REPUBLIC OF LITHUANIA

LAW ON ELECTRONIC SIGNATURE

July 11, 2000. No. VIII – 1822

(amended as of June 6, 2002. No. IX – 934)

Vilnius

CHAPTER I

GENERAL PROVISIONS

ARTICLE 1. Purpose of the Law

1. This Law shall regulate the creation, verification, and validity of electronic signature, signature users' rights and obligations, establish the certification services and requirements of their providers and the rights and functions of the institution of electronic signature supervision.

2. This Law shall not regulate the use of the signature-creation data, signature-verification data and use of electronic-signature-device to ensure confidentiality of information.

ARTICLE 2. Basic Definitions of this Law

1. Person is an enterprise, not having the rights of a legal person, a natural or legal person, including foreign persons.

2. Electronic Data (hereinafter referred to as-Data) includes all data processed by information technology means.

3. Data Processing includes all operations with data: selection, recording, classification, grouping, accumulation, storing, exchanging, copying, connecting, disclosure, supply, use and destruction.

4. Electronic Signature (hereinafter referred to as-Signature) means data, which are inserted, attached to or logically associated with other data for the purpose of confirming the authenticity of the latter and (or) identification of the signatory.

5. Secure-electronic-signature means signature, which meets all of the requirements indicated in this paragraph:

1) it is uniquely linked to the signatory;

2) it is capable of identifying the signatory;

3) it is created using a means that the signatory can maintain under his sole control;

4) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

6. Signed-data means data, to which an electronic signature is inserted, attached to or logically associated with.

7. Signatory means a capable natural person, who holds a signature-creation device and, acting voluntarily either on his own behalf or on behalf of the other person, whom he represents, creates a signature.

8. Signature-users means persons, who use electronic signature in their activity or obtain signed data from other persons.

9. Signature-creation-data means unique data, which are used by the signatory to create a signature.

10. Signature-creation-device means configured computer software and (or) hardware, used to implement the signature-creation data.

11. Secure-signature-creation-device means a signature-creation device which meets all of the requirements laid down in this paragraph:

1) the signature - creation data used for electronic signature generation can practically occur only once, and their secrecy is reasonably assured;

2) the signature-creation data, used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;

3) the signature creation data used for signature generation can be reliably protected by the legitimate signatory against the use of others;

4) in generating the signature, signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

12. Signature-verification-data means unique data, used in verifying an electronic signature.

13. Signature-verification-device means configured software and (or) hardware used to implement the signature-verification-data.

14. Certificate means an electronic attestation, which links signature-verification data to a signatory and confirms or allows to establish the identity of that signatory.

15. Qualified-certificate means a certificate produced by a certification-service-provider who fulfils the requirements laid down by the Government or its authorised institution. This certificate contains the following data:

1) notation to indicate that it is a qualified-certificate;

2) identifiers of the certification-service-provider and his country of residence;

3) name and surname or the pseudonym of the signatory ;

4) specific attributes of the signatory, if that is required considering the projected goals of the certificate's use;

5) signature-verification data, which corresponds to the signature-creation data under the control of the signatory;

6) periods of the beginning and end of validity of the certificate;

7) certificate identifier, supplied by certification-service-provider;

8) secure-electronic-signature of the certification-service-provider;

9) limitations on the scope of use of the certificate, if applicable;

10) limits of the value of transactions fort which the certificate can be used, if applicable;

16. Certification-service-provider means an enterprise, not having the rights of a legal person, or a legal person who issues certificates or provides other services related to electronic signature.

17. Electronic signature device means configured computer software and (or) hardware or the corresponding component thereof, used by certification service-providers in providing services linked with signature, or which are used in signature creation or verification.

CHAPTER II

SIGNATURE CREATION, VERIFICATION, VALIDITY, RIGHTS AND RESPONSIBILITY OF SIGNATURE-USERS

ARTICLE 3. Generation of Signature-creation and Verification Data

1. Following the request by a person, who has decided to use signature in his activities, the certification-service-provider, using an electronic-signature-device, shall create for him signature creation and verification data. This data may be created by the person himself.

