

215

ACT

of 15 March 2002

on electronic signature and on amendment of some acts as amended by Act No. 679/2004 Coll., Act No. 25/2006 Coll. and Act No. 275/2006 Coll.

The National Council of the Slovak Republic adopted the following Act:

PART I

Article 1

Subject of the Act

(1) This Act arranges relationships arising in relation to the execution and the use of the electronic signature, the rights and the obligations of natural persons and of legal persons in using the electronic signature, the credibility and the protection of electronic documents signed by the electronic signature.

(2) The Act can be used in the closed systems if participants of the closed system, unless laid down otherwise herein.

(3) The Act is cancelled from 1 June 2006.

Article 2

Definitions

For the purposes of this Act the following definitions shall apply:

(a) "Document" is any non-zero sequence of characters;

(b) "Digital document" is a numerically enciphered document;

(c) "Electronic document" is either a digital document maintained at a physical carrier transmitted or processed by a technical tool in an electronic, a magnetic, an optic or other form;

(d) "Signed electronic document" is an electronic document for which an electronic signature has been executed, if this electronic document is available together with the electronic signature of the respective document;

(e) "Private key" is secret information serving for the execution of the electronic signature of the electronic document;

(f) "Public key" is an information available to the authenticator; this information serves for the authentication of the correctness of the electronic signature executed by a private key belonging to a given public key;

(g) "Tool for execution of electronic signature" is technical equipment or software, or algorithms or a combination thereof, by means of which the signatory can put an electronic signature to an electronic document on the basis of an electronic document and a private key;

(h) "Security equipment for execution of the electronic signature" is a tool for execution of the electronic signature complying with the requirements hereof and serving for executing guaranteed electronic signatures;

(i) "Tool for electronic signature authentication" is technical equipment, or software, or algorithms, or a combination thereof, by means of which the authenticator, on the basis of the signed electronic document and the public key belonging to a private key that was used for the execution of this electronic signature, to verify correctness of the electronic signature;

(j) "Closed system" is a system serving exclusively for the own needs of the users of such a system, such a system is established on the basis of an agreement of the users concerning this system, closed system is not the information system of public administration¹;

(k) "Certification service" comprises in particular the issuance of certificates, the annulment of certificates, providing lists of annulled certificates, acknowledging the existence and validity of certificates, searching for and providing valid certificates;

¹ § 2 letter b) of the Act no. 275/2006 Coll. on Information Systems of the public administration and on the amendment and supplementing of certain Acts.

(l) "Accredited certification service" is in particular the issuance of qualified certificates, the annulment of qualified certificates, providing lists of annulled qualified certificates, acknowledging the existence and validity of qualified certificates, searching for and providing issued qualified certificates, and the issuing and authentication of time stamps;

(m) "Certification activity" is the provision of certification services, accepting applications for issuance of a certificate, maintenance of records, operations of required technical equipment and other activities necessary to provide certification services;

(n) "Administration of certificates" is certificate issuing, verification of certificate validity, certificate annulment, certificate archiving, and certification activities related thereto;

(o) "Product for the electronic signature" is technical equipment and software or their relevant parts intended for the certification service providers to carry out certification activities or authentication of electronic signatures;

(p) "Certification services provider" is a natural person or a legal entity carrying out certification services;

(q) "Certification authority" is a certification services provider who administers the certificates pursuant to subparagraph (n) above;

(r) "Accredited certification authority" is a certification authority providing certification services pursuant hereto, and that has the accreditation of the National Security authority² (hereafter referred to as "the authority");

(s) "The registration authority" is a certification services provider, who on behalf of the certification authority, performs selected certification activities and mediates the services of the certification authority to certificate holders and applicants for issuance of a certificate;

(t) "Signatory" is a natural person who is the holder of a private key and who by this key is able to put an electronic signature to an electronic document;

(u) "Certificate issuer" is a certification authority or the authority;

² Article 1, paragraph 2 of the Act No. 241/2001 Coll.,

Article 34 of the Act No. 575/2001 Coll. on the organization of activities of the government and the organization of central state administration.

(v) "Certificate holder" is:

1. a natural person to whom a certificate is issued by a certification authority on the basis of this act,
2. a certification authority,
3. the authority;

(w) "Authenticator of the electronic signature" is a natural person or a legal entity, who through a tool for electronic signature verification, a public key, a signed electronic document and an electronic signature of this document can authenticate the validity of a given electronic signature;

(x) "Security equipment for time stamp executing" is technical equipment and software complying with the requirements hereof and that can produce a time stamp of the given electronic document on the basis of time data, the respective electronic document and a private key produced for this purpose.

(y) "Electronic Registry" is technical device determined especially for accepting, sending and confirmation of electronic documents, electronic documents signed by the electronic signature and electronic documents signed by the qualified electronic signature.

Article 3

Electronic signature

(1) The electronic signature is information attached or otherwise linked to an electronic document. The electronic signature shall comply with the following requirements:

- (a) It may not effectively be issued without knowledge of the private key and the electronic document;
- (b) On the basis of the knowledge of this information and the public key belonging to this private key used in execution of this information it may be verified that the electronic document to which it is attached or logically linked otherwise, is equal to such an electronic document used for its execution.

(2) The signatory executes the electronic signature of an electronic document so that on the basis of his/her private key and the electronic document he/she issues new data complying with the requirements pursuant to paragraph (1) above.

Article 4

Guaranteed electronic signature

(1) The guaranteed electronic signature is an electronic signature that must comply with the requirements of Article 3 hereof:

- (a) it is executed by means of a private key intended for the execution of the guaranteed electronic signature;
- (b) it may be executed only with the security equipment for execution of the electronic signatures pursuant to Article 2, subparagraph (h);
- (c) the manner of its execution enables the identification in a reliable manner of which natural person executed the guaranteed electronic signature;
- (d) a qualified certificate to the public key belonging to the private key is issued, and this private key is used for the execution of the guaranteed electronic signature.

