

227/2000 Coll.

ACT

of 29th June 2000

on Electronic Signature and change to some other laws (Electronic Signature Act)

Amendment: 226/2002 Coll.

Amendment: 517/2002 Coll.

Amendment :440/2004 Coll.

Amendment: 635/2004 Coll.

Amendment: 501/2004 Coll., 444/2005 Coll.

The Parliament has hereby agreed on this Act of the Czech Republic:

FIRST PART

ELECTRONIC SIGNATURE

Section 1

Subject of the Act

In compliance with the law of the European Communities this Act shall regulate: 1) the use of electronic signature, electronic sign, the provision of certification services and related services rendered by providers domiciled in the territory of the Czech Republic, control of the duties laid down by this Act, and sanctions imposed for the violation of duties laid down therein.

Section 2

Definition of Some Terms

For the purpose of this Act, the following terms are understood to mean:

a) electronic signature means data in electronic form which are attached to a data message or which are logically connected therewith, and which serve as a method for unequivocal identification of the identity of the person signed in relation to the given data message,

b) guaranteed electronic signature means an electronic signature that meets the following requirements:

1. it shall be unequivocally connected with the signing person,
2. it shall facilitate identification of the signing person in relation to the given data message,
3. it shall be created and attached to the given data message by such means which the signing person can keep under its exclusive control,
4. it shall be attached to the data message to which it is related by such a method which provides for the identification of any subsequent change of data,

c) electronic sign means data in electronic form which are attached to the given data message or which are logically connected therewith, and which meet the following requirements:

1. they shall be unequivocally connected with the designating person and facilitate its identification through a qualified system certificate,

2. they shall be created and attached to the given data message by means for the creation of electronic signs which the designating person can keep under its exclusive control,
3. they shall be attached to the data message to which they are related by such a method which provides for the identification of any subsequent change of data,

d) data message means electronic data which can be transferred by means of electronic communication and stored on storage media used for the processing and transfer of data in electronic form,

e) signing natural person which is the holder of the means for the creation of electronic signatures and which acts in its own name or on behalf of another natural person or legal entity,

f) designating person is a natural person, a legal entity or an organizational component of the state which holds the means for the creation of electronic signs and which designates the given data message with an electronic sign,

g) certificate holder means a natural person, a legal entity or an organizational component of the state which has applied for the issuance of a qualified certificate or a qualified system certificate for itself or for the signing or designating person, and to which the certificate has been issued,

h) provider of certification services means a natural person, a legal entity or an organizational component of the state that issues certificates and keeps records thereof, eventually rendering other services connected with electronic signatures,

i) qualified provider of certification services means a provider of certification services who issues qualified certificates or qualified system certificates or qualified time stamps or means for safe creation of electronic signatures (hereinafter "qualified certification services") and who has met its reporting duty pursuant to section 6,

j) accredited provider of certification services means a provider of certification services who has been granted accreditation pursuant to this Act,

k) certificate means a data message issued by a provider of certification services, integrating data for the verification of electronic signatures with the signing person, and providing for the verification of its identity, or integrating data for the verification of electronic signs with the designating person, and providing for the verification of its identity,

l) qualified certificate means a certificate which has the essential elements pursuant to section 12 and which has been issued by a qualified provider of certification services,

m) qualified system certificate means a certificate which has the essential elements pursuant to section 12a and which has been issued by a qualified provider of certification services,

n) data for the creation of electronic signatures are singular data which the signing person uses for the creation of electronic signature,

o) data for the verification of electronic signatures are singular data used for the verification of electronic signature,

p) data for the creation of electronic signs are singular data used by the designating person for the creation of electronic signs,

q) data for the verification of electronic signs are singular data used for the verification of electronic signs,

r) qualified time stamp means a data message which has been issued by a qualified provider of certification services and which integrates data in electronic form with the given moment in time in a credible manner, and guarantees that the given data in electronic form indeed existed before the given moment in time,

s) means for the creation of electronic signatures refer to a technical device or programming equipment used for the creation of electronic signatures,

t) means for the verification of electronic signatures refer to a technical device or programming equipment used for the verification of electronic signatures,

u) means for the safe creation of electronic signatures refer to means for the creation of electronic signature which meets the requirements laid down by this Act,

v) means for the safe verification of electronic signatures refer to means for the verification of signature which meets the requirements laid down by this Act,

w) instrument of electronic signature means a technical device or programming equipment or components thereof, used for the safeguarding of certification services or for the creation or verification of electronic signatures,

x) means for the creation of electronic signs refer to an equipment which is used by the designating person for the creation of electronic signs and which meets the other elements laid down by this Act,

y) electronic registry means a workplace of a public administration body destined for the reception and dispatch of data messages,

z) accreditation means a certificate proving that the given provider of certification services meets the conditions laid down by this Act for the performance of the activities of an accredited provider of certification services.

Section 3

Compliance with the Requirements for Signature

(1) A data message shall be deemed signed, when equipped with an electronic signature. Unless proved contrary, it is believed that the signing person has been familiarized with the content of the data message before signing it.

(2) The use of guaranteed electronic signature based on qualified certificate and created by means for the safe creation of signature shall make it possible to verify that the given data message has indeed been signed by the person given in that qualified certificate.

Section 3a

(1) The use of electronic sign based on a qualified system certificate and created by means for the creation of electronic signs shall make it possible to verify that the given data message has indeed been designated by this particular electronic sign by the designating person.

(2) If the designating person has indeed designated the given data message, it shall be believed that the person has done so automatically without direct verification of the content of the given data message and has thus expressed its will.

Section 4

Compliance with the Original

The use of guaranteed electronic signature or electronic sign shall guarantee that should the content of the data message be violated since the moment when the message has been signed or designated, it shall be possible to ascertain such a violation.

Section 5

Duties of the Signing Person

(1) Signing person shall be obliged to:

- a) handle the means as well as the data for the creation of guaranteed electronic signature with due care to prevent their unauthorized use,
- b) notify, without delay, the provider of certification services who has issued the qualified certificate of an impending threat of misuse of its data for the creation of guaranteed electronic signature.

