Full text of the Electronic Signatures Act

227/2000 Coll.
ACT
of 29 June 2000
on electronic signatures and on the amendment to certain other acts
(Electronic Signatures Act)
as subsequently amended

Parliament has resolved upon the following Act of the Czech Republic:

PART ONE

ELECTRONIC SIGNATURES

Section 1

Purpose

The present act shall govern, in accordance with the law of the European Communities[1)], the use of electronic signatures, electronic marks, the provision of certification services and related services by providers established on the territory of the Czech Republic, supervision of obligations under the present act, and penalties for breach of obligations under the present act.

Section 2

Definition of certain terms

For the purposes of the present act:

a) electronic signature shall mean data in electronic form which are attached to or logically associated with a data message and which serve as a method of unequivocal authentication of a signatory in relation to a data message;

b) advanced electronic signature shall mean an electronic signature which meets the following requirements:

1. it is uniquely linked to the signatory;

[1)] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

2. it is capable of identifying the signatory in relation to a data message;
3. it has been created and attached to a data message using means that the signatory can maintain under his sole control;
4. it is linked to the data message to which it relates in such a manner that any subsequent change of the data is detectable;

c) electronic mark shall mean data in electronic form which are attached to or logically associated with a data message and meet the following requirements:
1. they are unequivocally linked to the marking person and are capable of identifying that person by means of a qualified system certificate;
2. they have been created and attached to a data message using an electronic mark creation device that the marking person can maintain under its sole control;
3. they are linked to the data message to which they relate in such a manner that any subsequent change of the data is detectable;

d) data message shall mean electronic data that can be transmitted by means of electronic communication and stored on storage media used to process and transmit data in electronic form;

e) signatory shall mean a natural person who holds a signature creation device and acts either on his own behalf or on behalf of another natural or legal person;

f) marking person shall mean a natural person, legal person or government body that holds an electronic mark creation device and marks a data message by an electronic mark;

g) certificate holder shall mean a natural person, legal person or government body that has applied for the issue of a qualified certificate or qualified system certificate for itself or for a signatory or a marking person and to which the certificate has been issued;

h) certification service provider shall mean a natural person, legal person or government body that issues certificates and keeps records thereof, and, if applicable, provides other services related to electronic signatures;

i) qualified certification service provider shall mean a certification service provider who issues qualified certificates or qualified system certificates or qualified time stamps or secure signature creation devices (hereinafter referred to as “qualified certification services”) and has complied with the notification duty under Section 6;

j) accredited certification service provider shall mean a certification service provider who has been granted accreditation under the present act;

k) certificate shall mean a data message which is issued by a certification service provider, links signature verification data to the signatory and is capable of authenticating the signatory; or links electronic mark verification data to the marking person and is capable of authenticating the marking person;

l) qualified certificate shall mean a certificate with the elements under Section 12 and has been issued by a qualified certification service provider;

m) qualified system certificate shall mean a certificate with the elements under Section 12a and has been issued by a qualified certification service provider;

n) signature creation data shall mean unique data which are used by the signatory to create an electronic signature;

o) signature verification data shall mean unique data which are used to verify an electronic signature;

p) electronic mark creation data shall mean unique data which are used by the marking person to create electronic marks;

q) electronic mark verification data shall mean unique data which are used to verify electronic marks;

r) qualified time stamp shall mean a data message which has been issued by a qualified certification service provider and links data in electronic form to a moment in time in a trustworthy manner, and guarantees that that data existed in electronic form before the given moment in time;

s) signature creation device shall mean hardware or software used to create electronic signatures;

t) signature verification device shall mean hardware of software used to verify electronic signatures;

u) secure signature creation device shall mean a signature creation device which meets requirements laid down in the present act;

v) secure signature verification device shall mean a signature verification device which meets requirements laid down in the present act;

w) electronic signature product shall mean hardware or software, or components thereof, used to provide certification services or to create or verify electronic signatures;

x) electronic mark creation device shall mean a device which is used by the marking person to create electronic marks and complies with the other relevant requirements laid down in the present act.

y) electronic filing office shall mean an office of a public authority designed for receiving and sending of data messages;

z) accreditation shall mean approval of compliance by a certification service provider with conditions laid down in the present act for the conduct of activities of an accredited certification service provider.

Compliance with signature requirements

(1) A data message shall be signed if it is furnished with an electronic signature. Unless proved otherwise, it shall be assumed that the signatory has familiarised himself with the contents of the data message before signing it.

(2) The use of an electronic signature based on a qualified certificate and created using a secure signature creation device shall enable it to be verified that a data message has been signed by the person identified in the qualified certificate.

Section 3a

(1) The use of an electronic mark based on a qualified system certificate and created using an electronic mark creation device shall enable it to be verified that a data message has been marked with an electronic mark by marking person.