(2) The guaranteed electronic signature is valid, if :

- (a) there is a qualified certificate to the public key belonging to the private key used in the course of executing an electronic signature;
- (b) it is provable that the qualified certificate pursuant to subparagraph (a) was valid at the time of the execution of the given electronic signature;
- (c) the electronic document to which the guaranteed electronic signature is attached or otherwise linked is equal to the document used for its execution and that is authenticated through the use of the public key given in the qualification certificate pursuant to subparagraph (a) above;

(3) The signatory shall execute the guaranteed electronic signature of an electronic document so that he/she produces new data complying with paragraph (1) on the basis of his/her private key and the given electronic document, using the security equipment for executing the electronic signature.

(4) Generally binding regulation issued by the authority shall set out the form and manner of execution of the guaranteed electronic signature.

(5) The public key belonging to the private key intended for the execution of the authority's guaranteed electronic signature shall be disclosed in the manner as set out in the generally binding regulation issued by the authority.

(6) The authority's guaranteed electronic signature shall be valid if the electronic document to which this guaranteed electronic signature is attached or logically linked otherwise is equal to the document used for its execution, where this has been authenticated through the use of the authority's public key disclosed pursuant to paragraph (5).

Article 5

Use of the electronic signature

(1) The electronic signature or the Qualified Electronic Signature is used in contact with bodies of the public administration. If Qualified Electronic Signature is used in contact with the public administration then its qualified certificate must be issued by the accredited certification authority.

(2) The authenticator authenticates any electronic signature through a tool for authentication of electronic signatures using the signed electronic document and the public key belonging to the given signatory.

(3) While authenticating the electronic signature the authenticator may request authentication of authenticity of the public key, that means authentication, whether the given public key belongs to the signatory. For this purpose the signatory's public key certificate may be used.

(4) While authenticating the guaranteed electronic signature the authenticator shall on the basis of the private key qualified certificate authenticate whether the public key for authentication of the guaranteed electronic signature belongs to the signatory.

(5) The generally binding regulation issued by the authority shall set out details concerning conditions of validity for guaranteed electronic signatures, and the procedure for authentication of guaranteed electronic signatures.

Article 6

Public key certificate

(1) The public key certificate (hereafter referred to as "the certificate") is an electronic document through which the issuer of this certificate acknowledges that the public key given in this certificate belongs to the person/entity to which this certificate is issued (hereafter referred to as "the certificate holder").

(2) The certificate comprises the body of the certificate and the electronic signature of the certificate.

(3) The body of the certificate is an electronic document in particular comprising the following:

- (a) identification data of the issuer of this certificate;
- (b) the identification number of the certificate;
- (c) identification data concerning the certificate holder;
- (d) the date and a time of the commencement and end of validity of the certificate;
- (e) the public key of the certificate holder;
- (f) an identification of algorithms for which the given public key is determined;
- (g) an identification of algorithms used in execution of the electronic signature of the body of the certificate.

(4) The certificate issuer executes the electronic signature of the body of the certificate using a public key determined for it.

(5) An alias may be used as identification data of the certificate holder pursuant to paragraph 3(c), however solely on the basis of data that the certification authority obtains from the applicant in submitting an application for issuance of a certificate, and on the basis of which there may be

unequivocally determined the identity of the given certificate holder. The certification authority shall state expressly in the certificate that it quotes an alias of the certificate holder as the identification data.

(6) A cross certificate is a certificate issued by the certification authority for a public key of another certification authority. The certification authority, through issuance of a cross certificate, enables the authentication of the electronic signatures on the basis of the certificates which another authorization authority has issued and signed by a private key belonging to the public key that is given in that cross certificate.

Article 7

Qualified certificate

(1) The qualified certificate is a certificate of a natural person, an accredited certification authority certificate, a cross accredited certification authority certificate, and a authority certificate, complying with the conditions pursuant to paragraphs 2 to 5 and Article 6.

(2) The qualified certificate is a certificate of a natural person is such a certificate that

(a) has been issued by an accredited certification authority to a natural person,

(b) has quoted therein that this certificate is the qualified certificate,

(c) has quoted therein a constraints concerning to use of that certificate, if a third party distinguishes such constraints,

(d) has the body of the certificate signed by the guaranteed electronic signature of an accredited certification authority, and this guaranteed electronic signature has been executed through a private key intended for this purpose.

(3) The accredited certification qualified certificate is such a certificate that

(a) has been issued by the authority to an accredited certification authority,

(b) has quoted therein that it is the qualified certificate,

(c) has quoted therein a purpose for which it has been intended for,

(d) has a body of the certificate signed by the guaranteed electronic signature of the authority.

(4) The accredited certification authority qualified cross certificate is such a cross certificate that:

- (a) has been issued by the authority to an accredited certification authority,
- (b) has quoted therein that it is the cross qualified certificate,
- (c) has the body of the certificate signed by the guaranteed electronic signature of the an accredited certification authority.

(5) The authority's qualified certificate is a certificate that complies with the requirements pursuant to paragraphs 3(b) to 3(d), and the authority has issued it for the own public key of the authority.

(6) The generally binding legal regulation issued by the authority shall set out the form and the contents of the qualified certificate as well as the particularities concerning the administration of qualified certificates.

(7) The qualified certificate shall be valid at the time period for which it is authenticated the validity of that qualified certificate, if

- (a) this time period is between the beginning and the end of validity of that certificate,
- (b) the guaranteed electronic signature of the body of the certificate is valid,
- (c) this certificate has not been annulled over this time period.