(2) Signing person shall be liable for damages caused by the violation of duties under section 1 pursuant to special legal regulations. 1a) However, the signing person shall be released from liability if it succeeds in proving that he who incurred the damage has failed to carry out all the acts necessary for verifying that the given guaranteed electronic signature is valid and its qualified certificate has not been invalidated.

Section 5a

Duties of the Designating Person

(1) Designating person shall be obliged to:

- a) handle the means as well as the data for the creation of electronic signs with due care to prevent their unauthorized use,
- b) notify, without delay, the provider of certification services who has issued the qualified system certificate of an impending threat of misuse of its data for the creation of electronic signs.

(2) Designating person shall be obliged to ensure that the means for the creation of electronic signs it uses meet the conditions laid down by this Act.

(3) Designating person shall be liable for damages caused by the violation of duties under subsection 1, even though it has not caused such damage itself, pursuant to special legal regulations, 1a) while the liability for defects pursuant to special legal regulations shall not be affected. However, the designating person shall be released from liability if it succeeds in proving that he who incurred damage has failed to carry out all the acts necessary for verifying that the given electronic sign is valid and its qualified system certificate has not been invalidated.

Section 5b

Duties of Certificate Holder

Certificate holder shall be obliged to provide, without undue delay, accurate, truthful and complete information to the provider of certification services in relation to the pertinent qualified certificate and in relation to the pertinent qualified system certificate.

Section 6

Qualified Provider of Certification Services

- (1) Qualified provider of certification services shall be obliged to
- a) ensure that anybody can make sure of his/her identity and his/her qualified system certificate on the basis of which he/she designates the issued qualified certificates or qualified system certificates and lists of certificates that have been invalidated, or qualified time stamps,
 - b) ensure that qualified certification services shall be provided by persons endowed with specialized knowledge and qualifications vital for providing qualified certification services and well versed in the appropriate security procedures,
 - c) use safe systems and safe instruments of electronic signature, ensure adequate safety of the procedures supporting those systems and procedures, and safeguard adequate cryptographic safety of those instruments; systems and instruments shall be deemed safe if and when meeting the requirements laid down by this Act and the executive regulation to implement the law, or if and when meeting the requirements of the technical standards given in the Commission Decision issued pursuant to Article 3 (5) of the Directive 99/93/EC,
 - d) use safe systems for the storage of qualified certificates and qualified system certificates or qualified time stamps in a verifiable form in a manner to ensure that records shall be kept or their changes made solely by authorized persons, and make it possible to check the correctness of records and to secure that any technical or programming changes violating those security requirements shall be evident,
 - e) have at his/her disposal throughout the time of his/her activities sufficient financial resources or other financial provisions to cover the operation in compliance with the requirements laid down in this Act and with a view to the risk of arising liability for damages,
 - f) prior to the conclusion of contract on the provision of qualified certification services with a person applying for the provision of services under this Act, inform that person in writing of the precise terms for using qualified certification services, complete with eventual limitations of their use, the terms of warranty claims and solution of arising disputes, and whether or not

such a person is accredited by the Ministry of Informatics (hereinafter the "Ministry") pursuant to Section 10; such information may be provided in electronic form.

(2) If not accredited by the Ministry, the provider of certification services shall be obliged to report to the Ministry at least 30 (thirty) days before the start of providing qualified certification service that he/she shall provide such services, and the moment when he/she starts providing such services. At the same time, he/she shall submit to the Ministry for verification his/her own qualified system certificate, as given in subsection 1 a).

(3) If accreditation has been withdrawn by the Ministry from qualified provider of certification services who acquired accreditation pursuant to section 10 of this Act, he/she shall be obliged, without delay, to notify of this fact the subjects to whom he/she provides his/her qualified certification services, and other persons concerned.

(4) Qualified provider of certification services shall provide services under this Act on the basis of contract. Such contract must be executed in writing.

(5) Qualified provider of certification services shall keep the information and documentation relating to the qualified certification services rendered, namely

- a) contract on the provision of qualified certification services, including the application for the provision of services,
- b) issued qualified certificate, issued qualified system certificate, or issued qualified time stamp,
- c) copies of the signing person's personal documents submitted or documents on the basis of which the identity of the designating person has been verified,
- d) certificate on the receipt of qualified certificate or qualified system certificate by its holder, eventually his/her consent with the publication of the given qualified certificate in the list of issued qualified certificates,
- e) statement by the certificate holder to the effect that he/she has been given information pursuant to subsection 1 f),
- f) documents and records relating to the life cycle of the issued qualified certificate or qualified system certificate whose essential elements shall be further specified by executive regulation.

(6) Qualified provider of certification services shall keep all the information and documentation on the services rendered under this Act for at least 10 (ten) years. Qualified provider shall be obliged to secure the information and documentation thus kept against loss, misuse, destruction and damage under the conditions to be specified by executive regulation. Pursuant to the first sentence, qualified provider of certification services shall be allowed to provide and keep information and documentation in electronic form. Unless stipulated otherwise by this Act, information and documentation shall be handled pursuant to special legal regulation. 2)

(7) Employees of qualified provider of certification services, eventually other natural persons who come into contact with personal data and data for the creation of electronic signatures of signing persons and with electronic signs of designating persons shall be obliged to keep the pledge of confidentiality of those data and security measures whose disclosure would jeopardize the safeguarding of those data. The pledge of confidentiality shall last even after the termination of the employment or other similar relationship, or after the completion of appropriate works; the said persons may be absolved of their pledge of confidentiality only by the person in whose interest that pledge has been made, or by a court.