(2) If the marking person marks the data message, it shall be assumed the marking person has made it automatically, without data message direct verification of the content and it is the expression of his will.

Section 4

Integrity of the original

The use of an advanced electronic signature or electronic mark shall guarantee that in the event of interference with the contents of a data message after it was signed or marked such interference will be identifiable.

Section 5

Obligations of the signatory

(1) A signatory shall be obliged to

a) handle advanced signature creation devices as well as data with due care so that no unauthorised use of those could occur;

b) notify without delay the certification service provider who has issued the qualified certificate that there is a risk of abuse of his advanced signature creation data.

(2) A signatory shall be liable, under special legal regulations[1a)], for damage caused by a breach of obligations under paragraph 1. However, he shall be exempted from liability if he proves that the damaged person had not taken all the action necessary to verify that the advanced signature was valid and its qualified certificate had not been revoked.

Section 5a

Obligations of the marking person

(1) A marking person shall be obliged to

a) handle the electronic mark creation device as well as data with due care so that no unauthorised use of those could occur;

b) notify without delay the certification service provider who has issued the qualified system certificate that there is a risk of abuse of its electronic mark creation data.

(2) A marking person shall be obliged to ensure that the electronic mark creation device which it uses complies with requirements laid down in the present act.

(3) Without prejudice to defects liability under special regulations[1a)], a marking person shall be liable, under special legal regulations[1a)], for damage caused by a breach of obligations under paragraph 1, even if it did not cause the damage. However, it shall be exempted from liability if it proves that the damaged person had not taken all the action necessary to verify that the electronic mark was valid and its qualified certificate had not been revoked.

Section 5b

Obligations of the certificate holder

A certificate holder shall be obliged to provide, without unnecessary delay, the certification service provider with accurate, true and complete information in relation to the qualified certificate and in relation to the qualified system certificate.

Section 6

Qualified certification service provider

(1) A qualified certification service provider shall be obliged to

a) ensure that everybody can ascertain his identity and his qualified system certificate on the basis of which he marks issued qualified certificates or qualified system certificates and certificate revocation lists, or qualified time stamps;

[1a)] Act No. 40/1964 Coll., Civil Code, as subsequently amended.

b) ensure that qualified certification services are provided by persons with the expert knowledge and qualifications necessary to provide a qualified certification service, and familiar with the relevant security procedures;

c) use secure systems and secure electronic signature products, ensure sufficient security of procedures supported by such systems and products, and ensure sufficient cryptographic security of such products; systems and products shall be deemed secure if they meet the requirements laid down in the present act and an implementing regulation or if they meet the requirements under technical norms listed in a Commission decision issued under Article 3 (5) of Directive 1999/93/EC;

d) use secure systems to store qualified certificates and qualified system certificates or qualified time stamps in a verifiable form in such a manner that only authorised persons can make entries or change them, information can be checked for authenticity and that any technical or software changes compromising these security requirements are apparent;

e) maintain sufficient financial resources or other financial security throughout the entire period of his activity to operate in conformity with the requirements laid down in the present act and with regard to the risk of liability for damages;

f) before entering into a contract on the provision of qualified certification services with a person applying for the provision of services under the present act, inform that person in writing of the precise terms and conditions regarding the use of the qualified certification services, including any limitations on their use, and of terms and conditions for complaints and dispute settlement and of whether he is accredited by the Ministry of Informatics (hereinafter referred to as "the Ministry") under Section 10 or not; the information may be transmitted electronically.

(2) If the certification service provider is not accredited by the Ministry, he shall notify the Ministry at least 30 days prior to the commencement of provision of a qualified certification service that he is going to provide it, and of the moment the provision of it will commence. At the same time, he shall submit to the Ministry his qualified system certificate referred to in paragraph 1 (a) for verification.

(3) If accreditation was withdrawn by the Ministry from a qualified certification service provider who was granted accreditation under Section 10 of the present act, he shall be obliged to inform without delay about that fact entities to which he provides his qualified certification services and other persons concerned.

(4) A qualified certification service provider shall provide services under the present act on the basis of a contract. The contract must be in writing.

(5) A qualified certification service provider shall store information and documents relating the qualified certification services provided under the present act, in particular

a) contract on the provision of a qualified certification service, including the application for the service provision;

b) the issued qualified certificate, issued qualified system certificate or issued qualified time stamp;

c) copies of submitted identification documents of a signatory or documents on the basis of which the identity of the marking person was verified;

d) acknowledgement of receipt of a qualified certificate or qualified system certificate by the holder and, if applicable, his consent of publication of the qualified certificate on the list of issued qualified certificates;

e) declaration by the certificate holder that he has been provided with information under Section 1 (f);

f) documents and entries related to the life cycle of the issued qualified or qualified system certificate the elements of which shall be specified in an implementing regulation.

