215

ACT

of 15 March 2002

on electronic signature and on the amendment and supplementing of certain acts as amended by Act No. 679/2004 Coll., Act No. 25/2006 Coll., Act No. 275/2006 Coll., Act No. 214/2008 Coll. and Act No. 289/2012 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 creation and the use of the electronic signature, the rights and the obligations of natural persons and of legal entities 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 unless otherwise agreed by participants.

Article 2

Definitions

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

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

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

(c) "Electronic document" is a digital document maintained at a physical carrier, transmitted or processed by technical means 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 created, if this electronic document is available together with the electronic signature of the respective document;

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

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

(g) "Signature-creation device" is technical equipment or software, or algorithms or a combination thereof, by means of which the signatory can create an electronic signature of an electronic document on the basis of an electronic document and a private key;

(h) "Secure Signature-Creation Device" is a device for creation of the electronic signature complying with the requirements laid down in the present Act and serving for creation of qualified electronic signatures;

(i) "Signature-verification device" is technical equipment or software, or algorithms, or a combination thereof, by means of which the verifier, on the basis of the signed electronic document and the public key belonging to a private key that was used for the creation of this electronic signature, can verify the 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 system users and the access to the system is available only to system users, the information system of public administration[1)] is not a closed system;

(k) "Certification service" comprises in particular the issuance of certificates, the revocation of certificate validity, providing the certificate revocation list, acknowledging the existence and validity of certificates, searching for and providing issued certificates;

(l) "Accredited certification service" is

1. the issuance of qualified certificates, the revocation of qualified certificate validity, providing the list of revoked qualified certificates, acknowledging the existence and validity of qualified certificates, searching for and providing issued qualified certificates (hereafter referred to as the qualified certificate administration);

[1)] Article 2 letter (b) of the Act No. 275/2006 Coll. on Information Systems in Public Administration and on the amendment and supplementing of certain acts.

2. the long-term preservation of electronic documents signed by a qualified electronic signature;

3. the issuance 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 revocation, certificate archiving, and certification activities related thereto;

(o) "Products for the electronic signature" are technical equipments and software, or their relevant parts intended for the certification service providers to carry out certification activities or intended for the electronic signature creation and verification;

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

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

(r) "Accredited certification authority" is a certification authority providing accredited certification services pursuant to this Act, and that has the accreditation of the National Security Authority[2)] (hereafter referred to as the NSA) to provide such services;

(s) "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 create an electronic signature of an electronic document;

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

(v) "Certificate holder" is:

1. a natural person to whom a certificate is issued by a certification authority pursuant

[2)] Article 34 of the Act No. 575/2001 Coll. on Organization of activities of the government and organization of central state administration.

to this Act,

2. a certification authority,

3. the NSA;

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

(x) "Secure device for time stamp creation" is technical equipment and software complying with the requirements of this Act and that can create 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 a technical device intended 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 logically linked to an electronic document. The electronic signature shall comply with the following requirements:

(a) It may not effectively be created 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 creation of this information it may be verified that the electronic document, to which it is attached or otherwise logically linked, is equal to the electronic document used for its creation.

(c) It contains a piece of information that identifies the signatory.

(2) The signatory creates the electronic signature of an electronic document so that on the basis of his/her private key and the electronic document he/she creates new data

complying with the requirements pursuant to paragraph (1) above.

Article 4

Qualified electronic signature

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

(a) it is created by means of a private key intended for the creation of the qualified electronic signature;

(b) it may be created only with the secure signature-creation device pursuant to Article 2, letter (h);

(c) the manner of its creation enables the identification in a reliable manner of which natural person created the qualified 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 creation of the qualified electronic signature.

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

(a) there is a qualified certificate of the public key belonging to the private key used for the creation of the given electronic signature;

(b) it is provable that the qualified certificate pursuant to letter (a) was valid at the time of creation of the given electronic signature;

(c) the electronic document to which the qualified electronic signature is attached or otherwise logically linked is equal to the document used for its creation and that is verified through the use of the public key given in the qualified certificate pursuant to letter (a) above;

(3) The signatory shall create the qualified 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 secure signature-creation device.

(4) The generally binding legal regulation issued by the NSA shall stipulate the format and method of the qualified electronic signature creation.