2. A certification-service-provider who issues qualified-certificates must give the signature-creation-data only to the person upon whose request they had been created, without keeping a copy of such for himself and ensuring their secrecy.

3. Signature-verification-data shall be public. The certification-service-provider shall enter them in the certificate of the signatory and provide it to all signature users. Should the signatory himself have generated the signature-creation and verification data, to issue a certificate, he shall transfer the signature-verification-data to the certification-service-provider.

ARTICLE 4. Issuing and Processing of Certificates

1. Certification-service-providers shall issue and process the certificates of signatories.

2. A natural person, requesting the certification-service-provider to issue his certificate, must submit some documents confirming his identity and the other information, which is requested to be included in the certificate.

3. A natural person, upon whose request a certificate has been issued, shall be liable for the authenticity of the documents in accordance with the laws of the Republic of Lithuania.

4. The certification-service-provider shall suspend the validity of the certificate:

1) upon a request by the signatory;

2) upon the request by law enforcement institutions authorised by the Government, in seeking to prevent crimes;

3) upon receiving information that the certificate data is false or that the signatory has lost control of signature-creation data corresponding to his certificate.

5. Suspension of the validity of the certificate shall be revoked upon obtaining a request by the signatory or a law enforcement institution authorised by the Government, upon the request whereof the validity of the certificate had been suspended. Should the validity of the certificate be suspended for reasons indicated in item 3 of paragraph 4 of this Article, suspension of the validity of the certificate shall be revoked upon the receipt of a request and explanation by the signatory, denying the information received from the certification-service-provider. Failure to receive such a request and explanation within one month of suspension of certificate validity, shall result in revocation of validity of the certificate.

6.A certification-service-provider shall revoke the validity of the certificate:

1) upon a request by the signatory;

2) upon loss of control by the signatory of signature-creation-data corresponding to the certificate;

3) upon the determination that false data have been submitted for issuing the certificate;

4) based upon the limitations of validity of the certificate, stipulated in the certificate in issuing it;

5) upon being informed, that the signatory has become incompetent;

6) upon being informed that the signatory has died;

7) upon violation by the signatory of the legal acts regulating use of signature or the conditions of the contract with the certification-service-provider;

8) upon the request of a person, whom the signing person has the right to represent, according to the information indicated on the certificate.

9) other instances established by laws.

7. The signatory must approach the certification-service-provider, who issued his certificate, concerning revocation of the validity of the certificate, if he has lost control of signature-creation-data corresponding to the certificate.

8.The signing person must immediately inform the certification-service-provider, who issued his certificate of changes in the data, indicated on the certificate, supplying documents which attest this. If informing about the decrease in the scope of the rights, indicated on the certificate, the documents attesting the changes in data shall not be required.

9.The damage incurred as a result of unlawful suspension or revocation of validity of the certificate, must be compensated by the persons responsible for it, according to the laws of the Republic of Lithuania.

ARTICLE 5. Validity of Foreign State Certificates

1. Qualified-certificates, issued by foreign state certification-service-providers shall be considered legally equivalent to the qualified-certificates issued by the Republic of Lithuania certification-service-providers, if:

1) they are issued by a certification-service-provider, who is accredited in the Republic of Lithuania;

2) they are issued by a certification-service-provider who is accredited in the European Union;

3) the certificate is guaranteed by the certification-service-provider of the

Republic of Lithuania, who corresponds to the requirements established by the Government or an institution authorised by it for certification-service-providers who issue qualified-certificates;

4) the certificate is guaranteed by a certification-service-provider of a European Union Member State, corresponding to the equivalent requirements for certified-service-providers who issue qualified-certificates, established by the Government of the Republic of Lithuania or an institution authorised by it.

2. Those foreign state certification-service-providers and the certificates issued by them, whose recognition is based upon international agreements shall also be recognised in the Republic of Lithuania.

ARTICLE 6. Creation of Signature

1. The signatory shall create a signature by means of a signature-creation-device from the data to be signed and signature-creation-data belonging to him alone.

