulatory enactments, certification service provision regulations published in the trusted certification service providers register and the

description of the certification service provision information system, equipment and procedure security;

2) to request written or oral explanations from the trusted certification service provider representatives and employees;

3) to become acquainted with documents and other information which relate to certification service provision; and

4) to request the examination of the information systems, equipment and procedures of the trusted certification service provider and to specify the issues to be investigated in the independent expert-examination.

(7) The supervisory institution has the right to bring an action in court to terminate the activities of a trusted certification service provider if the relevant trusted certification service provider violates this Law or other regulatory enactments.

(8) The decisions of the supervisory institution may be appealed to a court.

Section 22. Termination of the Activities of a Trusted Certification Service Provider, Declaration of Insolvency and Suspension of Service Provision

(1) A trusted certification service provider shall, without delay, inform in writing the supervisory institution and signatories with whom a certification service provision contract has been entered into, regarding the termination of activities, declaration of insolvency or suspension of service provision of the service provider.

(2) In the cases referred to in Paragraph one of this Section, the trusted certification service provider shall ensure the preservation of the data associated with the certification service, information, databases, registers, other pertinent information, the information system and certification service, and on the basis of mutual agreement transfer them to other trusted certification service providers.

(3) In respect of all transfer procedures and time periods, the supervisory institution shall be informed without delay in writing.

(4) If the transfer referred to in Paragraph two of this Section is not possible, the trusted certification service provider shall transfer the data associated with the certification service, information, databases, registers, other pertinent information, the information system and certification service under the supervision of the supervisory institution to the State archives.

(5) A signatory after receiving information regarding the termination of the activities of the trusted certification service provider, declaration of insolvency or suspension of service provision is entitled to transfer his or her own data associated with the issued qualified certificate to another trusted certification service provider at his or her discretion.

(6) The supervisory institution shall, without delay, revoke the accreditation of the terminated, declared insolvent or service provision suspended trusted certification

service provider, and shall include the information regarding this in the trusted certification service provider register.

Chapter VII

Duties and Liability of Trusted Certification Service Providers and Signatories

Section 23. Duties of Trusted Certification Service Providers

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 utilisation 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 regulatory enactments;
- 4) to ensure that signatory personal identification information is included in the qualified certificate only on the basis of a personal identification document presented in the presence of the signatory;
- 5) to ensure that the qualified certificate is issued by entering into a contract with the signatory regarding the provision of certification services;
- 6) before entering into a contract, informing the signatory in writing regarding the regulations and conditions that relate to the use of qualified certificates, including regarding any restrictions on the use of certificates, regarding procedures for examining complaints and disputes, and regarding the civil liability of the certification service provider. Information may be sent electronically and confirmed with the secure electronic signature of the trusted certification service provider. Relevant parts of this information shall be made available to persons who rely on the qualified certificate upon the request of such persons;
- 7) before entering into a contract, informing the signatory in writing regarding the certification service provision regulations and security measures, which are performed by the trusted certification service provider in order to prevent the illegal use of the issued qualified certificate;
- 8) after the issue of a qualified certificate, informing the signatory in writing regarding the conditions included in the certificate and restrictions regarding the use of the certificate;
- 9) to comply with this Law, other regulatory enactments, certification service provision regulations published in the trusted certification service providers register and the description of the certification service provision information system and procedure security;