Section 6a

Duties of Qualified Provider of Certification Services when Issuing Qualified Certificates and Qualified System Certificates

(1) Qualified provider of certification services who issues qualified certificates or qualified system certificates (hereinafter "certificates issued as qualified") shall be obliged to:

- a) ensure that certificates issued by him/her as qualified shall contain all the essential elements laid down by this Act,
- b) ensure that certificates issued by him/her as qualified shall be accurate, truthful and complete,
- c) while using appropriate means, safely verify, before the issue of a certificate as qualified, the identity of the signing person or the identity of the designating person, eventually its special features, if and when required by the purpose of such a certificate,
- d) find out whether, at the moment of submitting application for the issue of a certificate as qualified, the signing person had at its disposal the personal data for the creation of electronic signatures corresponding with the data for the verification of electronic signatures, or the designating person had the data for the creation of electronic signatures corresponding with the data for the verification of electronic signs, as required by the application for the issue of certificate,
- e) ensure the operation of a safe and publicly accessible list of certificates issued as qualified for the publication of which the certificate holder has given his/her consent in compliance with section 6 subsection 5 d), and to provide for this list to be available also to remote access, and for the data contained in the list to be updated with each change without undue delay,
- f) ensure the operation of a safe and publicly accessible list of certificates issued as qualified which have been invalidated, also by remote access,
- g) ensure that the date and the time giving the actual hour, minute and second when the pertinent certificate issued as qualified was really issued or invalidated shall be accurately determined,
- h) adopt adequate measures against the misuse and forgery of certificates issued as qualified,
- i) provide, on request, to third parties substantive information on the conditions for using certificates issued as qualified, including limitations of their use, and information on whether

it has been accredited by the Ministry or not; such information may be provided electronically.

(2) If qualified provider of certification services who issues certificates as qualified creates for the signing person data for the creation of electronic signatures, or for the designating person data for the creation of electronic signs, he/she:

- a) must ensure the classification of such data before their submission, he/she shall not be allowed to copy such data and keep them longer than necessary,
- b) must guarantee that these data correspond with the data for the verification of electronic signatures, or the data for the verification of electronic signs.

(3) Qualified provider of certification services who issues certificates as qualified must invalidate certificate forthwith, if its holder, the signing person or the designating person requests so, or if he/she is notified of impending danger of the misuse of the data for the creation of electronic signatures or electronic signs, or in case the certificate has been issued on the grounds of false or erroneous data.

(4) Qualified provider of certification services must also invalidate forthwith certificate issued as qualified, if he/she has demonstrably learnt that the signing or designating person has died or has been extinguished or if court has rendered it incapable of legal acts or limited its capability of legal acts, 2a), or if the data on the basis of which the certificate has been issued have lost their truthfulness.

Section 6b

Duties of the Qualified Provider of Certification Services when Issuing Qualified Time Stamps

(1) Qualified provider of certification services who issues qualified time stamps shall be obliged to:

- a) ensure that the time stamps issued by him/her as qualified shall contain all the essential elements laid down by this Act,
- b) ensure that, when creating the given qualified time stamp, the time data inserted into the qualified time stamp shall correspond with the actual value of the coordinated global time,
- c) ensure that the data in electronic form, which constitute the subject of the application for the issue of qualified time stamp, shall unequivocally correspond with the data in electronic form contained in the issued qualified time stamp,
- d) adopt adequate measures against forgery of qualified time stamps,
- e) provide, on request, to third persons substantive information on the conditions for using qualified time stamps, including limitations of their use, and information whether he/she has been accredited by the Ministry or not; such information may be provided electronically

(2) Qualified provider of certification services shall issue a qualified time stamp without delay after receiving request for its issuance.

Section 7

Liability for Damage

(1) Qualified provider of certification services shall be responsible for damage caused by the violation of duties laid down by this Act pursuant to special legal regulations. 1a)

(2) Qualified provider of certification services shall not be responsible for damage which ensues from the use of a certificate issued as qualified and which has been incurred as a result of non-compliance with the limitation imposed on its use pursuant to section 12 subsection 1 i) and j), and section 12a h).

Section 8

Protection of Personal Data

Protection of personal data shall be governed by a special legal regulation. 3)

Section 9

Accreditation and Supervision

(1) The granting of accreditation to act as accredited provider of certification services as well as supervision of the compliance with this Act shall belong to the Ministry.

(2) The Ministry shall

- a) grant and revoke accreditations to act as accredited provider of certification services to subjects operating in the territory of the Czech Republic,
- b) supervise the activities of accredited providers of certification services and qualified providers of certification services, imposing on them corrective measures and fines for violating duties under this Act,
- c) keep records of granted accreditations and their changes, and records of qualified providers of certification services,
- d) keep records of the issued qualified system certificates which are used by qualified provider of certification services pursuant to section 6 subsection 1 a) and which have been entrusted to the Ministry pursuant to section 6 subsection 2,
- e) publish, on an ongoing basis, a list of granted accreditations, a list of qualified providers of certification services, and their qualified services, and qualified system certificates pursuant to d), also in a mode facilitating remote access,
- f) evaluate compliance of the instruments of electronic signature with the requirements laid down by this Act and executive regulation,
- g) meet other duties laid down by this Act.

(3) For the purpose of performing supervision, accredited provider of certification services and qualified provider of certification services shall be obliged to enable authorized Ministry personnel, to an indispensable extent, access to its commercial and operational premises, submit, on request, all the documentation, records, documents, written documents and other background materials connected with

his/her activities, enable them, to an indispensable extent, access to his/her information system, and provide information, and all necessary coordination.

- (4) Unless stipulated otherwise by this Act, the Ministry shall proceed in the performance of its supervision pursuant to a special legal regulation 4)
- (5) Qualified provider of certification services who has failed to meet the coordination duty pursuant to subsection 3, may receive disciplinary fine up to the sum of 1 000 000 Kč.

Section 10

Conditions for Granting Accreditation for the Provision of Certification Services

(1) Each provider of certification services may ask the Ministry to be granted accreditation for the performance of the activity of accredited provider of certification services.

(2) In his/her application for accreditation pursuant to subsection 1, the applicant shall be obliged to establish the following:

- a) in case of a legal entity, its commercial company or name, seat, eventually the address of the organizational constituent of a foreign person in the territory of the Czech Republic, and the applicant's identification number, if granted; in case of a natural person, its name, eventually names, surname, eventually annex, domicile, place of business, if different from the domicile, and the applicant's identification number, if granted,
- b) document on the authorization to business activity and for persons entered in the Commercial Register also statement from the Commercial Register not older than 3 (three) months,
- c) statement from the criminal records of businessman - natural person or statutory representatives of the legal entity in case the applicant is a legal entity, not older than 3 (three) months,
- d) factual, personal and organizational prerequisites for the activity of a qualified provider of certification services pursuant to sections 6, 6a and 6b of this Act,
- e) information on which particular certification services the applicant intends to provide.

(3) If application fails to contain all the required data, the Ministry shall suspend the procedure, and call on the applicant to supplement them within a stipulated deadline. If the applicant fails to do so within the given deadline, the Ministry shall terminate the procedure.