Article 8

Annulled certificates list

(1) The annulled certificates list is an electronic document through that the certificate issuer administrates certificates, notifying a premature annulment/revocation of their validity.

(2) The annulled certificates list comprises of a body of the annulled certificates list and of an electronic signature of the body of the annulled certificates list.

(3) The body of the annulled certificates list is an electronic document comprising in particular the following:

- (a) identification data of the certificate issuer administrating certificates;

(b) the date and a time of the issuance of the annulled certificates list;

(c) the date and a time of the latest issuance of the annulled certificates list;

(d) a list of the certificate identification numbers had been annulled together with the date and a time of their annulment/revocation.

(4) The electronic signature of the body of the annulled certificates list is produced by a certificate issuer administrating such certificates, using a private key intended for it.

(5) The annulled qualified certificates list is a list of annulled certificates through that the qualified certificate issuer, administrating such certificates, notifies a premature annulment/revocation of their validity. The annulled qualified certificates list shall comply with the requirements pursuant to paragraphs 1 to 4, and concurrently:

(a) has been issued by an accredited certification authority, or by the authority;

(b) the electronic signature of the body of the annulled certificates list is produced using a private key intended for this purpose;

(c) the accredited certification authority or the authority issued a certificate to the public key belonging to the private key pursuant to subparagraph (b).

(6) The generally binding regulation issued by the authority shall stipulate the format, the periodicity of issuing, and the manner of issuance of annulled qualified certificates lists.

Article 9

Time stamp

(1) "Time stamp" is an information attached to an electronic document or logically linked to it otherwise and must comply with the following requirements:

(a) it may not be produced effectively without knowledge of a private key intended for this purpose and without an electronic document;

(b) on the basis of the knowledge of the public key belonging to a private key used in producing it, it is possible to authenticate that the electronic document to which it is attached or logically linked otherwise is equal to the electronic document used for its execution;

- (c) an accredited authority has produced it using a private key intended for this purpose;
- (d) it may be executed solely by using a security equipment for time stamp executing pursuant to Article 2, paragraph (x); the generally binding legal regulations issued by the authority shall stipulate details concerning the requirements for such a security equipment;
- (e) an accredited certification authority has issued a qualified certificate to the public key belonging to a private key used for executing it;
- (f) it enables unequivocally to identify the date and the time when it has been executed.

(2) The generally binding legal regulation issued by the authority shall set out the format and the manner of executing time stamps, as well as the requirements for the maintenance of time stamp documentation.

Article 10

Authority

- (1) The Authority is the central body of the state administration for the electronic signature.
- (2) The authority shall meet the following roles:
 - (a) Conducting control over the observance of this Act (Article 11);
 - (b) Considering applications for accreditation by the accredited authorities acting in the territory of the Slovak Republic; granting and withdrawing accreditation to certification authorities; issuing certificates of accreditation;
 - (c) Issuing public key qualified certificates pursuant to Article 7, paragraph 3 to the accredited certification authorities being accredited by it;
 - (d) Disclosing its own public key pursuant to Article 4, paragraph 5(a), issuing the qualified certificate of its own public key pursuant to Article 7, paragraph 5;
 - (e) Issuing qualified certificates of public keys to external certification authorities pursuant to Article 17, paragraph 1(a) and (c);
 - (f) Recording certification authorities acting in the Slovak Republic;

(g) Maintaining records of accredited certification authorities acting in the territory of the Slovak Republic and a list of certification authorities of which accreditation has been withdrawn by it; such a list is disclosed through the disclosing it at a free-accessible Internet page;

(h) Annuling qualified certificate which has been issued to an accredited authority, if it withdraws accreditation of the accredited certification authority, or if that accredited certification authority terminates its activity;

(i) Maintaining the register of external certification authorities recognized by the authority in the territory of the Slovak Republic;

(j) Certification of products for the electronic signature, in particular the security equipment for execution of the electronic signature and the security equipment for time stamp executing, issuance of recommendations, standards, and guidelines in the field of the electronic signature;

(k) Performance of tasks arising to it from law; for performing its task it may request for cooperation also other state bodies and other natural persons and legal entities.

(3) The requirements for the administration of qualified certificates of an accredited authority shall be applicable also to the authority.

Article 11

Control

(1) The Authority may control an accreditation authority since the date when that accreditation authority has notified the authority of the beginning of its activity. A part of control of the accredited authority is also the control of registration authorities acting on behalf of that accredited authority.

(2) For the purposes of the conduct of control the certification authority shall be obliged to enable the empowered personnel of the authority in the inevitable extent to enter in a business and operational rooms upon request to present the completed documentation, records, documents, papers, as well as other supporting documents related to its activity, enabling in the inevitable

extent access to the information system and to provide the information necessary for cooperation.

(3) The authority personnel appointed to conduct control are authorized to require cooperation and information related to the conduct of certification activities from the personnel of an accredited certification authority, of a certification authority, or of a registration authority. The personnel conducting control shall be obliged to maintain confidentiality regarding the matters learnt in the conducting of control. The confidentiality duty shall continue also after their termination of the relationship to the authority. The personnel have not the confidentiality duty if the specific act stipulates so.

(4) If the authority in conducting control identifies that an accreditation authority breaches its obligations arising from this Act, it may in particular:

(a) Restrict, maximum for a 3-month period, or ban a certification authority to conduct or continue in the conduct of any of the certification activities or a certification service, if it has identified that the certification authority:

1. has been not enough security reliable³ to it to act as the certification authority;
2. has not complied with the requirements pursuant to law and generally binding legal regulations;

(b) Impose to annul qualified certificates, if it has identified that qualified certificates had been falsified or insufficiently protected against falsification, or if the equipment for executing guaranteed electronic signatures has reported a security shortcomings that could enable an unobserved falsification of the guaranteed electronic signature or the electronic document signed by such guaranteed electronic signature.