2. The signatory shall be liable for the protection of signature-creation-data and signature-creation-device.

3. The signatory shall not have the right to transfer signature-creation-data to another natural person.

ARTICLE 7. Verification of Signature

1.Verification of signature means establishment of signed data authenticity and establishment of the validity of signature and identification of the signatory thereof.. The signature shall be verified with signature-verification-device, using signed data and certificate of signatory.

2. The institution of electronic signature supervision shall set the requirements for the procedure of signature verification.

3. The recipients of signed data shall be responsible for verification of the signature and keeping the device being used for this purpose.

ARTICLE 8. Force of Signature

1. A secure-electronic-signature, created by a secure-signature-creation-device and based on a qualified-certificate which is valid, shall have the same legal force that a hand-written signature in written documents has and shall be admissible as evidence in court.

2. A signature may not be deemed invalid based on any of the grounds listed below, that it is:

1) in electronic form;

2) not based upon a qualified-certificate:

3) not based upon a qualified-certificate issued by an accredited certification-service-provider;

4) not created by a secure signature-creation device.

3. In all cases, the electronic signature shall have the legal power laid down in paragraph one of this Article, provided that the signature users shall reach an agreement among themselves.

4. The power of the electronic signature of a legal person shall be given the same recognition as that signed by a representative of the legal person, confirmed by the stamp of the legal person, appearing in written documents, taking into account the power of the electronic signature in accordance with paragraphs one, two and three of this Article.

CHAPTER III

CERTIFICATION SERVICES AND REQUIREMENTS FOR THEIR PROVIDERS

ARTICLE 9. Certification Services

1. Certification-service-providers shall provide these certification services, linked to signature use:

1) primary - certificate issuing and provision of certificate data to signature users for signature verification;

2) secondary - creation of the time stamp of signed data, person consultation, person registration to obtain certificates and other services assigned to this category;

2. The institution of electronic signature supervision shall determine the procedure of the provision of secondary services.

ARTICLE 10. Registration of Certification Service Providers

Certification-service-providers of the Republic of Lithuania who issue qualified-certificates, must register with the institution of electronic signature supervision according to the procedure established by the Government or its authorised institution.

ARTICLE 11. Accreditation of Certification-service -providers

1. Certification-service-providers may voluntarily accredit themselves with an institution of electronic signature supervision. Accreditation is the assessment of a certification-service-provider's ability to perform his functions. Accreditation is not a required condition of certification-service-providers.

2. An institution of electronic signature supervision shall establish the requirements of voluntary accreditation of certification-service-providers and procedure of accreditation.

3. The number of certification-service-providers desirous of accreditation shall be unlimited.

ARTICLE 12. Obligations, Rights and Liability of Certification-service-providers

1. In order to issue a certificate, a signatory shall sign a contract with a certification-service-provider. In drawing up a contract, the certification-service-provider must:

1) inform the signatory regarding the procedure, use and limitations of the certificate and voluntary accreditation of the certification-service-provider;

2) in issuing a signatory's certificate, require that the person

submit documents confirming his identity;

3) ensure protection of a person's data, regulated by the Law on

Legal Protection of Personal Data and other Republic of Lithuania laws.

2. A certification-service-provider must:

1) provide certificate data for signature users for verification of signatures twenty-four hours per day;

2) suspend or revoke without any delay, the validity of a signatory's certificate in instances stipulated in paragraphs 4 and 6 of Article 4;

3) inform without any delay, the signatory concerning the suspension or revocation of his certificate;

4) revoke without any delay, the suspension of validity of the certificate, upon receiving a request from the signatory or a law enforcement institution authorised by the Government, upon the request whereof it had been suspended.

3. A certification-service-provider who issues qualified-certificates must:

1) collect the information stipulated by the Government or an institution authorised by it, pertaining to certificate processing and replies to inquiries posed by signature users and to keep it for the stipulated length of time;

2) insure own civil responsibility by a sum no less than that stipulated by the institution of electronic signature supervision.

4. A certification-service-provider, who issues qualified-certificates, shall have the right to set limitations of certificate use purpose, limits of the value of transactions, when the certificate may be used, and shall not be liable for the damage suffered by signature users, should the limitations indicated in the certificate have been violated.