(4) If the applicant meets all the conditions for granting accreditation prescribed by this Act, the Ministry shall issue a ruling by which the accreditation shall be granted. In the opposite case, it shall reject the application for granting accreditation.

Section 10a

Terms for Expanding Services of Accredited Provider of Certification Services

(1) Accredited provider of certification services can expand the provision of qualified certification services by adding the issue of qualified certificates, qualified system certificates, qualified time stamps, or by issuing the means for safe creation of electronic signatures pursuant to this Act (hereinafter "enlarged services").

(2) Accredited provider of certification services shall be obliged to notify the Ministry of the expansion of services pursuant to subsection 1 so that the Ministry shall receive the notification at least 4 (four) months before the start of the provision of such services.

(3) In the notification, accredited provider of certification services must prove the factual, personnel and organizational prerequisites for securing enlarged services.

(4) If accredited provider of certification services fails to establish the facts pursuant to subsection 3, or if such facts prove to be incomplete or inaccurate, the Ministry shall notify the pertinent accredited provider of certification services, cautioning that if these defects are not eliminated within a deadline to be specified by the Ministry, it shall prohibit the expansion of services by its ruling.

(5) The Ministry shall prohibit expansion of services already announced if the accredited provider of certification services has failed to meet all the conditions prescribed for the provision of enlarged services.

(6) The Ministry shall issue a ruling on its ban on the expansion in providing qualified certification services within 90 (ninety) days of the moment it received the notification at the latest.

Section 11

(1) In the public administration sector, only guaranteed electronic signatures and qualified certificates issued by accredited providers of certification services (hereinafter "recognized electronic signature") may be used for the purpose of signature. This also applies to the exercise of executive power towards natural persons and legal entities. If a recognized electronic signature is used in the public administration sector, a qualified certificate must contain such data to render the given person unequivocally identifiable. The actual structure of data on the basis of which a person may be unequivocally identified shall be laid down by the Ministry in executive regulation.

(2) Written documents of public administration bodies in electronic form designated by an electronic sign, based on a qualified system certificate issued by an accredited provider of certification services or signed by a recognized electronic signature shall have the same legal effect as public instruments issued by those authorities.

(3) Public administration body shall receive and send data messages pursuant to subsection 1 through electronic registry.

Section 12

Essential Elements of Qualified Certificate

(1) Qualified certificate shall contain the following:
a) designation showing that it is being issued as a qualified certificate under this Act,

- b) in case of a legal entity, its commercial company or name and state where the qualified provider is domiciled; in case of a natural person, its name, eventually names, surnames, eventually annex, and state where the qualified provider is domiciled,
- c) name, eventually names, and surname of the signing person or its pseudonym with appropriate designation explaining that a pseudonym is involved,
- d) special signs of the signing person, if required by the purpose of the qualified certificate,
- e) data for the verification of signature corresponding with the data for the creation of signature that are under the signing person's control,
- f) electronic sign of the provider of certification services based on the qualified system certificate of the provider who issues the given qualified certificate,
- g) number of the qualified certificate unique for the given provider of certification services,
- h) beginning and end of the validity of the qualified certificate,
- i) eventually data on whether the use of the qualified certificate restricts the nature and scope solely for a specific application,
- j) eventually limitation of the value of transactions for which the given qualified certificate can be used.

(2) Limitations imposed on using the qualified certificate pursuant to subsection 1 i) and j) must be obvious to third parties.

(3) Qualified certificate may contain other personal data only with the consent of the signing person.

Section 12a

Essential Elements of Qualified System Certificate

Qualified system certificate shall contain the following:

- a) designation showing that it is being issued as a qualified system certificate under this Act,
- b) in case of a legal entity, its commercial company or name and state where the qualified provider is domiciled; in case of a natural person, its name, eventually names, surnames, eventually annex, and the state where the qualified provider is domiciled.
- c) unequivocal identification of the designating person, eventually of the means for the creation of electronic signs,
- d) data for the verification of electronic signs corresponding with the data for the creation of electronic signs that are under the designating person's control,

- e) electronic sign of the provider of certification services, based on the qualified system certificate of the provider who issues the given qualified system certificate,
- f) number of the qualified system certificate unique for the given qualified provider of certification services,
- g) beginning and end of the validity of the qualified system certificate,
- h) limitations imposed on using the qualified system certificate, while such limitations must be obvious to third parties.

Section 12b

Essential Elements of Qualified Time Stamp

Qualified time stamp shall contain the following:

- a) number of the given qualified time stamp unique for the provider of qualified certification services,
- b) designation of rules according to which provider of qualified certification services has issued the given qualified time stamp,
- c) in case of a legal entity, its commercial company or the name and state where the qualified provider is domiciled; in case of a natural person, its name, eventually names, surname, eventually annex, and the state where the qualified provider is domiciled,
- d) value of the time which corresponds with the coordinated global time when creating the given qualified time stamp,
- e) data in electronic form for which the qualified time stamp was issued,
- f) electronic sign of the qualified provider of certification services who issued the given qualified time stamp

Section 13

Duties of the Qualified Provider of Certification Services when Terminating Activities

(1) Qualified provider of certification services must report his/her intention to terminate his/her activity to the Ministry at least 3 (three) months prior to the planned day of termination of the said activities, and exert all the possible efforts to ensure that records kept pursuant to section 6 subsection 5 shall be taken over by another qualified provider of certification services. Qualified provider of certification services must also demonstrably notify each signing person, designating person and holder, to whom he/she provides his/her certification services, of his/her intention to terminate his/her activity at least 2 (two) months prior to the planned date of termination of activity.

(2) If qualified provider of certification services cannot ensure that the records kept pursuant to section 6 subsection 5 shall be taken over by another qualified provider of certification services, he/she shall be obliged, within 30 (thirty) days prior to the planned date of termination of activity at the latest, to report to the Ministry his/her intention to terminate

his/her activity. In such a case, the Ministry shall take over the record-keeping, and notify the subjects concerned.

(3) Provisions of subsections 1 and 2 shall also be reasonably applied when qualified provider of certification services extinguishes, dies or ceases to perform his/her activities, without complying with his/her reporting duty pursuant to subsection 1.