(5) The restriction of activities or the ban on activities of the certification authority pursuant to paragraph 4 do not prejudice the validity of certificates issued by the certification authority till this restriction or this ban.

(6) The restriction of activities or the ban on activities of the accredited certification authority pursuant to paragraph 4, or the withdrawal of accreditation of the accredited certification

³ Article 6, paragraphs (8) and Article 48 of the Act no, 241/2001 Coll.

authority do not prejudice the validity of qualified certificates issued by this the accredited certification authority till this restriction, this ban, or this withdrawal.

Article 12

Certification authority

(1) The certification authority is the certification services provider, and concurrently, it conducts the certification activity.

(2) Providing certification services is considered as business⁴.

(3) It is not required a permit for the conduct of performing certification activities and providing certification services pursuant to this Act.

(4) Accredited certification services are provided on the basis of an accreditation granted by the authority.

(5) Any certification authority shall be obliged already prior to the commencing of providing services to disclose the following:

(a) A Certification Code, in particular comprising the information to whom and under what terms and conditions it provides for services, types of issued certificates, the rights and the obligations of users of its services, a specimen of application for providing services, the rules of using and annulling certificates;

(b) Technical specifications, formats, norms and standards used in conducting activities;

(c) A price list of paid services provided by it, as well as free-of-charge provided services;

(d) Restrictions/limitations in providing its services, if applicable;

(e) The manner of the authentication of identity of an applicant asking for providing its services;

(f) Any information concerning its accreditation.

(6) In addition, any certification authority is obliged to :

⁴ Article 2 of the Commercial Code

(a) Disclose its identification data and the information concerning its certificates;

(b) Notify the authority of the beginning of its activity minimally 30 days in advance.

(7) The certification authority is obliged to quote in the notification of the commencing the activity its business name, the registered office and the identification data of the applicant, a document regarding the authorization to conduct business activities; in the event of a legal entity the certificate of the Register of Companies not older than three months, and the information indented for disclosure pursuant to this Act.

(8) Any certification authority is obliged to disclose the data pursuant to paragraphs 5 and 6 a) on a free Internet page.

Article 13

Accreditation

(1) Any certification authority may ask the Authority for accreditation.

(2) As the accredited certification authority may be any legal entity or any natural person possessing material, room, technical, personnel, organizational and legal conditions for providing accredited certification services. The generally binding legal regulation issued by the authority shall set out details concerning the conditions for providing accredited certification services.

(3) Any certification authority is obliged to present to an application for accreditation to the authority the following:

(a) business name, the registered office, and the identification data of the applicant;

(b) a certificate of the Register of Companies, not older than three months;

(c) a certificate of the Register of Companies of the representatives of statutory bodies of a legal entity, or a certificate of the Criminal Register of a natural person not older than three months;

(d) a public key belonging to the private key which will be used for signing to certificates issued by it,

(e) an outcome of the security audit of its activity,

(f) the information being disclosed pursuant hereto.

(4) If the applicant asking for accreditation does not comply with the condition for granting accreditation pursuant hereto, the authority takes a decision within 90 days since the receipt of the application for accreditation, and it issues a certificate to the certification authority. The granting of accreditation authorizes the certification authority to provide accredited certification services.

(5) If an application for accreditation is not complete, then the authority calls for the certification authority to complete this application at latest within seven days, and, it suspends the proceeding on the accreditation granting for this time period. If the applicant for accreditation by the time of suspension does not complete its application, then the authority refuses such an application.

(6) If the authority identifies that an accredited certification authority does not comply with the conditions for providing accredited certification services, then it may suspend the validity of its accreditation up to three months, and concurrently to impose to take a remedy measures. If the accredited certification authority does not meet the imposed measures within the set time period, then the authority abolishes its accreditation.

(7) Any certification authority, which accreditation has been cancelled, may again apply for granting accreditation.

(8) The application for accreditation is subjects to the administration fee⁵.

Article 14

Obligations of the certification authority and the accredited certification authority in providing certification services and accredited certification services

(1) Certification authority is obliged to:

(a) hold elaborated security rules, and rules of the conduct of certification activities,

(b) observe its security rules and its rules of conduct of certification activities over the whole time period of providing its services,

⁵ National Council of the Slovak Republic Act No. 145/1995 Coll. on the administration fees as amended.

(c) conduct certification activities to disable the execution of copies of private keys, or the maintenance of data of private keys of users of its services; this is not applicable to such private keys which the certification authority uses for the conduct of its own certification services,

(d) notify the authority of any change in the contents and the extent of certification activities provided by it within 30 days;

(e) issue certificates on request on the basis of the contract, which:

1. has been drawn up in a written form and contains an autograph signature of the user; or
2. is an electronic document signed by the guaranteed signatures of both contracting parties;

(f) provide the applicant, prior to conclusion of the contract, with an exhaustive and clear information, in written or electronic form, about its security policy and the rules of providing certification services, and upon request, to provide other natural persons showing the entitled interest with such information;

(g) provide the applicant, requesting issuance of a certificate, with information concerning the products for electronic signatures and the procedures suitable for execution and authentication of the electronic signature;

(h) inform the certificate holder on the possible legal consequences of the used procedure for execution of the electronic signature, as well as about the obligations of the certificate holder and the responsibility of the certification authority;

(i) in the course of conduction of certification activities to provide for:

1. Issuance of certificates comprising of all particularities stipulated herein;
2. In the event if the certificates issued by it comprise of any restrictions, such restrictions shall be evident and recognizable for third parties;
3. Annulment service for certificates issued by it;
4. Disclosure of annulled certificates list;

5. Without any delay informing in writing or in the electronic form the certificate holder about the annulment of his/her certificate;

(j) maintain the operation documentation concerning its certification activities; the generally binding legal regulation issued by the authority shall set out the content and the extent of the operation documentation;

(k) store the relevant documentation concerning to issued certificates pursuant to specific Act⁶.