(5) The public key belonging to the private key intended for the creation of the NSA qualified electronic signature shall be released in the manner as set out in the generally

binding legal regulation issued by the NSA.

(6) The NSA qualified electronic signature shall be valid if the electronic document to which this qualified electronic signature is attached or otherwise logically linked is equal to the document used for its creation, where this has been verified through the use of the NSA public key released in the manner 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 the qualified electronic signature is used in contact with the public administration then the qualified certificate must be issued by the accredited certification authority and must contain the personal number of the certificate holder.

(2) The verifier verifies the electronic signature through a device for verification of electronic signatures using the signed electronic document and the public key belonging to the given signatory.

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

(4) While verifying the qualified electronic signature the verifier shall on the basis of the qualified certificate of the public key verify whether the public key for the qualified electronic signature verification belongs to the signatory.

(5) The generally binding legal regulation issued by the NSA shall stipulate details concerning conditions of validity for qualified electronic signatures, the procedure for verification and conditions of the qualified electronic signature verification.

Article 6

Certificate

(1) A 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 body 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 time of the beginning and the 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 intended for;

(g) an identification of algorithms used in creation of the electronic signature of the body of the certificate.

(4) The certificate issuer creates the electronic signature of the body of the certificate using a private key intended for it.

(5) A pseudonym may be also used as identification data of the certificate holder pursuant to paragraph (3) letter (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 unambiguously determined the identity of the given certificate holder. The certification authority shall state expressly in the certificate that it quotes the pseudonym 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.

(7) A certificate of an accredited certification authority is the certificate which

(a) was issued by the NSA to the accredited certification authority,

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

(c) has a body of the certificate signed by the NSA electronic signature.

(8) A cross certificate of an accredited certification authority is the cross certificate which:

(a) was issued by the accredited certification authority to another accredited certification

authority,

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

(c) has a body of the certificate signed by the electronic signature of the accredited certification authority.

(9) The NSA certificate is the certificate which fulfils the requirements pursuant to paragraph (7) letters (b) and (c) and was issued by the NSA to the own public key of the NSA.

(10) The generally binding legal regulation issued by the NSA shall stipulate the format and content of certificates pursuant to paragraphs (7) to (9) and details about their administration.

Article 7

Qualified certificate

(1) The qualified certificate is a certificate of a natural person complying with the requirements pursuant to Article 6 and

(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 constraints concerning the use of that certificate, if a relying party distinguishes such constraints,

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

(2) The qualified certificate shall be valid at the time period for which its validity is verified, if

(a) this time period is between the beginning and the end of validity of the certificate,

(b) the electronic signature of the body of the certificate is valid,

(c) this certificate has not been revoked over this time period.

(3) The qualified certificate pursuant to paragraph (1) may be also issued to

(a) a natural person acting on behalf of another natural person, the natural person – entrepreneur or the legal entity (hereafter referred to as a deputized person),

(b) a natural person who is authorized to perform activities pursuant to a special regulation,[2b)]

(c) a natural person who carries out functions pursuant to a special regulation,[2c)]

(d) a natural person who is a public official.[2d)]

(4) An accredited certification authority shall issue a qualified certificate to a natural person pursuant to paragraph (3) letter (a) who shall submit the authorization to act on behalf of a deputized person or a natural person who shall prove its position pursuant to paragraph (3) letters (b) to (d).

(5) The qualified certificate issued pursuant to paragraph (3) shall be used by a certificate holder to prove the authorization pursuant to paragraph (3) letters (a) and (b) or to prove the position pursuant to paragraph (3) letters (c) and (d).

(6) In case the authorization of persons pursuant to paragraph (3) letter (a) was annulled or ceased to exist, a deputized person is obliged to apply for the certificate revocation forthwith. In case the deputized person died, was certified dead, ceased to exist or was annulled, the certificate holder is obliged to apply for the certificate revocation. In case the authorization of persons pursuant to paragraph (3) letter (b) or the position of persons pursuant to paragraph (3) letters (c) and (d) was annulled or ceased to exist, the relevant public authority is obliged to apply for the certificate revocation forthwith.

(7) The qualified certificate issued to a natural person pursuant to paragraph (3) letters (b) to (d) cannot contain the pseudonym pursuant to Article 6 (5).