- 10) to inform the supervisory institution, without delay, regarding all circumstances that hinder compliance with this Law, other regulatory enactments, certification service provision regulations published in the trusted certification service providers register and the description of the certification service provision information system and procedure security;
- 11) to revoke without delay, a qualified certificate in the cases referred to in Section 18, Paragraph two of this Law;
- 12) if the facts referred to in Section 18, Paragraph two, Clauses 2 and 3 cannot be verified without delay and without doubt, to suspend the operation of the qualified certificate until the relevant facts have been ascertained;
- 13) to inform the signatory, his or her authorised persons or heirs, without delay, regarding the revocation of the qualified certificate or its suspension of operation;
- 14) to maintain continuously in the free of charge and freely accessible on-line regime, full electronic signature-verification data, and issued, revoked, suspended and renewed qualified certificate registers and time-stamp register;
- 15) to perform full accounting of the issuance, revocation, suspension of operation and renewal of qualified certificates, as well as of time-stamp procedures;
- 16) to preserve information associated with qualified certificates and time-stamps for a specified time according to procedures specified in this Law and other regulatory enactments;
- 17) to regularly perform with the information system associated with the provision of certification services, an equipment and procedure security audit and to preserve the audit notes; In the audit notes shall be recorded all measures which are associated with the issuance, revocation, suspension of operation and renewal of qualified certificates, and measures which are associated with the stamping of electronic documents with a time stamp, as well as any other data changes; The audit notes shall be preserved permanently. The audit notes shall be secured by the physical and logical protection specified in regulatory enactments;
- 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 electronic signature-creation data;
- 20) to ensure that the time-stamp indicates an internationally co-ordinated precise time;
- 21) according to the procedures specified by regulatory enactments, 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 comply with the Personal Data Protection Law and regulatory enactments that regulate the security of information systems;

23) to transfer revoked and operation terminated qualified certificate registers to the State archive in accordance with Cabinet regulations that determine the procedures and time periods in which electronic documents shall be evaluated, collected and transferred to the State archive; and

24) to insure for its own civil liability.

Section 24. Liability of Trusted Certification Service Providers

(1) A trusted certification service provider shall be liable for losses that are caused to a person who reasonably relied upon the qualified certificate in relation to:

1) compliance with the requirements of this Law or other regulatory enactments in the issuing a qualified certificate, as well as compliance with and fulfilment of the trusted certification service provision regulations included in the trusted certification service providers register or the description of the certification service provision information system, equipment and procedure security;

2) the information included in the qualified certificate;

3) the conformity of the electronic signature-creation data to the electronic signature-verification data included in the certificate at the moment of the issue the qualified certificate; and

4) the utilisation of the electronic signature-creation data and electronic signature-verification data in an appropriate way.

(2) A trusted certification service provider shall be liable for losses that are caused to a person who reasonably relied upon the qualified certificate if the revocation or suspension of operation of such certificate has not registered.

(3) A trusted certification service provider shall not be liable for losses that are caused to a person who reasonably relied upon the qualified certificate that is utilised disregarding the conditions or restrictions included therein or exceeds the transaction amount restriction indicated in the certificate.

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) before entering into a contract regarding certification service provision, to confirm in writing that he or she has become acquainted with the certification service provision regulations published in the trusted certification service providers register, the description of the certification service provision information system, equipment and procedures security and other security measures which the trusted certification

service provider has performed in order 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 utilised without the knowledge of the signatory;

5) to request without delay that the trusted certification service provider to revoke the qualified certificate or to suspend the operation thereof if there is a basis to believe that the electronic signature-creation data have been utilised without the knowledge of the signatory; and

6) to request without delay that the trusted certification service provider revoke 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 utilisation; and

3) there has been a basis to believe that the electronic signature-creation data has been utilised 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.

Chapter VIII

Recognition of Qualified Certificates Issued in Foreign States

Section 26. Recognition of Qualified Certificates Issued in Foreign States

Qualified certificates issued in foreign states shall have the legal status and legal effect specified in this Law if the status of the certificate and the electronic signature-verification data associated with the certificate can be verified being located in the Republic of Latvia, and the qualified certificate conforms to at least one of the following conditions:

1) it conforms to all of the requirements of this Law and other regulatory enactments;

2) a certification service provider voluntarily accredited to the supervisory institution has submitted it;

3) a certification service provider voluntarily accredited to the supervisory institution has guaranteed it;

4) it is recognised in the Republic of Latvia in accordance with international agreements; or

5) a certification service provider accredited in a Member State of the European Union has issued it or a certification service provider accredited in a Member State of the European Union guarantees it.

Transitional Provision

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

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,

The Chairperson of the Saeima

I. Ūdre

Rīga, 20 November 2002