(6) A qualified certification service provider shall store all information and documents on the services provided under the present act for a period of at least 10 years. The qualified provider shall be obliged to protect the stored information and documents from loss, abuse, destruction or damage under conditions that shall be specified in an implementing regulation. The information and documents referred to in the first sentence may be recorded and stored in electronic form. Unless the present act provides otherwise, the information and documents shall be handled under a special legal regulation.[2)]

(7) The personnel of a qualified certification service provider and, if applicable, other natural persons coming into contact with personal data and signatories' signature creation data and marking persons' electronic mark creation data shall be obliged not to disclose the data and the security measures the publication of which would jeopardise the security of the data. The duty of non-disclosure shall continue even after the termination of the employment or other contract, or completion of relevant works; the above persons may be released from the duty of non-disclosure only by the person, in whose interest they have the duty, or by court.

Section 6a

Obligations of the qualified certification service provider relating to the issuance of qualified certificates and qualified system certificates

(1) A qualified certification service provider who issues qualified certificates or qualified system certificates (hereinafter referred to as "certificates issued as qualified") shall be obliged to

a) ensure that the certificates issued by him as qualified contain all elements specified under the present act;

b) ensure that the data given in the certificates issued by him as qualified are accurate, true and complete;

[2)] Act No. 97/1974 Coll., on archiving, as subsequently amended.

c) prior to the issuance of a certificate as qualified, verify, by appropriate means, the identity of the signatory or the identity of the marking person and any specific attributes of the person if required by the purpose of such a certificate,

d) ascertain whether, at the time of the lodging of the application for the issuance of a certificate as qualified, the signatory held the signature creation data corresponding to the signature verification data or the marking person held the electronic mark creation data corresponding to the electronic mark verification data contained in the certificate issuance application;

e) ensure the operation of a secure and publicly accessible list of certificates issued as qualified, the publication of which was authorised by certificate holders in accordance with Section 6 paragraph 5) (d), and ensure the accessibility of the list even via remote access, and update the data contained in the list upon every change without unnecessary delay;

f) ensure the operation of a secure and publicly accessible list of certificates issued as qualified that have been revoked (certification revocation list), even via remote access;

g) ensure that the date and time, with an indication of the hour, minute and second of issuance or revocation of the certificate issued as qualified, can be determined precisely;

h) take appropriate measures against abuse and forgery of certificates issued as qualified;

i) provide upon request to third parties essential information on terms and conditions regarding the use of certificates issued as qualified, including limitations on their use and information on whether he is accredited by the Ministry or not; such information may be provided electronically.

(2) If a qualified certification service provider who issues certificates as qualified generates signature creation data for a signatory or electronic mark creation data for a marking person, he must

a) ensure that the data are kept secret before they are handed over, must not copy and store the data longer than necessary;

b) ensure that the data correspond to the signature verification data or electronic mark verification data.

(3) A qualified certification service provider who issues certificates as qualified must without delay revoke a certificate if the holder, signatory or marking person request it or if they notify him that there is a risk of abuse of their signature creation data or electronic mark creation data or in the case of the certificate having been issued on the basis of false or incorrect data.

(4) A qualified certification service provider must also without delay revoke a certificate issued as qualified if he learns, in a demonstrable manner, that the signatory or marking

person has died or was dissolved or incapacitated or its legal capacity was limited by court[2a)] or if data, on the basis of which the certificate was issued, became untrue.

Section 6b

Obligations of the qualified certification service provider relating to the issuance of qualified time stamps

(1) A qualified certification service provider who issues qualified time stamps shall be obliged to

a) ensure that the time stamps issued by him as qualified contain all the elements specified under the present act;

b) ensure that the time data included in a qualified time stamp correspond to the value of the coordinated universal time at the time of creation of the qualified time stamp;

c) ensure that the data in electronic form which are the subject of application for issuance of a qualified time stamp, unequivocally correspond to the data in electronic form contained in the issued qualified time stamp;

d) take appropriate measures against forgery of qualified time stamps;

e) provide upon request to third parties essential information on terms and conditions regarding the use of qualified time stamps, including limitations on their use and information on whether he is accredited by the Ministry or not; such information may be provided electronically.

(2) A qualified certification service provider shall issue a qualified time stamp without delay after receiving an application for its issuance.

Section 7

Liability for damage

(1) A qualified certification service provider shall be liable under special legal regulations[1a)] for damage caused by a breach of obligations laid down in the present act.

(2) A qualified certification service provider shall not be liable for damage resulting from the use of a certificate issued as qualified that was due to violation of limits for its use under Section 12 paragraph 2 (i) and (j) and Section 12a (h).

Section 8

[2a)] Section 10 of Act No. 40/1964 Coll., Civil Code, as subsequently amended.