(8) The generally binding legal regulation issued by the NSA shall stipulate the format and content of qualified certificates and details about their administration.

[2b)] For example the Slovak National Council Act No. 323/1992 Coll. on Notaries and Notarial Activities (The Code of Notarial practice) as amended, the Act No. 586/2003 Coll. on Advocacy and on the amendment and supplementing of the Act No. 455/1991 Coll. on Small Trade Business (The Trade Licence Act) as amended, the Slovak National Council Act No. 233/1995 Coll. on Executors and Execution (Code of Execution Procedure) and on the amendment and supplementing of certain acts as amended, the Act No. 382/2004 Coll. on Experts, Interpreters and Translators and on the amendment and supplementing of certain acts as amended.

[2c)] For example the Act No. 385/2000 Coll. on Judges and Judicial Apprentices and on the amendment and supplementing of certain acts as amended, the Act No. 153/2001 Coll. on Prosecution as amended.

[2d)] Article 2 (1) of the Constitution Act No. 357/2004 Coll. on Public Interest Protection at Performance of Public Functions as amended by Act No. 545/2005 Coll.

Article 8

Certificate Revocation List

(1) A certificate revocation list is an electronic document through which the certificate issuer, administrating certificates, notifies a premature revocation of their validity.

(2) The certificate revocation list comprises a body of the certificate revocation list and an electronic signature of the body of the certificate revocation list.

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

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

(b) the date and time of the issuance of the certificate revocation list;

(c) the date and time of the latest issuance of further certificate revocation list;

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

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

(5) The certificate revocation list containing qualified certificates is the certificate revocation list through which the qualified certificate issuer, administrating such certificates, notifies a premature revocation of their validity. The certificate revocation list containing qualified certificates 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 NSA;

(b) the electronic signature of the body of the certificate revocation list is created using a private key intended for this purpose;

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

(6) The generally binding legal regulation issued by the NSA shall stipulate the format, the periodicity of issuing, and the manner of issuance of the certificate revocation list containing qualified certificates.

Article 9

Time stamp

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

(a) it cannot be created 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 for its creation, it is possible to verify that the electronic document to which it is attached or otherwise logically linked is equal to the electronic document used for its creation;

(c) an accredited certification authority has created it using a private key intended for this purpose;

(d) it may be created solely by using a secure device for time stamp creation pursuant to Article 2, letter (x); the generally binding legal regulation issued by the NSA shall stipulate details concerning the requirements for such a secure device;

(e) an accredited certification authority has issued a certificate to the public key belonging to a private key used for its creation;

(f) it enables unambiguously to identify the date and the time when it has been created.

(2) The generally binding legal regulation issued by the NSA shall stipulate the format and the manner of time stamp creation, requirements for the source of time data for time stamp as well as the requirements for the maintenance of time stamp documentation.

Article 10

The NSA

(1) The NSA is the central body of the state administration for the electronic signature.

(2) The NSA shall meet the following roles:

(a) Conducting supervision over the observance of this Act (Article 11);

(b) Considering applications for accreditation of certification authorities acting in the territory of the Slovak Republic; granting and withdrawing accreditation to

certification authorities; issuing certificates of accreditation;

(c) Issuing certificates of public keys pursuant to Article 6 (7) to the NSA-accredited certification authorities;

(d) Releasing its own public key pursuant to Article 4 (5) and issuing the certificate of its own public key pursuant to Article 6 (9);

(e) Issuing certificates of public keys to foreign certification authorities pursuant to Article 17 (1) letters (a) and (c);

(f) Recording certification authorities operating in the Slovak Republic;

(g) Maintaining a list of accredited certification authorities operating in the territory of the Slovak Republic and a list of certification authorities the accreditation of which has been withdrawn by the NSA; such a list is published by the NSA on its website;

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

(i) Maintaining the register of foreign certification authorities whose certificates were recognized by the NSA for the usage in the territory of the Slovak Republic;

(j) Certificating products for the electronic signature, in particular the secure signature-creation devices and the secure devices for time stamp creation, issuing recommendations, standards, and guidelines in the field of the electronic signature;

(k) Performing tasks arising from this Act; for performing its tasks the NSA may request for cooperation also other state bodies and other natural persons and legal entities;