(2) Any accredited certification authority is obliged to hold designed the security rules, and the rules for the conduct of certification activities prepared pursuant to the rules set out in the generally binding legal regulation issued by the authority.

(3) In addition, any accredited certification is obliged to:

(a) demonstrate the reliability necessary for provision of certification services pursuant to the conditions set out in the generally binding legal regulation (Article 13, paragraph 2);

(b) provide the applicant, asking for issuance of a qualified certificate, with the information about the conditions of using certificates, about the restrictions of using certificates, and the methods of solving disputes, and upon request to provide other natural person or other legal entity showing the entitled interest with such information;

(c) provide the applicant, asking for issuance of a qualified certificate, with the information about technical products, procedures and equipment which the authority has certified pursuant to Article 10, paragraph 2(j), as well as the products for the electronic signature suitable for the execution and the authentication of the guaranteed electronic signature;

(d) while issuing qualified certificates or providing a guarantee pursuant to Article 17, paragraph 1(b) to ensure, that

1. all the information comprising the certificate is correct and exact at the time of the issuance of the certificate;

⁶ National Council of the Slovak Republic Act No. 149/1975 Coll. concerning the archiving as amended.

2. the person given in the certificate at the time of issuance of the certificate is the holder of the private key corresponding to the public key quoted in the certificate;
3. the private key and the public key, belonging to it, correspond to each other in use of the products and the procedures for the electronic signature to execute and to authenticate the electronic signature, delivered or recommended by a certification authority;
4. the certificate is annulled within the set time after the receipt of the entitled application for its annulment;
5. the certificate annulment service is available.

Article 15

Annulment of certificates

- (1) Any certification authority is obliged to annul any certificate administrating by it if:
 - (a) the provisions of this Act have not been complied with at the issuance of the certificate;
 - (b) the certificate has been issued on the basis of untrue data;
 - (c) the certificate holder or the person, whose data are quoted in the certificate, has asks the certification authority for annulment of the certificate;
 - (d) the court has imposed, upon the certification authority, to annul the certificate;
 - (e) the certificate holder demised (in the event of natural persons) or has been winded-up or lapsed (in the event of legal entities);
 - (f) other person than that given in the certificate knows the private key belonging to the public key quoted in the certificate.
- (2) In annulling certificate pursuant to paragraph (1) the certification authority is obliged to annul the certificate within a time period stipulated in its certification code.
- (3) The certificate is deemed as annulled from the time of issuance of the first annulled certificates list comprising that annulled certificate. The validity of the annulled certificate may not be renewed.

(4) Any certification authority is obliged to maintain the documentation concerning applications and incentives for the certificate annulment. The documentation shall comprise in particular the year, month, day, hour, minute and second of the acceptance of applications for the certificate annulment, or identifications of the reasons for the certificate annulment, or reasons for the certificate annulment, as well as data enabling to establish identity of the person asked for the certificate annulment, or to identify the institution or person that submitted the incentive for the certificate annulment.

Article 16

Obligation of the certification authority in administrating certificates

(1) Any certification authority, through the issuing of the public key certificate, acknowledges the authenticity of the submitted public key as well as the fact that the certificate holder disposes of the private key to which belongs the submitted public key.

(2) Any certification authority acknowledges the authenticity of the submitted public key and the certificate holder's certificate so that after the authentication of required particularities issues to the applicant a certificate that is signed by the certification authority through the electronic signature using its private key.

(3) Any certification authority shall conduct the authentication of required particularities of the applicant asking for issuance of a certificate (i.e., documents, ownership of the private key belonging to the submitted public key); this can be done directly by this certification authority or through a registration authority acting on behalf of the given certification authority.

(4) Any certification authority is obliged to establish the conditions enabling the authenticator to authenticate validity of the certificate issued by this certification authority. For this goal any certification authority is obliged to ensure that the public key is available to the authenticator from several information sources.

Article 17

Recognition of external certificates

(1) Any certificate or any qualified certificate, issued by an certification authority with its registered office abroad (hereafter referred to as “the external certification authority”), whose validity can be authenticated in the Slovak Republic can be recognized in the Slovak Republic, if:

(a) the external certification authority, which has issued such a certificate, is registered by the authority, or the external certification authority, which has issued such a certificate, is accredited in the Slovak Republic;

(b) the certification authority with its registered office in the Slovak Republic, in compliance with the requirements of law, provides a guarantee for the certificate validity (e.g., through the issuance of a cross public key certificate of the external certification authority), or the accredited certification authority with its registered office in the Slovak Republic, complying with law, provides a guarantee for the certificate validity (e.g., through the issuance of a cross public key qualified certificate of the external certification authority);

(c) International treaty signed by the Slovak Republic stipulates that the external qualified certificate is recognized as the qualified certificate, or the external certification authority is recognized as the accredited certification authority in the Slovak Republic.

(2) Through the date of the Slovak Republic joining the European Union, any certificate, issued by the certification authority with its registered office in any Member State of the European Union, whose validity can be authenticated in the Slovak Republic, shall become equal to any certificate issued in the Slovak Republic. The qualified certificate issued by the given certification authority shall have the equal legal force and effect as the qualified certificate issued in the Slovak Republic.

Article 18

Archive maintenance

(1) Any certification authority is obliged for minimally ten years to maintain in the archive:

(a) the documentation concerning the organizational, technical and security means used for compliance with the requirements arising from law and from the relevant regulations;

(b) originals of applications for issuance of certificates together with the respective documents proving identity of the applicant;

(c) the documents pursuant to Article 15 (4) corresponding to any annulled certificate.