5. A certification-service-provider who issues qualified-certificates shall be liable for:

1) accuracy of issued certificate's data;

2) that the person indicated in the issued certificate is the holder of the signature-creation-data, corresponding to the signature-verification-data indicated in the certificate;

3) correlation between signature-creation-data and signature-verification-data, when he creates both these data, upon the request of the person;

4) suspension or revocation of the validity of the certificate on time.

6. A certification-service-provider, who issues qualified-certificates or guarantees the qualified-certificates issued by other certification-service-providers, shall compensate signature users for inflicted damages, according to the procedure established by laws.

ARTICLE 13. Revocation of Certification Service Provision

1. A certification-service- provider must no later than one month prior to the revocation of certification service, inform of this the signatories, whose certificates he issued and whose certificates are valid, as well as other certification-service-providers, with whom he has signed contracts of guarantee.

2. A certification-service-provider may revoke the validity of all the certificates he issued no earlier than one month after the announcement concerning the projected revocation of certification-service-provision.

3. A certification-service-provider, issuing qualified-certificates, must no later than one month prior to revocation of the certification service, inform the institution of electronic signature supervision, concerning this.

4. A certification-service-provider who issues qualified-certificates must, within one month from the announcement of the projected revocation of certification-service-provision, hand over all of his issued qualified-certificates and information stipulated by the institution of electronic signature supervision, concerning certificate processing and the inquiries by signature users, to a successor of the activity or institution of electronic signature supervision.

CHAPTER IV

SUPERVISION OF ELECTRONIC SIGNATURE

ARTICLE 14. Functions of Institution of Electronic Signature Supervision

1. An institution authorised by the Government shall perform the functions of electronic signature supervision.

2. The institution of electronic signature supervision shall:

1) draft the requirements of signature equipment;

2) draft the requirements for certification-service-providers issuing qualified-certificates;

3) establish the requirements of the procedure of signature verification;

4) establish the requirements and procedure of voluntary accreditation for certification-service-providers;

5) accredit certification-service-providers;

6) draft the procedure of registration of certification-service-providers who issue qualified-certificates, register them and openly publish the list thereof in the “Official Gazette;”

7) supervise how the information linked to qualified-certificate managing and signature users inquiries, collected by a certification-service-provider, is being managed;

8) revoke by his request, the registration of a certification-service-provider who issues qualified-certificates;

9) establish the procedure of providing secondary certification services;

10) maintain contact with corresponding institutions of electronic

signature supervision abroad exchange information, collect and openly publish it;

11) prepare annual accounts of the implementation of this Law no later than by the first day of April of each year and submit them to the Government and Seimas.

12) perform the other functions defined in the by-laws of this institution.

ARTICLE 15. Rights of Institution of Electronic Signature Supervision

1. An institution of electronic signature supervision shall have the right to revoke the accreditation of an accredited certification-service-provider, having established that he violated the requirements set forth for accredited certification-service-providers.

2. An institution of electronic signature supervision shall have the right to warn a certification-service-provider who issues qualified-certificates and to suspend or annul his registration, upon having established that he has violated the requirements set forth by the Government or its authorised institution, for certification-service-providers who issue qualified-certificates.

3. The decisions adopted by institutions of electronic signature supervision regarding accreditation of an accredited certification-service-provider or the revocation of registration of a certification-service-provider who issues qualified-certificates, shall be appealed in accordance with the procedure established by laws.

CHAPTER V

FINAL PROVISIONS

ARTICLE 16. Implementation of the Law

1. The Government shall approve the legal acts, which are drafted according to sub-paragraphs one, two and six of paragraph two of Article 14 of this Law, by the institution, which manages the electronic signature.

2. Items 2 and 4 of paragraph 1 of Article 5 shall come into force, following the accession of the Republic of Lithuania to the to the European Union.

I promulgate this Law passed by the Seimas of the Republic of Lithuania.

PRESIDENT OF THE REPUBLIC VALDAS ADAMKUS