(l) Providing the accredited certification services to the NSA officials and employees and upon request to officials of the police force and employees of the Ministry of Interior of the Slovak Republic to perform the tasks stipulated by a special regulation,[2e)] to officials of armed forces and employees of the Ministry of Defence of the Slovak Republic to perform the tasks stipulated by a special regulation,[2f)] to officials and employees of the Slovak Information Service, to employees of the Ministry of Justice of the Slovak Republic, to courts of the Slovak Republic and to the office of public

---

[2e)] Article 11 letters (a) and (d) of the Act No. 575/2001 Coll. as amended.

[2f)] Article 12 letters (a) to (g) of the Act No. 575/2001 Coll. as amended by the Act No. 78/2005 Coll.

prosecution to perform the tasks stipulated by a special regulation;[2g)]

(m) Maintaining a list of all issued qualified certificates together with the information on their validity sent pursuant to Article 14 (3) letter (e) and providing the information from that list;

(n) Issuing certificates to the NSA-accredited certification authorities for the time stamp service pursuant to Article 2 letter (l) point 3;

(o) Providing the European Commission and Member States of the European Union with lists of accredited certification authorities operating in the territory of the Slovak Republic, with lists of certification authorities whose accreditation was withdrawn by the NSA, with information from the register of foreign certification authorities whose certificates were recognized by the NSA for the usage in the Slovak Republic, and informing forthwith the European Commission and Member States of the European Union of each change and additional information provided.

(p) Maintaining a list of electronic addresses of the location of public authorities' electronic registries which is published by the NSA on its website.

(3) Requirements for the administration of qualified certificates by an accredited certification authority shall be also applicable to the NSA.

Article 11

Supervision

(1) The NSA may supervise a certification authority since the date when that certification authority has notified the NSA of the beginning of its activity. A supervision of the certification authority also includes the supervision of registration authorities acting on behalf of that certification authority.

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

[2g)] Act No. 757/2004 Coll. on Courts and on the amendment and supplementing of certain acts as amended. Act No. 153/2001 Coll. as amended.

information and required cooperation.

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

(4) If the certification authority or the accredited certification authority has utility or business premises located outside the territory of the Slovak Republic, the supervision pursuant to Article 11 shall be replaced by an audit conduct pursuant to Article 25 and the NSA requirements.

(5) If the NSA in conducting the supervision identifies that the certification 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 with the conduct of any of the certification activities or a certification service, if it has identified that the certification authority:
   1. has not been enough security reliable[3)] to act as the certification authority;
   2. has not complied with the requirements pursuant to the Act and generally binding legal regulations;

(b) Impose the revocation of qualified certificates, if it has identified that qualified certificates had been falsified or insufficiently protected against falsification, or if the device for the qualified electronic signature creation has reported security shortcomings that could enable an unobserved falsification of the qualified electronic signature or the electronic document signed by such qualified electronic signature.

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

[3)] Article 6 (8) and Articles 49 and 50 of the Act No. 215/2004 Coll. on Protection of classified information and on the amendment and supplementing of certain acts.

certification authority till this restriction or this ban.

(7) The restriction of activities or the ban on activities of the accredited certification authority pursuant to paragraph (5), or the withdrawal of accreditation of the accredited certification authority do not prejudice the validity of qualified certificates issued by this accredited certification authority till this restriction, this ban, or this withdrawal.

(8) In conducting the supervision pursuant to this Act except procedures laid down in paragraph (4), the NSA proceeds in accordance with principal rules for supervision stipulated by a special regulation.[3a)]

Article 12

Certification authority

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

(2) Providing accredited certification services is considered as business[4)] except conducting the certification activities pursuant to Article 10 (2) letter (l).

(3) It is not required a permit for the conduct of 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 NSA.

(5) The certification authority shall be obliged already prior to the commencing of providing services to release the following without charge:

(a) A certificate policy, in particular comprising the information to whom and under what terms and conditions it provides 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 revoking certificates;

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

[3a)] The Slovak National Council Act No. 10/1996 Coll. on Control in the State Administration as amended.
[4)] Article 2 of the Commercial Code

(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, the certification authority is obliged to:

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

(b) Notify the NSA 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 release pursuant to this Act.