(2) If the security and the durability of electronic records are safeguarded, the certification authority may maintain the documents pursuant to paragraph (1) also in the electronic form.

Article 19

Responsibility of the accreditation authority for damage

(1) The accredited certification authority is responsible for any damage due to the breaching of its obligations pursuant to the generally binding regulations on the compensation for damage⁷.

(2) If the extent of use of the qualified certificate is limited, then the accredited certification authority is not responsible for damages due to it that the certificate has been used in discrepancy to the restrictions given in the certificate.

(3) If the qualified certificate quotes a limitations concerning the amount of transactions for which it can be used then the accredited certification authority is not responsible for damages due to exceeding of this amount.

(4) It is not possible to exclude in advance the responsibility of the accredited certification authority pursuant to paragraph 1.

Article 20

Obstacles in the activity and termination of activities

(1) Any certification authority is obliged to notify the authority of the occurrence of an obstacle in the conduct of its certification services pursuant to the operation code within 30 days since the date when it has identified such obstacles.

⁷ Article 420 and 420a of the Civil Code

(2) Any accredited certification authority shall notify without any delay the authority if any obstacle arises in the conduct of its accredited certification services pursuant to the operation code.

(3) If any certification authority intends to terminate the conduct of certification services it is obliged to notify of such intention at latest six months in advance the authority as well as any holder of the valid certificate issued by this certification authority.

(4) If any certification authority intends to terminate the conduct of its activity, it can agree with another certification authority upon the taking over of the issued and annulled certificates lists and the operational documentation. If no certification authority takes over such lists, the validity of certificates issued by the lapsing certification authority shall lapse since the date of the lapse of that certification authority.

(5) If any accredited certification authority intends to terminate its activity it can agree with another accredited certification authority upon the taking over of the issued and annulled certificates lists and the operational documentation. If no certification authority takes over such lists, the authority takes them over.

(6) Prior to the termination of activities of an certification authority, its statutory representative is obliged to provide for the conduct of control of the compliance with the Act on the protection of personal data.

Article 21

Registration authority

(1) The registration authority pursuant to Article 2 (s) acts on behalf of the certification authority or on the basis of a contract concluded with the certification authority.

(2) The conduct of certification activities by the registration authority on behalf of the certification authority or on the basis of a contract concluded with the certification authority is not subject to any license or permit.

(3) The registration authority in the conduct of its activity is bond by the certification code of the certification authority on behalf of which is acting, or with which has concluded a contract.

(4) The registration authority shall in particular:

- (a) accept applications for issuance of a certificate;
- (b) Check out concert of data in the application for issuance of a certificate with the data in the presented identification card of the applicant asking for issuance of a certificate;
- (c) Send out applications for issuance of a certificate to the certification authority
- (d) Hand over certificates to applicants asking for issuance of a certificate.

Article 22

Obligations of the certificate holder

(1) Any certificate holder is obliged to

- (a) treat his/her private key with the due diligence to disable any misuse of his/her private key;
- (b) quote accurate, true, and complete information in relation to the certificate of his/her public key;
- (c) without any delay ask the certification authority administrating his/her certificate for the annulment of his/her certificate if he/she finds out that an unauthorized use of his/her private key occurs, or if there is a risk of any unauthorized use of his/her private key, or if any changes in data quoted in the certificate occur.

(2) The certificate holder is responsible for any damage due to the breaching of any obligations of the certificate holder pursuant to the generally binding legal regulations covering the compensation of damage⁸.

Article 23

Protection of personal data

The specific regulation applies to the information system of the provider of certification services.

⁸ Act no. 52/1998 Coll. on the protection of personal data in information systems

Article 24

Requirements of the products for the electronic signature

(1) The security equipment for execution of the electronic signature shall be used for executing guaranteed electronic signatures; such equipment protects the private key stored in it against misuse by an unauthorized person, enabling in a reliable manner to recognize any falsification of electronic signatures and signed electronic documents.

(2) Provisions of paragraph 1 shall adequately apply to the security equipment for execution the electronic signature, if this equipment is used for issuance of private keys.

(3) Any security equipment for execution of the electronic signature and any procedure for execution of guaranteed electronic signature must

(a) in a reliable manner ensure that the signed electronic document in the course of execution of guaranteed electronic signature is not changed;

(b) enable that the electronic document, which will be signed electronically, is displayed to the signatory already prior to a moment when the procedure for execution of guaranteed electronic signature is started up;

(c) guarantee the probability that a private key is executed more than once is negligible;

(4) Such equipment and such procedures for execution and maintenance of qualified certificates must be used to avoid any falsification of qualified certificates.

(5) The equipment and procedures for the electronic signature authentication must safeguard that:

(a) the signed electronic document is not changed in authenticating of the guaranteed electronic signature;

(b) the guaranteed electronic signature is authenticated in a reliable manner, and the outcome of authentication is correctly displayed;

(c) it may be established that the signed electronic document is equal to the electronic document to which the guaranteed electronic signature is executed;

(d) the authenticator may establish a person to whom the given guaranteed electronic signature belongs to, and the use of an alias is clearly denominated.

(6) Paragraphs 1 to 5 adequately apply to the security equipment for the security equipment for the execution of a time stamp pursuant to Article 9.

(7) The authority shall authenticate and acknowledge the compliance of the technical equipment and procedures for executing guaranteed electronic signatures, time stamps, as well as the products for the electronic signature with the security requirements pursuant to Article 10, paragraph 2(j).

(8) The generally binding legal regulation issued by the authority shall set out the requirements for the products for the electronic signature.

Article 25

Audit

(1) Any accredited certification authority shall be obliged to be audited repeatedly by an external audit aimed at the security of provision of certification activities; such an external audit shall terminate at latest within 12 months since obtaining of accreditation, or since the date of the termination of a previous audit. The generally binding legal regulation issued by the authority shall set out details concerning the requirements of auditing, the extent of auditing, as well as the qualification of auditors.