Personal data protection

Personal data protection shall be governed by a special legal regulation.[3)]

Section 9

Accreditation and supervision

(1) It shall be the in the power of the Ministry to grant accreditation to operate as an accredited certification service provider as well as to supervise the compliance with the present act.

(2) The Ministry shall

a) grant and withdraw accreditation to operate as an accredited certification service provider to entities operating on the territory of the Czech Republic;

b) carry out supervision of activities of accredited certification service providers and qualified certification service providers, imposes corrective measures on them and fines for breaches of obligations under the present act;

c) keep records of accreditation granted and changes thereto and records of qualified certification service providers;

d) keep records of issued qualified system certificates which are used by a qualified certification service provider under Section 6 paragraph 1 (a) and which have been verified by the Ministry under Section 6 paragraph 2;

e) publish on an ongoing basis a review of accreditation granted, review of qualified certification service providers and their qualified services, and qualified system certificates under letter (d), which shall be done also in a manner allowing remote access;

f) determine conformity of electronic signature products with requirements laid down in the present act and an implementing regulation;

g) meet other obligations laid down in the present act.

(3) For the purposes of supervision, an accredited certification service provider and a qualified certificate provider shall be obliged to grant entry to business and operating premises to the extent necessary to authorised Ministry personnel, submit upon request all documentation, entries, written instruments and other materials relating to his activities, give them to the extent necessary access to his information system, and provide information and render all necessary assistance.

[3)] Act No. 101/2000 Coll., on personal data protection and amendment to certain other acts.

(4) Unless provided otherwise in the present act, the Ministry shall proceed under a special legal regulation when carrying out supervision.[4)]

(5) A procedural fine of up to CZK 1 000 000 may be imposed on a qualified certification service provider who has not complied with obligations under paragraph 3.

Section 10

Conditions for granting accreditation to provide certification services

(1) Every certification service provider can apply with the Ministry to be granted accreditation to conduct activities of an accredited certification service provider. The lodging of an application for accreditation shall be subject to an administrative fee.[5)]

(2) In an application for accreditation under paragraph 1, the applicant must provide

a) in the case of a legal person, evidence of the corporate name or name, domicile, or address of a branch of the foreign entity on the territory of the Czech Republic, if applicable, and applicant identification number, if assigned; in the case of a natural person, evidence of the name, or names, if applicable, surname, or specification, if applicable, place of establishment, place of business, if different from the place of establishment, and applicant identification number, if assigned;

b) a document of authorisation for business activity and, if registered in the Commercial Register, also a copy of the entry in the Commercial Register not older than 3 months;

c) a criminal record statement of the entrepreneur–natural person, or of authorised representatives of the legal person if the applicant is a legal person, not older than 3 months;

d) evidence of factual, personnel and organisational qualifications for the activity of a qualified certification service provider under Sections 6, 6a and 6b of the present act;

e) information on which qualified certification services the applicant intends to provide;

f) a proof of payment of the administrative fee.

(3) If the application does not contain all the data required, the Ministry shall suspend the proceedings and call on the applicant to complete the application by a specified deadline. If the applicant fails to do so by the deadline, the Ministry shall discontinue the proceedings. The administrative fee shall not be returned.

(4) If the applicant meets all the conditions to be granted accreditation prescribed in the present act, the Ministry shall issue a decision granting him the accreditation. Otherwise, the Ministry shall reject the application for accreditation.

[4)] Act No. 552/1991 Coll., on state audit, as subsequently amended.
[5)] Act No. 368/1992 Coll., on administrative fees, as subsequently amended.

Section 10a

Conditions for extension of services of an accredited certification service provider

(1) An accredited certification service provider may extend the provision of qualified certification services to include also issuance of qualified certificates, qualified system certificates, qualified time stamps or issuance of secure signature creation devices under the present act (hereinafter referred to as "extended services").

(2) An accredited certification service provider shall be obliged to notify the Ministry of an extension under paragraph 1 in such a manner that the Ministry receives the notification at least 4 months before the commencement of provision of the service.

(3) In the notification to the Ministry, the accredited certification service provider must provide evidence of factual, personnel and organisational qualifications to provide the extended services.

(4) If the accredited certification service provider fails to provide evidence under paragraph 3 or the evidence is incomplete or inaccurate, the Ministry shall advise the accredited certification service provider thereof noting that unless the failures are corrected by a deadline that it shall set for the purpose, it will ban the extension of services in a decision.

(5) The Ministry shall ban the announced extension if the accredited certification service provider fails to comply with all the conditions prescribed by the present act for the provision of extended services.

(6) The Ministry shall issue a decision banning the extension of provision of qualified certification services at the latest within 90 days of receipt of the notification.