(8) The certification authority is obliged to release the data electronically pursuant to paragraphs (5) and (6) letter (a) on its website.

Article 13

Accreditation

(1) A certification authority may ask the NSA for accreditation.

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

(3) The certification authority is obliged to submit to the NSA along with the application on accreditation the following

(a) business name, the registered office or the address of a place of business activity of the foreign person enterprise or an organizational part of the foreign person enterprise in the territory of the Slovak Republic, 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 Criminal Register 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 the certificates issued by the certification authority;

(e) the information about the fact which accredited certification services wants to provide;

(f) an outcome of the security audit of its activity;

(g) the information being released pursuant to this Act.

(4) If the applicant asking for accreditation has complied with the conditions for granting accreditation pursuant to this Act, the NSA takes a decision within 90 days since the receipt of the application for accreditation, and 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 NSA 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 NSA refuses such an application.

(6) If the NSA 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 remedy measures. If the accredited certification authority does not meet the imposed measures within the set time period, then the NSA revokes its accreditation.

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

(8) The application for accreditation is subject to the administrative fee[5)].

[5)] The Slovak National Council Act No. 145/1995 Coll. on Administrative Fees as amended.

Article 14

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

(1) A certification authority is obliged to:

(a) hold elaborated security rules, and a certification practice statement,

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

(c) conduct certification activities to disable the creation 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 NSA of any change in the contents and the extent of certification services 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 a handwritten signature; or
2. is an electronic document signed by the qualified electronic signature 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 rules of providing certification services, and upon request, to provide other natural person or legal entity 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 creation and verification of the electronic signature;

(h) inform the certificate holder on the possible legal consequences of the used procedure for creation 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 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 relying parties;
3. Revocation service for certificates issued by it;
4. Release of the certificate revocation list;
5. Without any delay informing in writing or in the electronic form the certificate holder about the revocation of his/her certificate;

(j) maintain the operating documentation concerning its certification activities; the generally binding legal regulation issued by the NSA shall stipulate the content and the extent of the operating documentation;

(k) archive the relevant documentation concerning the issued certificates pursuant to a specific act.[6)]

(2) An accredited certification authority is obliged to hold elaborated security rules and a certification practice statement pursuant to rules stipulated by the generally binding legal regulation issued by the NSA.

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

(a) demonstrate the reliability necessary for provision of certification services pursuant to conditions stipulated by 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 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 devices which the NSA has certified pursuant to Article 10 (2) letter (j), as well as the products for the electronic signature suitable for the creation and verification of the qualified electronic signature;

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

1. all the information comprising the qualified certificate is correct and exact at

---

[6)] Act No. 395/2002 Coll. on Archives and Registries and on the amendment of certain acts as amended.

the time of the issuance of the certificate;

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 create and verify the electronic signature, delivered or recommended by a certification authority;
4. the certificate shall be revoked within the set time after the receipt of the entitled application for its revocation;
5. the certificate revocation service is available.

(e) send the lists of issued qualified certificates and lists of revoked qualified certificates to the NSA; the format, method and periodicity of sending these lists shall be stipulated by the generally binding legal regulation issued by the NSA.

Article 15

Revocation of certificates

(1) A certification authority is obliged to revoke a certificate administrating by it if:

(a) the requirements 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 or other person appointed in the contract with the certificate holder requests the certification authority to revoke the certificate;

(d) the court has imposed, upon the certification authority, to revoke 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;

(g) the certificate holder pursuant to Article 7 (3) or a deputized person requests the revocation of the certificate.

(2) In revoking the certificate pursuant to paragraph (1) the certification authority is

obliged to revoke the certificate within a time period stipulated in its certificate policy.

(3) The certificate is deemed revoked from the time indicated as the revocation time in the list pursuant to Article 8 or included in the information pursuant to paragraph (5). The validity of the revoked certificate may not be renewed.

(4) The certification authority provides the information about the status of the certificate by providing the certificate revocation list pursuant to Article 8 containing all certificates, whose validity was prematurely revoked. The certificate whose validity was prematurely revoked must be once, as a minimum, included in the list pursuant to Article 8.