(2) Any accredited certification authority is obliged to present a final report on the outcomes of audit to the authority, this reports shall be accompanied with possible remedy measures, setting terms until when the given shortcomings are fixed. Any accredited certification authority is obliged to present a final report on the outcomes of audit to the authority within 30 days since the termination of the audit process.

(3) If the authority, on the basis of a final report on the outcomes of audit, finds out that any accredited certification authority has breached the obligations stipulated herein, the authority shall impose a remedy measures upon such accredited certification authority, as well as a term within that such accredited certification authority is obliged to fix shortcomings.

Article 26

Sanctions

- (1) The authority shall, for any breach of the obligations pursuant to this Act, impose a fine:
- (a) up to SKK 10,000 000 upon a legal entity or a natural person that provides accreditation certification services without an accreditation;
 - (b) up to SKK 10,000 000 to any accredited certification authority which:
 - 1. does not provide certification services in accordance with this Act and with the security rules set out in the generally binding regulation issued by the authority;
 - 2. does not provide the annulment service for certificates;
 - 3. does not disclose certificates annulled by it;
 - 4. does not disclose its identification data or certificates used in providing certification services;
 - 5. breaches the obligation to notify the authority of the beginning of its activity pursuant to Article 12 paragraph 6(b);
 - 6. conducts an activity which has been suspended for it temporarily.
 - (c) up to SKK 5 million upon an accredited certification authority, also repeatedly, if such accredited certification authority does not provide or conceals information, or does not cooperate with the authority in a control conducted by the authority pursuant to Article 11;
 - (d) up to SKK 1 million, also repeatedly, upon an accredited certification authority breaching the obligations of the accredited certification authority pursuant to Article 14, paragraph 1 (c);
 - (e) up to SKK 1 million upon an accredited certification authority breaching the obligation to annul a certificate or to maintain the required documentation pursuant to Article 15, paragraph 4;
 - (f) up to SKK 1 million upon a certification authority, whose registration authority:
 - 1. does not provide services pursuant to the procedures and in accordance with the security rules of the certification authority;

2. does not provide for accurate, true and complete data concerning the registered persons;
3. does not maintain the documentation concerning the manner of providing services and the security of provided services, does not protect the personal data of registered persons pursuant to the specific regulation;

(g) up to SKK 1 million upon a legal entity misusing a private key of the signatory;

(h) up to SKK 500,000, also repeatedly, upon an accredited certification authority not meeting the obligation to get audited pursuant to Article 25, paragraph 1, or not presenting a final report on the outcomes of audit within the time term pursuant to Article 25, paragraph 2;

(i) up to SKK 500,000 upon a certification authority that

1. does not meet the notification obligation pursuant to Article 14, paragraph 1(d);
2. does not notify the authority within the time period set out herein of the termination of its activity;
3. breaches the obligations of the certificate holder pursuant to Article 22;
4. breaches the obligations of maintaining the archive pursuant to Article 18, paragraph 1(j);

(j) up to SKK 100,000 upon a natural person has misused a private key of the signatory, or submitted untrue data in filing an application for issuance of a certificate.

(2) In imposing a fine, seriousness, duration, and consequences of the illegal acting shall be taken into consideration.

(3) The authority may impose a fine pursuant to paragraph (1) within one year since the date when it finds out the breach of an obligation, but at latest within three years since the date when this breach of an obligation has occurred.

(4) Incomes from fines shall be incomes of the State Budget of the Slovak Republic.

(5) The right of compensation of damages shall not be prejudiced through imposing of a fine pursuant to paragraph 1.

Article 27

Authorization provision

The generally binding legal regulation issued by the authority shall set out details concerning the manner and the process of using the electronic signature.

Article 28

Common provision

The generally binding regulation on the administration proceeding⁹ is applicable to the proceeding of the authority pursuant to this Act, unless this Act stipulates otherwise.

PART II

The following: Act No. 40/1964 Coll., Commercial Code in the wording or the 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., NC SR Act No. 278/1993 Coll., NC SR Act No. 249/1994 Coll., Act No. 153/1997 Coll., Act No. 211/1997 Coll., Act No. 252/1999 Coll., Act No. 218/2000 Coll., Act No. 261/2001 Coll., Act No. 281/2001 Coll., Act No. 23/2002 Coll., Act No. 34/2002 Coll., and Act No. 184/2002 Coll. shall be supplemented as follows:

The following sentence shall be added to Article 25 40 (4) after first sentence:

”The written form is maintained always if the legal act executed through electronic means has been signed by the guaranteed electronic signature.”

⁹ Act no. 71/1967 Coll. on the administration proceeding (Administration Code).

PART III

The following: Act No. 99/1963 Coll., Civil Court Code in the wording of the 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., NC SR Act No. 5/1993 Coll., NC SR Act No. 46/1994 Coll., NC SR Act No. 190/1995 Coll., NC SR Act No. 232/1995 Coll., NC SR Act No. 233/1995 Coll., NC SR Act No. 22/1996 Coll., NC SR Act No. 58/1996 Coll., Constitutional Court SR Judgment No. 281/1996 Coll., Act No. 211/1997 Coll., Constitutional Court SR Judgment No. 359/1997 Coll., of the Act No. 124/1998 Coll., Act No. 144/1998 Coll., Act No. 169/1998 Coll., Act

No. 187/1998 Coll., Act No. 225/1998 Coll., Act No. 233/1998 Coll., Act No. 235/1998 Coll., Constitutional Court SR Judgment No. 318/1998 Coll., Act No. 331/1998 Coll., Act No. 46/1999 Coll., Constitutional Court SR Judgment No. 66/1999 Coll., Constitutional Court SR Judgment No. 166/1999 Coll., Constitutional Court SR Judgment No. 185/1999 Coll., Act No. 223/1999 Coll., Act No. 303/2001 Coll., and Act No. 501/2001 Coll. shall be amended as follows:

In Article 42 (1) first sentence read: "The filing to minutes may be done in written form or orally, via electronic means signed by the guaranteed electronic signature pursuant to the specific act, telegraphically or via facsimile."