Section 14 Corrective Measures

(1) If the Ministry finds out that accredited provider of certification services or qualified provider of certification services has violated the duties laid down by this Act, it shall impose on him/her the duty to remedy the situation within a stipulated time limit, eventually specifying which particular measures this provider of certification services is obliged to adopt to eliminate the defects.

(2) If accredited provider of certification services has committed a more serious breach of the duties laid down by this Act, or fails to eliminate the defects ascertained by the Ministry within stipulated time limit, the Ministry shall be authorized to revoke the accreditation previously granted.

(3) If the Ministry decides on the revocation of accreditation, it can, concurrently, rule on the invalidation of the certificates issued as qualified by the given provider of certification services at the time of the validity of his/her accreditation.

Section 15 Cancellation of Qualified Certificate or Qualified System Certificate

The Ministry can order qualified provider of certification services, as a preliminary measure 7), invalidation of the certificate issued as qualified, if there is reasonable suspicion that the given certificate was forged or issued on the basis of false data. Decision on the invalidation of the certificate used as qualified may also be issued when it was established that the signing or designating person uses the means for the creation of signature or the means for the creation of electronic signs that display security defects that would make possible forgery of guaranteed electronic signatures or electronic signs, or an alteration of the signed or designated data.

Section 16 Recognition of Foreign Qualified Certificates

(1) Certificate issued by provider of certification services domiciled in a Member State of the European Union as qualified shall be a qualified certificate within the intentions of this Act.

(2) Certificate issued as qualified within the intentions of this Act in other than a Member State of the European Union shall be qualified certificate within the intentions of this Act if:

- a) the given provider of certification services meets the conditions of the European Communities legislation 1), and was accredited to act as an accredited provider of certification services in a Member State of the European Union,
- b) the given provider of certification services domiciled in a Member State of the European Union who meets the conditions laid down by the European Communities legislation, 1) shall assume responsibility for the validity and correctness of the certificate to the same extent as in his/her own qualified certificates, or
- c) this ensues from an International Treaty.

Section 17

Means for Safe Creation and Verification of Electronic Signatures

(1) Helped by appropriate technical and programming means and procedures, the means for safe creation of electronic signature shall ensure at least that:

- a) data for the creation of signature shall occur only once, and their classification shall be duly safeguarded,
- b) given adequate safeguards, data for the creation of signature shall not be deduced from the knowledge of the mode of their creation, and signature shall be protected against forgery by means of the existing available technology,
- c) data for the creation of signature shall be reliably protected by the signing person against misuse by a third party.

(2) Means for safe creation of electronic signature shall neither alter data they are signing nor prevent those data from being submitted to the signing person prior to the process of the signing proper.

(3) Prior to their use, means for safe creation and verification of electronic signatures must be safely issued and data for the creation of electronic signatures must be created in those means or added thereto in a credible manner.

(4) Helped by appropriate technical and programming means and procedures, the means for safe verification of signature shall ensure at least that:

- a) data used for the verification of signature shall correspond with the data displayed to the person verifying,
- b) signature shall be reliably verified and the result of this verification duly displayed,
- c) verifying person shall reliably ascertain the content of the signed data,
- d) truthfulness and validity of the certificate during the verification of the signature shall be reliably ascertained,
- e) the result of verification and the identity of the signing person shall be duly displayed,
- f) it shall be clearly stated that a pseudonym is used,

g) all the changes affecting security shall be established.

Section 17a

Means for the Creation of Electronic Signs

(1) Helped by appropriate technical and programming means and procedures, the means for the creation of electronic signs shall ensure at least that:

a) data for the creation of electronic signs shall be sufficiently classified and reliably protected by the designating person against misuse by a third party,

b) the signing person shall be notified that it commences the use of this particular means.

(2) Means for the creation of electronic signs shall be set in a way that, even without the designating person's additional check, precisely those and only those particular data messages selected by the designating person for designation shall be designated.

(3) Means for the creation of electronic signs shall be protected against unauthorized alteration and guarantee that such an alteration shall be obvious to the designating person.

Section 18

Administrative Delicts of Legal Entities

(1) Qualified provider of certification services who

a) fails to ensure that anybody can ascertain his/her identity and his/her qualified system certificate pursuant to section 6 subsection 1 a),

b) fails to ensure that qualified certification services shall be provided by persons with professional knowledge and qualifications necessary for the qualified certification services rendered and well versed in appropriate security procedures,

c) by failing to provide adequate security of the used systems and instruments of electronic signature and the procedures supporting those systems and instruments pursuant to section 6 subsection 1 c) and d) shall threaten the security of the qualified certification services being rendered,

d) has at his disposal no adequate financial resources or other financial provisions pursuant to section 6 subsection 1 e), thus threatening the security of the qualified certification services being rendered,

e) fails to meet the information duty pursuant to section 6 subsection 1 f), section 6 subsection 3, or section 13 subsection 1,

f) fails to meet the reporting duty pursuant to section 6 subsection 2, including the submission of qualified system certificate for verification, or pursuant to section 13 subsection 1, or 2,

g) provides certification services on the basis of contract other than written,

h) fails to keep information and documentation pursuant to section 6 subsection 5,

i) fails to keep all the information and documentation pursuant to section 6 subsection 6 for a period of at least 10 (ten) years, or

j) fails to keep the information and documentation against loss, misuse, destruction or damage pursuant to section 6 subsection 6,
shall be fined up to the sum of 10 000 000 Kè.

(2) Qualified provider of certification services who issues qualified certificates or qualified system certificates, and who

a) fails to ensure that the certificates issued by him/her as qualified shall contain all the essential elements laid down by this Act,

b) fails to ensure that the data given in the certificates issued as qualified shall be accurate, truthful and complete,

c) fails to verify the identity of the person pursuant to section 6a subsection 1 c),

d) fails to ensure data compliance pursuant to section 6a subsection 1 d),

e) fails to ensure the operation of a safe and publicly accessible list of certificates issued as qualified, and fails to ensure its accessibility and updating pursuant to section 6a subsection 1 e),

f) fails to ensure the operation of a safe and publicly accessible list of certificate issued as qualified which have been invalidated, also by remote access,

g) fails to ensure that the date and time with the specification of the hour, minute and second when the certificate issued as qualified was indeed issued or invalidated shall be precisely specified,

h) by failing to adopt adequate measures against the misuse and forgery of certificates issued as qualified shall threaten the security of the qualified certification services being rendered,

i) fails to meet the information duty pursuant to section 6a subsection 1 i),

j) fails to secure compliance and classification of data pursuant to section 6a subsection 2, if creating such data for the signing or designating person,

k) copies and keeps data pursuant to section 6a subsection 2, if creating such data for the signing or designating person, or

l) fails to invalidate the certificate pursuant to section 6a subsections 3 and 4, shall be fined up to the sum of 10 000 000 Kè.