(5) If there have been created technical conditions the certification authority provides the information about the status of the certificate also in the form of receipt of the qualified certificate existence and validity. Particularities of the receipt format of the qualified certificate existence and validity shall be stipulated by the generally binding legal regulation issued by the NSA.

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

Article 16

Obligations of the certification authority in administrating certificates

(1) A 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) The certification authority acknowledges the authenticity of the certificate holder's public key so that after the verification of required particularities it issues to the applicant a certificate that is signed by the certification authority through the electronic signature using

its private key.

(3) The certification authority shall conduct the verification 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) The certification authority is obliged to establish the conditions enabling the verifier to verify the validity of the certificate issued by this certification authority. For this purpose the certification authority is obliged to ensure that the public key is available to the verifier from several information sources.

Article 17

Recognition of certificates issued in other country

(1) A certificate or a qualified certificate, issued by a certification authority with its registered office abroad (hereafter referred to as the foreign certification authority), whose validity can be verified in the Slovak Republic, can be recognized in the Slovak Republic, if:

(a) the foreign certification authority, which has issued the certificate, is registered by the NSA, or the foreign certification authority, which has issued the qualified 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 this Act, provides a guarantee for the certificate validity (e.g. through the issuance of a cross certificate of the public key of the foreign certification authority), or the accredited certification authority with its registered office in the Slovak Republic, complying with the requirements of this Act, provides a guarantee for the qualified certificate validity (e.g. through the issuance of a cross certificate of the public key of the foreign certification authority);

(c) international treaty signed by the Slovak Republic stipulates that the qualified certificate issued in other country is recognized as the qualified certificate, or the foreign certification authority is recognized as the accredited certification authority in the Slovak Republic.

(2) On the day of the Slovak Republic accession to the European Union, a certificate issued by the certification authority with its registered office in any Member State of the European Union, whose validity can be verified in the Slovak Republic, shall become equal to a 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) A 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 this Act 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 (6) corresponding to any revoked 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 accredited certification authority for damage

(1) An accredited certification authority is responsible for any damage due to the breaching of its obligations pursuant to the generally binding legal regulations on the compensation for damage[7)].

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

(3) If the qualified certificate quotes a limitation concerning the amount of transactions

[7)] Articles 420 and 420a of the Civil Code

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) A certification authority is obliged to notify the NSA of the occurrence of an obstacle in the conduct of its certification services pursuant to the operating rules within 30 days since the date when it has identified such obstacles.

(2) An accredited certification authority shall notify without any delay the NSA if any obstacle arises in the conduct of its accredited certification services pursuant to the operating rules.

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

(4) If the certification authority intents to terminate the conduct of its activity, it can agree with another certification authority upon the taking over of the issued and revoked certificates lists and the operating 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 the accredited certification authority intents to terminate its activity it can agree with another accredited certification authority upon the taking over of the issued and revoked certificates lists and the operating documentation. If no accredited certification authority takes over such lists, the NSA takes them over.

(6) Prior to the termination of activities of a 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.[8)]

[8)] Act No. 428/2002 Coll. on Protection of Personal Data, as amended.

Article 21

Registration authority

(1) A registration authority pursuant to Article 2 letter (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 pursuant to this Act.

(3) The registration authority in the conduct of its activity is bound by a certificate policy 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 if the data in the application for issuance of a certificate are truthful and current;

(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) A 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 revocation 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 damage[7)].

Article 23

Protection of personal data

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

Article 24

Requirements of the products for the electronic signature

(1) Secure signature-creation devices shall be used for storage of private keys and creation of qualified electronic signatures; such device protects the private key stored in it against misuse by an unauthorized person, enabling in a reliable manner to recognize any falsification of qualified electronic signatures and signed electronic documents.

(2) Provisions of paragraph (1) shall adequately apply to the secure signature-creation device, if this device is used for creation of private keys.

(3) Secure signature-creation devices and procedures for creation of the qualified electronic signature must

(a) in a reliable manner ensure that the signed electronic document in the course of creation of the qualified 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 creation of the qualified electronic signature is started up;

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

(4) Creation and maintenance of qualified certificates requires the use of such devices and procedures which avoid any falsification of qualified certificates.