Section 11

(1) For the purpose of signing in the sphere of public authorities, it shall be possible to use only advanced electronic signatures and qualified certificates issued by accredited certification service providers (hereinafter referred to as "recognised electronic signatures"). That shall apply also to the exercise of public authority on natural and legal persons. If a recognised electronic signature is used in the sphere of public authorities, the qualified certificate must contain such data as to make the person unequivocally identifiable. The structure of data on the basis of which it is possible to unequivocally identify a person shall be laid down by the Ministry in an implementing legal regulation.

(2) Documents of public authorities in electronic form marked by an electronic mark based on a qualified system certificate issued by an accredited provider of certification services or signed using a recognised electronic signature shall have the same legal effect as public deeds issued by those authorities.

(3) A public authority shall receive and send data messages under paragraph 1 using an electronic filing office.

Section 12

Elements of the qualified certificate

(1) A qualified certificate must contain

a) an indication that it is issued as a qualified certificate under the present act;

b) in the case of a legal person, the corporate name or name and state in which the qualified provider is established; in the case of a natural person, the name, or names, if applicable, surname, or specification, if applicable, and state in which the qualified provider is established;

c) the name, or names, if applicable, and surname of the signatory or a pseudonym with the relevant indication that it is a pseudonym;

d) a specific attribute of the signatory if required by the purpose of the qualified certificate;

e) signature verification data which correspond to signature creation data which are under the control of the signatory;

f) electronic mark of the certification service provider based on a qualified system certificate of the provider issuing the qualified certificate;

g) the number of the qualified certificate unique with the given certification service provider;

h) the beginning and end of the period of validity of the qualified certificate;

i) data on whether the use of the qualified certificate shall be limited with regard to nature and scope only to certain uses, if applicable;

j) limits on the value of transactions for which the qualified certificate can be used, if applicable.

(2) Limitations on the use of a qualified certificate under paragraph 1 (i) and (j) must be apparent to third parties.

(3) The qualified certificate may contain further personal data only with permission of the signatory.

Section 12a

Elements of the qualified system certificate

A qualified system certificate must contain

a) an indication that it is issued as a qualified system certificate under the present act;

b) in the case of a legal person, the corporate name or name and state in which the qualified provider is established; in the case of a natural person, the name, or names, if applicable, surname, or specification, if applicable, and state in which the qualified provider is established;

c) unequivocal identification of the marking person, or of the electronic mark creation device, if applicable;

d) electronic mark verification data corresponding to electronic mark creation data which are under the control of the signatory;

e) electronic mark of the certification service provider based on a qualified system certificate of the provider issuing the qualified system certificate;

f) the number of the qualified system certificate unique with the given certification service provider;

g) the beginning and end of the period of validity of the qualified system certificate;

h) limitations on the use of the qualified system certificate, and such limitations must be recognisable to third parties.

Section 12b

Elements of the qualified time stamp

A qualified time stamp must contain

a) the number of the qualified time stamp unique with the given qualified certification service provider;

b) an indication of rules under which the qualified certification service provider issued the qualified time stamp;

c) in the case of a legal person, the corporate name or name and state in which the qualified provider is established; in the case of a natural person, the name, or names, if applicable, surname, or specification, if applicable, and state in which the qualified provider is established;

d) time value corresponding to the coordinated universal time at the time of creation of the qualified time stamp;

e) data in electronic form for which the qualified time stamp has been issued;

f) electronic mark of the qualified certification service provider who issued the qualified time stamp.

Section 13

Obligations of the qualified certification service provider upon termination of activities

(1) A qualified certification service provider must notify the Ministry of an intention to terminate his activities at least 3 months before the planned date of termination of activities and must make every effort to have the records kept under Section 6 paragraph 5 taken over by another qualified certification service provider. Further, the qualified certification service provider must demonstrably inform each signatory, marking person and holder to whom he provides his certification services about his intention to terminate activities at least 2 months before the planned date of termination of activities.

(2) If a qualified certification service provider is not able to ensure that the records kept under Section 6 paragraph 5 are taken over by another certification service provider, he shall be obliged to notify the Ministry thereof at least 30 days before the planned date of termination of activities. In that case the Ministry shall take the records over and notify the entities concerned thereof.

(3) The provisions of paragraphs 1 and 2 shall also be reasonably applied if a qualified certification service provider is dissolved, dies or terminates his activities without complying with the notification obligation under paragraph 1.

Section 14

Corrective measures

(1) If the Ministry ascertains that an accredited certification service provider or qualified certification service provider is in breach of obligations laid down in the present act, it shall charge him to provide for a correction by a specified deadline, or if applicable, determine what measures to remove the inadequacies the certification service provider is obliged to take.

(2) If an accredited certification service provider commits a more serious breach of obligations laid down in the present act or does not remove by the specified deadline the inadequacies ascertained by the Ministry, the Ministry shall be entitled to withdraw the accreditation granted to him.