(3) Qualified provider of certification services who issues qualified time stamps, and who

a) fails to ensure that the time stamps issued by him/her as qualified shall contain all the essential elements laid down in section 12b,

- b) fails to ensure that the time data inserted in the qualified time stamp shall correspond with the value of the coordinated global time when creating the given qualified time stamp,
- c) fails to ensure that the data in electronic form, which constitute the subject of the application for the issue of qualified time stamp, shall correspond with the data in electronic form contained in the issued qualified time stamp,
- d) fails to adopt adequate measures against forgery of qualified time stamps, thus threatening the security of the qualified certification services being rendered,
- e) fails to meet the information duty pursuant to section 6b subsection 1 e), or
- f) fails to issue qualified time stamp forthwith after the receipt of the application for its issue, shall be fined up to the sum of 10 000 000 Kè.

(4) Qualified provider of certification services who issues the means for safe creation of electronic signatures and who

- a) fails to issue the means for safe creation of electronic signatures safely pursuant to section 17 subsection 3, or
- b) fails to create in those means or fails to add thereto data for the creation of electronic signatures in a credible manner pursuant to section 17 subsection 3, shall be fined up to the sum of 10 000 000 Kè.

(5) Accredited provider of certification services who fails to meet the reporting duty pursuant to section 10a subsection 2 shall be fined up to the sum of 10 000 000 Kè.

(6) Accredited provider of certification services who violates the ban issued by the Ministry pursuant to section 10a subsection 5 shall be fined up to the sum of 10 000 000 Kè.

Section 18a

Administrative Infractions

(1) Qualified provider of certification services shall commit an administrative infraction by

- a) failing to ensure that anyone can ascertain his/her identity and his/her qualified system certificate pursuant to section 6 subsection 1 a),
- b) failing to ensure that qualified certification services shall be provided by persons endowed with specialized knowledge and qualifications vital for providing qualified certification services and well versed in appropriate security procedures,
- c) failing to ensure adequate security of the used systems and instruments of electronic signature and procedures supporting these system and instruments pursuant to section 6 subsection 1 c) and d), shall threaten the security of the qualified certification services being rendered,
- d) having at his/her disposal no adequate financial resources or other financial provisions for the operation pursuant to section 6 subsection 1 e), thus threatening the security of qualified certification services being rendered,

- e) failing to meet the information duty pursuant to section 6 subsection 1 f), section 6 subsection 3, or section 13 subsection 1,
- f) failing to meet the reporting duty pursuant to section 6 subsection 2, including the submission of a qualified system certificate for verification, or pursuant to section 13 subsection 1 or 2,
- g) providing certification services on the basis of contract other than written,
- h) failing to keep information and documentation pursuant to section 6 subsection 5,
- i) failing to keep all the information and documentation pursuant to section 6 subsection 6 for a period of at least 10 (ten) years, or
- j) failing to ensure that the kept information and documentation shall be secured against loss, misuse, damage or destruction pursuant to section 6 subsection 6.

(2) Qualified provider of certification services who issues qualified certificates or qualified system certificates shall commit an administrative infraction by

- a) failing to ensure that the certificates issued by him/her as qualified shall contain all the essential elements laid down by this Act,
- b) failing to ensure that the data given in the certificates issued as qualified shall be accurate, truthful and complete,
- c) failing to verify the identity of the person pursuant to section 6a subsection 1 c),
- d) failing to ensure data compliance pursuant to section 6a subsection 1 d),
- e) failing to ensure the operation of a safe and publicly accessible list of certificates issued as qualified and failing to ensure its accessibility and updating pursuant to section 6a subsection 1 e),
- f) failing to ensure the operation of a safe and publicly accessible list of certificates issued as qualified which have been invalidated, also by remote access,
- g) failing to ensure that the date and time giving the hour, minute and second when the certificate was issued as qualified or invalidated shall be accurately determined,
- h) by having failed to adopt measures against the misuse and forgery of certificates issued as qualified shall threaten the security of the qualified certification services being rendered,
- i) failing to meet the information duty pursuant to section 6a subsection 1 i),
- j) failing to ensure data compliance and classification pursuant to section 6a subsection 2, if creating such data for the signing or designating person,
- k) copying and keeping data pursuant to section 6a subsection 2, if creating such data for the signing or designating person, or

l) failing to invalidate certificate pursuant to section 6a subsections 3 and 4.

(3) Qualified provider of certification services who issues qualified time stamps shall commit an administrative infraction if he/she

a) fails to ensure that the time stamps issued by him/her as qualified shall contain all the essential elements laid down in section 12b,

b) fails to ensure that the time data inserted into the qualified time stamp shall correspond with the value of the coordinated global time at the time of creating the said qualified time stamp,

c) fails to ensure that data in electronic form, which constitute the subject of the application for the issue of a qualified time stamp, shall correspond with the data in electronic form contained in the qualified time stamp issued,

d) fails to adopt adequate measures against forgery of the qualified time stamp, thus threatening the security of the qualified certification services being rendered,

e) fails to meet the information duty pursuant to section 6b subsection 1 e), or

f) fails to issue a qualified time stamp forthwith following the receipt of the application for its issue.

(4) Qualified provider of certification services who issues the means for safe creation of electronic signatures shall commit an administrative infraction if he/she

a) fails to issue the means for safe creation of electronic signature safely pursuant to section 17 subsection 3, or

b) fails to create in those means or fails to add thereto data for the creation of electronic signatures in a credible manner pursuant to section 17 subsection 3.

(5) A natural person shall commit an administrative infraction by violating the duty of confidentiality pursuant to section 6 subsection 7.