PART IV

The following: Act No. 511/1992 Coll. on the administration of taxes and levies and on the amendment in the system territorial financial bodies in the wording of the NC SR Act No. 102/1993 Coll., NC SR Act No. 165/1993 Coll., NC SR Act No. 253/1993 Coll., NC SR Act No. 254/1993 Coll., NC SR Act No. 172/1994 Coll., NC SR Act No. 187/1994 Coll., NC SR Act No. 249/1994 Coll., NC SR Act No. 367/1994 Coll., NC SR Act No. 374/1994 Coll., NC SR Act No. 58/1995 Coll., NC SR Act No. 146/1995 Coll., NC SR Act No. 304/1995 Coll., NC SR Act No. 386/1996 Coll., Act No. 12/1998 Coll., Act No. 219/1999 Coll., Act No. 367/1999 Coll., Act No. 240/2000 Coll. and Act No. 493/2001 Coll. shall be amended as follows:

1. In Article 31 (9) read:

”(9) The registration or the notification pursuant to this Act is presented to the tax administrator on a printed form issued by the Ministry, or may be presented via electronic means signed by the guaranteed electronic signature pursuant to the specific act; the taxation subject is obliged to declare, on such electronic means, that this is the first tax registration, or to quote whether it/he/she has been already tax registered; if yes, when and with which tax administrator, giving the allocated tax identification number, name or title under which it/he/she has been registered, and whether this registration has been withdrawn or abolished, and the reasons why it has been done. The Ministry and the Central Directorate may extend data required for the registration, either in the printed form of registration or in electronic form signed to by the guaranteed electronic signature, if it is dealt with data inevitable for the proper administration of separate taxes.”

2. In Article 31 (17) read:

”(17) The tax payer of a tax of incomes arising from the depending activity and the function benefits is obliged to present within 30 days after the elapsing of calendar quarter an overview of the withdrawn and transferred advances of this income tax and the tax levied through the specific rate for the elapsed quarter to the tax administrator, using the form the specimen thereof is stipulated by the Ministry, or if the respective Tax Office discloses so, it/he/she may present also via the electronic means signed to by the guaranteed electronic signature pursuant to the specific at.”

PART V

Act No. 71/1967 Coll. on the administration proceeding (The Administration Code) shall be amended as follows:

In Article 19 (1) read:

“(1) The filing to minutes may be done in written form, or orally, or via the electronic means signed to by the guaranteed electronic signature pursuant to specific act. It can be done also telegraphically; such filing containing a suggestion in the given matter shall be either in written form or orally added to minutes within three days.”

PART VI

The following: Act No. 141/1961 Coll. on the criminal court proceeding (Criminal Code) in the wording of the Act No. 57/1965 Coll., Act No. 58/1969 Coll., Act No. 149/1969 Coll., Act No. 156/1969 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., NC SR Act No. 6/1993 Coll., NC SR Act No. 156/1993 Coll., NC SR Act No. 178/1993 Coll., NC SR Act No. 247/1994 Coll., Constitutional Court SR Judgment No. 222/1998 Coll., Act No. 256/1998 Coll., Act No. 272/1999 Coll., Act No. 173/2000 Coll., Act No. 366/2000 Coll. and Act No. 253/2001 Coll. shall be amended as follows:

In Article 59 (1) read:

“(1) The filing is always considered pursuant to its contents, even though it is not correctly denominated. It may be done in writing, orally into a minutes/record, or via the electronic means signed to by the guaranteed electronic signature pursuant to the specific act, telegraphically, by facsimile, or by Teletype. The filing done telegraphically, by facsimile, or by teletype, must be confirmed in writing or orally to minutes The provisions of Article 158 remain unconcerned.”

PART VII

The following: NC SR Act No.145/1995 Coll. on the administration fees in the wording of NC SR Act No. 123/1996 Coll., NC SR Act No. 224/1996 Coll., Act No. 70/1997 Coll., Act No. 1/1998 Coll., Act No. 232/1999 Coll., Act No. 3/2000 Coll., Act No. 142/2000 Coll., Act No. 211/2000 Coll., Act No. 468/2000 Coll. and Act No. 553/2001 Coll. shall be amended as follows:

The Title XX shall be added to Annex to the Act on Administration Fee Price

”TITLE XX

THE ELECTRONIC SIGNATURE

Item 268

- (a) The filing an application for accreditation of the certification services provider
..... SKK 20,000
- (b) The filing an application for acknowledgement of the compliance of the technical equipment
for executing and authenticating the electronic signature
..... SKK 10,000.”

PART VIII

This Act enters into force and effect on 1 May 2002, except of Article 4, Article 5, paragraphs (1), (4) and (5), Article 7, Article 8, paragraphs (5) and (6), Article 9, Article 10, paragraphs (2) (a) to (e), (g) and (h) and paragraph (3), Article 11, Article 12, paragraph (4), Article 13, Article 14, paragraphs (2) and (3), Article 24, Article 25. and Article26, which enter into effect since 1 September 2002.

The Act No. 679/2004 Coll. entered into force on 1 January 2005.

The Act No. 25/2006 Col. entered into force on 1 February 2006.

The Act No. 275/2006 Coll. entered into force on 1 June 2006.

Rudolf Schuster

Jozef Migaš

Mikuláš Dzurinda