(3) If the Ministry decides to withdraw the accreditation, it may at the same time decide about revocation of certificates issued as qualified by the certification service provider in the period of validity of the accreditation.

Section 15

Order of revocation of a qualified certificate or qualified system certificate

As a preliminary measure[7)], the Ministry may order a qualified certification service provider to revoke a certificate issued as qualified if there is a justified suspicion that the certificate has been forged or if it was issued on the basis of false data. The decision on the revocation of a certificate issued as qualified may be issued also if it has been ascertained that a signatory or marking person uses a signature creation device or electronic mark creation device which shows security deficiencies that would enable forgery of advanced electronic signatures or electronic marks or changes to signed or marked data.

Section 16

Recognition of foreign qualified certificates

(1) A certificate that is issued as qualified by a certification service provider established in a Member State of the European Union shall be a qualified certificate under the present act.

(2) A certificate issued in a state other than a Member State of the European Union as qualified as defined under the present act, shall be a qualified certificate under the present act if

a) the certification service provider complies with conditions of European Community law[1)] and has been accredited to operate as an accredited certification service provider in a Member State of the European Union, or

b) a certification service provider established in a Member State of the European Union complying with conditions of European Community law[1)] takes over responsibility for the validity and correctness of the certificate in the same extent as with his qualified certificates, or

c) it arises out of an international treaty.

Section 17

Secure signature creation and verification devices

(1) A secure signature creation device must, by appropriate technical and software means and procedures, ensure at least that

a) the signature creation data may occur only once and that their secrecy is properly assured

---

[7)] Section 43 of the Act No. 71/1967 Coll., on administrative procedure (Rules of Administrative Procedure), as subsequently amended.

b) the signature creation data cannot, with proper assurance, be derived using knowledge of their generation and the signature is protected against forgery using currently available technology;

c) the signature creation data can be reliably protected by the signatory against abuse by a third party.

(2) Secure 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.

(3) Secure signature creation devices must be securely issued before use and signature creation data must be generated in such devices in a trustworthy manner or added into them.

(4) A secure signature verification device must, by appropriate technical and software means and procedures, ensure at least that

a) the data used for verifying the signature correspond to the data displayed to the verifier;

b) the signature is reliably verified and the result of that verification is correctly displayed;

c) the verifier can reliably establish the contents of the signed data;

d) the authenticity and validity of the certificate at the time of signature verification are reliably ascertained;

e) the result of verification and the signatory's identity are properly displayed;

f) the use of a pseudonym is clearly indicated;

g) any security-relevant changes can be detected.

Section 17a

Electronic mark creation devices

(1) An electronic mark creation device must, by appropriate technical and software means and procedures, ensure at least that

a) the electronic mark creation data are kept sufficiently secret and reliably protected by the marking person against abuse by a third party;

b) the marking person is informed that it commences use of the device.

(2) An electronic mark creation device must be configured in such a manner that, without further control by the marking person, it marks just and only those data messages that the marking person selects for marking.

(3) An electronic mark creation device must be protected from unauthorised change and must guarantee that any change to it will be apparent to the marking person.

Section 18

Administrative delicts of legal persons

(1) A fine of up to CZK 10 000 000 shall be imposed on a qualified certification service provider who

a) fails to ensure that everybody can ascertain his identity and his qualified system certificate under Section 6 paragraph 1 (a);

b) fails to ensure that qualified certification services are provided by persons with the expert knowledge and qualifications necessary to provide qualified certification services, and familiar with the relevant security procedures;

c) by failing to ensure sufficient security of the systems used and electronic signature products, and procedures supported by such systems and products under Section 6 paragraph 1 (c) and (d), jeopardises the security of the qualified certification services provided;

d) fails to have sufficient financial resources or other financial security available for the operation under Section 6 paragraph 1 (e), thereby jeopardising the security of the qualified certification services provided;

e) fails to comply with the duty to inform under Section 6 paragraph 1 (f), Section 6 paragraph 3 or Section 13 paragraph 1;

f) fails to comply with the notification duty under Section 6 paragraph 2, including the submission of the qualified system certificate for verification, or under Section 13 paragraphs 1 or 2;

g) provides certification services based on a different than written contract;

h) fails to keep the information and documents under Section 6 paragraph 5;

i) fails to keep all information and documentation under Section 6 paragraph 6 for a period of at least 10 years, or

j) fails to protect the stored information and documents from loss, abuse, destruction or damage under Section 6 paragraph 6.