(6) Fine amounting up to the sum of 10 000 000 Kè may be imposed for administrative infractions pursuant to subsections 1 to 4.

(7) Fine amounting up to the sum of 250 000 Kè may be imposed for administrative infractions pursuant to subsection 5.

Section 19 Common Provisions

(1) Legal entity shall not be responsible for administrative infraction if it succeeds in proving that it has exerted maximum efforts that could be required to prevent the said breach of legal liability.

(2) When meting out fine to be imposed on a legal entity, the seriousness of the given administrative infarction shall be taken into account, primarily the manner in which it was committed and its consequences, and the circumstances under which it was committed.

(3) Responsibility of a legal entity for an administrative infarction shall expire, if the relevant administrative authority has not commenced its procedure on it within 1 (one) year from the day on which it learnt of the infarction, but within 3 (three) years of the time it was committed at the latest.

(4) In the first instance, administrative infarctions under this Act shall be dealt with by the Ministry.

(5) Provisions of the Act on the Liability and Prosecution of Legal Entity shall apply to the liability for acts arising during the business activities of a natural person 8), or in direct connection therewith.

(6) Fines shall be collected and enforced by Customs Office having local jurisdiction. Yields of the fines shall constitute the revenue of the state budget.

Section 20

Authorization Provisions

(1) The Ministry shall lay down, in its executive regulation, the method of meeting the information duty pursuant to section 6 subsection 1 a) and f), and subsection 3, the qualification requirements pursuant to section 6 subsection 1 b), the requirements for safe systems and safe instruments pursuant to section 6 subsection 1 c) and d), the method of keeping information and documentation pursuant to section 6 subsection 5 and 6, and the method of documenting compliance with those requirements.

(2) The Ministry shall lay down, in its executive regulation, the method of verifying data compliance pursuant to section 6a subsection 1 d), the method of safeguarding security of lists pursuant to section 6a subsection 1 e) and f), the determination of date and time pursuant to section 6a subsection 1 g), the essential elements of measure pursuant to section 6a subsection 1 h), the method of meeting the information duty pursuant to section 6a subsection 1 i), the method of protecting data and securing data compliance pursuant to section 6a subsection 2, the method of invalidating certificates pursuant to section 6a subsections 3 and 4, and the method of documenting compliance with those requirements

(3) The Ministry shall lay down, in its executive regulation, the method of ensuring accuracy of time when creating qualified time stamp pursuant to section 6b subsection 1 b), the method of securing data compliance pursuant to section 6b subsection 1 c), the essential elements of measure pursuant to section 6b subsection 1 d), the method of meeting the information duty pursuant to section 6b subsection 1 e), and the method of documenting compliance with those requirements.

(4) The Ministry shall lay down, in its executive regulation, the actual structure of data on the basis of which a person may be unequivocally identified, and the procedures of public administration bodies to be applied in receiving and sending data messages through electronic registry pursuant to section 11 subsection 3.

(5) The Ministry shall lay down, in its executive regulation, the method of safeguarding procedures that must support the means for safe creation and verification of electronic signatures when protecting data for the creation of electronic signatures pursuant to section 17, and the means for the creation of electronic signs when protecting data for the creation of electronic signs pursuant to section 17a, and the method of documenting compliance with those requirements.

SECOND PART

Amendment of the Civic Code

Section 21

Act No. 40/1964 Coll., the Civic Code, as amended by Act No. 58/1969 Coll., Act No. 131/1982 Coll., Act No. 94/1988 Coll., Act No. 188/1988 Coll., Act No. 87/1990 Coll., Act No. 105/1990 Coll., Act No. 116/1990 Coll., Act No. 87/1991 Coll., Act No. 509/1991 Coll., Act No. 264/1992 Coll., Act No. 267/1994 Coll., Act No. 104/1995 Coll., Act No. 118/1995 Coll., Act No. 89/1996 Coll., Act No. 94/1996 Coll., Act No. 227/1997 Coll., Act No. 91/1998 Coll., Act No. 165/1998 Coll., Act No. 159/1999 Coll., Act No. 363/1999 Coll., Act No. 27/2000 Coll., and Act No. 103/2000 Coll., shall be amended as follows:

In Section 40 subsection 3 the following sentence shall be added:

"If a legal act is performed by electronic means, it can be signed electronically pursuant to special legal regulations."

THIRD PART

Amendment of Act No. 337/1992 Coll., on the Administration of Taxes, Fees and Charges

Section 22

Act No. 337/1992 Coll., on the Administration of Taxes, Fees and Charges, as amended by Act No. 35/1993 Coll., Act No. 157/1993 Coll., Act No. 302/1993 Coll., Act No. 315/1993 Coll., Act No. 323/1993 Coll., Act No. 85/1994 Coll., Act No. 255/1994 Coll., Act No. 59/1995 Coll., Act No. 118/1995 Coll., Act No. 323/1996 Coll., Act No. 61/1997 Coll., Act No. 242/1997 Coll., Act No. 91/1998 Coll., Act No. 168/1998 Coll., Act No. 29/2000 Coll., Act No. 159/2000 Coll., and Act No. 218/2000 Coll., shall be amended as follows:

In Section 21 subsections 2 and 3 shall read as follows:

"(2) If this or special Act thus stipulates, tax subjects shall report on their tax liability to their competent tax administrator their tax returns, reports and final accounts on prescribed printed forms. Printed forms published in electronic form may be signed electronically pursuant to special regulations.

(3) Other filings on tax matters, such as notifications, applications, proposals, objections, appeals etc., may be submitted in written form or orally into protocol or

electronically signed pursuant to special regulations, or by using other transmission techniques (telex, telefax etc.).".