(2) A fine of up to CZK 10 000 000 shall be imposed on a qualified certification service provider who issues qualified certificates or qualified system certificates and

a) fails to ensure that the certificates issued by him as qualified contain all elements specified under the present act;

b) fails to ensure that data given in the certificates issued as qualified are accurate, true and complete;

c) fails to verify the identity of a person under Section 6a paragraph 1 (c);

d) fails to ensure data correspondence under Section 6a paragraph 1 (d);

e) fails to ensure the operation of a secure and publicly accessible list of certificates issued as qualified and fails to ensure its accessibility and updating under Section 6a paragraph 1 (e);

f) fails to ensure the operation of a secure and publicly accessible list of certificates issued as qualified that have been revoked, even via remote access;

g) fails to ensure that the date and time, with an indication of the hour, minute and second of issuance or revocation of the certificate issued as qualified, can be determined precisely;

h) by failing to take appropriate measures against abuse and forgery of certificates issued as qualified jeopardises the security of the qualified certification services provided;

i) fails to comply with the duty to inform under Section 6a paragraph 1 (i);

j) fails to ensure data correspondence and secrecy under Section 6a paragraph 2, if he generates the data for the signatory or marking person;

k) copies and stores data under Section 6a paragraph 2, if he generates the data for the signatory or marking person, or

l) fails to revoke a certificate under Section 6a paragraphs 3 and 4.

(3) A fine of up to CZK 10 000 000 shall be imposed on a qualified certification service provider who issues qualified time stamps and

a) fails to ensure that the time stamps issued by him as qualified contain all elements specified under Section 12b;

b) fails to ensure that the time data inserted in a qualified time stamp correspond to the value of the coordinated universal time at the time of creation of the qualified time stamp;

c) fails to ensure that the data in electronic form which are the subject of application for issuance of a qualified time stamp correspond to the data in electronic form contained in the issued qualified time stamp;

d) fails to take appropriate measures against forgery of qualified time stamps, jeopardising the security of qualified certification services;

e) fails to comply with the duty to inform under Section 6b paragraph 1 (e), or

f) fails to issue a qualified time stamp without delay after receiving an application for its issuance.

(4) A fine of up to CZK 10 000 000 shall be imposed on a qualified certification service provider who issues secure signature creation devices and

a) fails to issue secure signature creation devices in a secure manner under Section 17 paragraph 3, or

b) fails to generate in such devices or add into them signature creation data in a trustworthy manner under Section 17 paragraph 3.

(5) A fine of up to CZK 10 000 000 shall be imposed on an accredited certification service provider who fails to comply with the notification duty under Section 10a paragraph 2.

(6) A fine of up to CZK 10 000 000 shall be imposed on an accredited certification service provider who breaches the ban issued by the Ministry under Section 10a paragraph 5.

Section 18a

Administrative infractions

(1) A qualified certification service provider shall commit an administrative infraction by

a) failing to ensure that everybody can ascertain his identity and his qualified system certificate under Section 6 paragraph 1 (a);

b) failing to ensure that qualified certification services are provided by persons with the expert knowledge and qualifications necessary to provide qualified certification services, and familiar with the relevant security procedures;

c) jeopardising the security of the qualified certification services provided by failing to ensure sufficient security of the systems used and electronic signature products, and procedures supported by such systems and products under Section 6 paragraph 1 (c) and (d);

d) failing to have sufficient financial resources or other financial security available for the operation under Section 6 paragraph 1 (e), thereby jeopardising the security of the qualified certification services provided;

e) fails to comply with the duty to inform under Section 6 paragraph 1 (f), Section 6 paragraph 3 or Section 13 paragraph 1;

f) fails to comply with the notification duty under Section 6 paragraph 2, including the submission of the qualified system certificate for verification, or under Section 13 paragraphs 1 or 2;

g) provides certification services based on a different than written contract;

h) fails to keep the information and documents under Section 6 paragraph 5;

i) fails to keep all information and documentation under Section 6 paragraph 6 for a period of at least 10 years, or

j) fails to protect the stored information and documents from loss, abuse, destruction or damage under Section 6 paragraph 6.

(2) A qualified certification service provider who issues qualified certificates or qualified system certificates shall commit an administrative infraction by

a) failing to ensure that the certificates issued by him as qualified contain all elements specified under the present act;

b) failing to ensure that data given in the certificates issued as qualified are accurate, true and complete;

c) failing to verify the identity of a person under Section 6a paragraph 1 (c);

d) failing to ensure data correspondence under Section 6a paragraph 1 (d);

e) failing to ensure the operation of a secure and publicly accessible list of certificates issued as qualified and failing to ensure its accessibility and updating under Section 6a paragraph 1 (e);

f) failing to ensure the operation of a secure and publicly accessible list of certificates issued as qualified that have been revoked, even via remote access;

g) failing to ensure that the date and time, with an indication of the hour, minute and second of issuance or revocation of the certificate issued as qualified, can be determined precisely;

h) jeopardising the security of the qualified certification services provided by failing to take appropriate measures against abuse and forgery of certificates issued as qualified;

i) failing to comply with the duty to inform under Section 6a paragraph 1 (i);

j) failing to ensure data correspondence and secrecy under Section 6a paragraph 2, if he generates the data for the signatory or marking person;

k) copying and storing data under Section 6a paragraph 2, if he generates the data for the signatory or marking person, or

l) failing to revoke a certificate under Section 6a paragraphs 3 and 4.