FOURTH PART

deleted

Section 23

deleted

FIFTH PART

Amendment of the Rules of Civil Procedure

Section 24

Act No. 99/1963 Coll., Rules of Civil Procedure, as amended by Act No. 36/1967 Coll., Act No. 158/1969 Coll., Act No. 49/1973 Coll., Act No. 20/1975 Coll., Act No. 133/1982 Coll., Act No. 180/1990 Coll., Act No. 328/1991 Coll., Act No. 519/1991 Coll., Act No. 263/1992 Coll., Act No. 24/1993 Coll., Act No. 171/1993 Coll., Act No. 117/1994 Coll., Act No. 152/1994 Coll., Act No. 216/1994 Coll., Act No. 84/1995 Coll., Act No. 118/1995 Coll., Act No. 160/1995 Coll., Act No. 238/1995 Coll., Act No. 247/1995 Coll., finding of the Constitutional Court No. 31/1996 Coll., Act No. 142/1996 Coll., finding of the Constitutional Court No. 269/1996 Coll., Act No. 202/1997 Coll., Act No. 227/1997 Coll., Act No. 15/1998 Coll., Act No. 91/1998 Coll., Act No. 165/1998 Coll., Act No. 326/1999 Coll., Act No. 360/1999 Coll., finding of the Constitutional Court No. 2/2000 Coll., Act No. 27/2000 Coll., Act No. 30/2000 Coll., Act No. 46/2000 Coll., Act No. 105/2000 Coll., Act No. 130/2000 Coll., Act No. 155/2000 Coll., and Act No. 220/2000 Coll., shall be amended as follows:

In Section 42 subsection 1 the first sentence shall read: "Filing may be made in written form, orally into protocol, in electronic form signed electronically pursuant to special regulations, by telegraph or by telefax.".

SIXTH PART

Amendment of the Code of Criminal Procedures

Section 25

Act No. 141/1961 Coll., on Criminal Proceedings (Code of Criminal Procedures), as amended by Act No. 57/1965 Coll., Act No. 58/1969 Coll., Act No. 149/1969 Coll., Act No. 48/1973 Coll., Act No. 29/1978 Coll., Act No. 43/1980 Coll., Act No. 159/1989 Coll., Act No. 178/1990 Coll., Act No. 303/1990 Coll., Act No. 558/1991 Coll., Act No. 25/1993 Coll., Act No. 115/1993 Coll., Act No. 292/1993 Coll., Act No. 154/1994 Coll., finding of the Constitutional Court No. 214/1994 Coll., finding of the Constitutional Court No. 8/1995 Coll., Act No. 152/1995 Coll., Act No. 150/1997 Coll., Act No. 209/1997 Coll., Act No.

148/1998 Coll., Act No 166/1998 Coll., Act No. 191/1999 Coll., Act No. 29/2000 Coll., and Act No. 30/2000 Coll., shall be amended as follows:

In Section 59 subsection 1 shall read:

"(1) Filing shall always be considered according to its content even though it is incorrectly designated. It can be made in written form, orally into protocol, in electronic form signed electronically pursuant to special regulations, by telegraph, telefax or telex."

SEVENTH PART

Amendment of the Protection of Personal Data Act

Section 26

Act No. 101/2000 Coll., on the Protection of Personal Data and change in some laws, shall be amended as follows:

In Section 29 subsection 4 , which reads as follows, shall be added:

"(4) The authority shall grant and revoke accreditation to act as accredited provider of certification services and supervise compliance with the duties laid down by the Electronic Signature Act."

EIGHTH PART

Amendment of the Administrative Fees and Charges Act

Section 27

Act No. 368/1992 Coll., on Administrative Fees and Charges, as amended by Act No. 10/1993 Coll., Act No. 72/1994 Coll., Act No. 85/1994 Coll., Act No. 273/1994 Coll., Act No. 36/1995 Coll., Act No. 118/1995 Coll., Act No. 160/1995 Coll., Act No. 301/1995 Coll., Act No. 151/1997 Coll., Act No. 305/1997 Coll., Act No. 149/1998 Coll., Act No. 157/1998 Coll., Act No. 167/1998 Coll., Act No. 63/1999 Coll., Act No. 166/1999 Coll., Act No. 167/1999 Coll., Act No. 223/1999 Coll., Act No. 326/1999 Coll., Act No. 352/1999 Coll., Act No. 357/1999 Coll., Act No. 360/1999 Coll., Act No. 363/1999 Coll., Act No. 46/2000 Coll., Act No. 62/2000 Coll., Act No. 117/2000 Coll., Act No. 133/2000 Coll., Act No. 151/2000 Coll., Act No. 153/2000 Coll., Act No. 154/2000 Coll. Act No 156/2000 Coll., and Act No. 158/2000 Coll., shall be amended as follows:

1. In the Annex to the Act (Rates of Administrative Fees and Charges) new Part XII , which reads as follows, shall be added:

"PART XII

PROCEDURES PURSUANT TO THE ELECTRONIC SIGNATURE ACT

Item 162

a) submission of application for the accreditation of provider of certification services

Kč 100 000,-

b) submission of application for the evaluation of compliance of the instruments of electronic signature with the requirements Kč 10 000,-".

2. LIST TO THE TARIFF OF RATES shall be amended by Part XII , which reads as follows:

"PART XII

Procedure pursuant to Electronic Signature Act 162."

3. Full stop after Part XI shall be deleted.

NINTH PART

EFFECTIVENESS

Section 28

This Act shall come into force on the first day of the third calendar month after its promulgation.

signed by Klaus

signed by Havel

signed by Zeman.

Selected Provisions of the Amendments

Article II of Act No. 440/2004 Coll.

Transitional Provisions

Providers of certification services who had been granted accreditation to act as accredited providers of certification services before the day this Act came into force shall be obliged to adjust the service of issuing qualified certificates to Act No. 227/2000 Coll., on Electronic Signature and on change to some other laws (Electronic Signature Act), as amended by Article. I of this Act by 1st July 2005.

1) The European Parliament and Council Directive 99/93/ES from 13th December 1999 on the Community principles for electronic signatures.

1a) Act No 40/1964 Coll., Civic Code, as amended by later regulations.

2) Act No. 97/1974 Coll., on Archive-keeping, as amended by later regulations.

2a) Section 10 Act No. 40/1964 Coll., Civic Code, as amended by later regulations.

3) Act No. 101/2000 Coll., on the Protection of Personal Data and on change of some laws.

4) Act No. 552/1991 Coll., on State Control, as amended by later regulations.

5) Act No. 368/1992 Coll., on Administrative Fees and Charges, as amended by later regulations.

7) Section 43 Act No. 71/1967 Coll., on Administrative Procedures (Administrative Rules), as amended by later regulations.

8) Section 2 subsection 2 of Act No. 513/1991 Coll., Commercial Code, as amended by later regulations.