(3) A qualified certification service provider who issues qualified time stamps shall commit and administrative infraction by

a) failing to ensure that the time stamps issued by him as qualified contain all elements specified under Section 12b;

b) failing to ensure that the time data inserted in a qualified time stamp correspond to the value of the coordinated universal time at the time of creation of the qualified time stamp;

c) failing to ensure that the data in electronic form which are the subject of application for issuance of a qualified time stamp, correspond to the data in electronic form contained in the issued qualified time stamp;

d) failing to take appropriate measures against forgery of qualified time stamps, jeopardising the security of qualified certification services;

e) failing to comply with the duty to inform under Section 6b paragraph 1 (e), or

f) failing to issue a qualified time stamp without delay after receiving an application for its issuance.

(4) A qualified certification service provider who issues secure signature creation devices shall commit an administrative infraction by

a) failing to issue secure signature creation devices in a secure manner under Section 17 paragraph 3, or

b) failing to generate in such devices or add into them signature creation data in a trustworthy manner under Section 17 paragraph 3.

(5) A natural person shall commit an administrative infraction by breaching the non-disclosure duty under Section 6 paragraph 7.

(6) A fine of up to CZK 10 000 000 can be imposed for administrative infractions under paragraphs 1 to 4.

(7) A fine of up to CZK 250 000 can be imposed for an administrative infraction under paragraph 5.

Section 19

General provisions

(1) A legal person shall not be responsible for an administrative delict if it proves that it made every effort that could be required to prevent the breach of a legal obligation.

(2) The seriousness of the administrative delict, in particular the manner of how it was committed and its consequences or the circumstances under which it was committed, shall be considered when determining the rate of the fine.

(3) The liability of a legal person for an administrative delict shall terminate unless an administrative authority commences proceedings concerning the delict within 1 year of learning of it, at the latest, however, within 3 years of the day it was committed.

(4) Administrative delicts under the present act shall be heard by the Ministry in the first instance.

(5) Provisions of the present act as to the liability of and penalties to a legal person shall apply to liability for action taken in the conduct of business by a natural person[8)] or in direct relation thereto.

(6) Fines shall be collected and enforced by the financial authority with the local jurisdiction. Proceeds of fines shall be an income of the state budget.

Section 20

Delegating provisions

(1) The Ministry shall lay down, in an implementing legal regulation, the manner of complying with the duty to inform under Section 6 paragraph 1 (a) and (f) and paragraph 3, qualifications requirements under Section 6 paragraph 1 (b), requirements on secure systems and secure products under Section 6 paragraph 1 (c) and (d), the manner of storing information and documents under Section 6 paragraphs 5 and 6, and the manner of proving compliance with such requirements.

(2) The Ministry shall lay down, in an implementing legal regulation, the manner of verifying data correspondence under Section 6a paragraph 1 (d), the manner of ensuring the security of lists under Section 6a paragraph 1 (e) and (f), determining the date and time under Section 6a paragraph 1 (g), elements of measures under Section 6a paragraph 1 (h), the manner of complying with duty to inform under Section 6a paragraph 1 (i), the manner of protecting and ensuring the correspondence of data under Section 6a paragraph 2, the manner of revocation of certificates under Section 6a paragraphs 3 and 4 and the manner of proving compliance with such requirements.

(3) The Ministry shall lay down, in an implementing legal regulation, the manner of ensuring exactness of time at the time of creation of a qualified time stamp under Section 6b paragraph 1 (b), the manner of ensuring data correspondence under Section 6b paragraph 1 (c), elements of measures under Section 6b paragraph 1 (d), manner of complying with the duty to inform under Section 6b paragraph 1 (e) and the manner of proving compliance with such requirements.

(4) The Ministry shall lay down, in an implementing legal regulation, the structure of data on the basis of which it is possible to unequivocally identify a person, and the procedures of public authorities applied when receiving and sending data messages using an electronic filing office under Section 11 paragraph 3.

(5) The Ministry shall lay down, in an implementing legal regulation, the manner of ensuring procedures that must be supported by secure signature creation and verification

---

[8)] Section 2 paragraph 2 of the Act No. 513/1991 Coll., Commercial Code, as subsequently amended.

devices when protecting signature creation data under Section 17 and by electronic mark creation devices when protecting electronic mark creation data under Section 17a, and the manner of proving compliance with such requirements.

Section 28

Validity

The present act shall come into effect on the first day the next month of its publication (1st of October 2000).