(5) Technical devices and procedures for the qualified electronic signature verification must safeguard that:

(a) the signed electronic document is not changed in verification of the qualified electronic signature;

(b) the qualified electronic signature is verified in a reliable manner, and the outcome of verification is correctly displayed;

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

(d) the verifier may establish a person to whom the given qualified electronic signature belongs to, and the use of a pseudonym is clearly denominated.

(6) Paragraphs (1) to (5) adequately apply to secure devices for the time stamp creation pursuant to Article 9.

(7) The NSA shall evaluate and acknowledge the conformity of technical devices and procedures for the creation of qualified electronic signatures, time stamps, as well as other products for the electronic signature with the requirements pursuant to this Act on the basis of an application in the certification process.

(8) The NSA shall evaluate and acknowledge the conformity of an electronic registry with the requirements pursuant to this Act on the basis of an application. The NSA shall issue the certificate of compliance with the requirements pursuant to this Act.

(9) The NSA in proceedings pursuant to paragraph (7) shall decide within 90 days since the complete application for certification of a secure product for the qualified electronic signature has been delivered. If the NSA decides on the conformity of the secure product for the qualified electronic signature with the requirements of this Act, it shall issue the certificate of the secure product for the qualified electronic signature whose validity is maximally five years.

(10) The NSA in proceedings pursuant to paragraph (8) shall decide within 90 days since the complete application for recognition of the conformity of the electronic registry with the requirements of this Act has been delivered. If the NSA decides on the conformity of the electronic registry with the requirements of this Act, it shall issue the certificate of compliance with the requirements of this Act whose validity is maximally five years.

(11) The applicant is obliged to, pursuant to paragraphs (7) and (8), submit to the NSA along with the application the following

(a) technical documentation of the subject matter of the application which is necessary in

the conformity proceedings;

(b) certificates or the security audit of the subject matter of the application; the application pursuant to paragraph (8) does not require the security audit;

(c) the subject matter of the application.

(12) The application is deemed to be complete if it contains the particularities pursuant to paragraph (11). If the application is not complete, the NSA shall ask the applicant to complete the application within 15 working days at the latest. If the applicant does not complete the application by the date stated, the NSA shall stop the proceedings pursuant to paragraphs (7) and (8).

(13) To evaluate the conformity of secure devices for the qualified electronic signature creation and verification with the security requirements the NSA is authorized to require from the applicant the submission of the outcome of performed security audit of the subject matter of the application.

(14) If during the validity period of the certificate of the product for electronic signature issued by the NSA on the basis of proceedings on recognition of the conformity of technical devices for the electronic signature creation and verification the security requirements of this Act have not been changed, the NSA on the basis of the application shall decide in shortened proceeding within 60 days to prolong the validity of the certificate of the product for electronic signature.

(15) Submitting the application for recognition of the conformity of secure devices for the electronic signature creation and verification, submitting the application for recognition of the conformity of the electronic registry with the requirements of this Act and submitting the application for prolonging the validity of the certificate of the product for electronic signature are subject to the administrative fee.[5)]

(16) Products for electronic signature used for the electronic signature creation whose conformity was evaluated by the body pursuant to Article 3 (4) of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures are products for electronic signature pursuant to this Act.

(17) The generally binding legal regulation issued by the NSA shall stipulate the requirements for the products for the electronic signature.

Article 25

Audit

(1) An 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 the accreditation, or since the date of the termination of a previous audit. The generally binding legal regulation issued by the NSA shall stipulate details concerning the requirements of auditing, the extent of auditing, as well as the qualification of auditors.

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

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

(4) Requirements pursuant to paragraphs (1) to (3) apply, as appropriate, to the audit of the certification authority and the accredited certification authority substituting the supervision (Article 11(4))

Article 25a)

Public authorities are obliged to notify without any delay the NSA of the electronic address of the location of the electronic registry which is used for receiving the submissions in the form of electronic documents signed by the electronic signature or electronic documents signed by the qualified electronic signature and of any change of its location.

Article 26

Offences

(1) An offence is committed if someone:

a) misuses a private key of a signer;

b) submits untrue data along with the application for the certificate issuance;

c) breaks the obligation to request the certificate revocation without any delay pursuant to Article 7 (6).

(2) The offence committed pursuant to paragraph (1) letter (a) can be fined up to 3 300 €, the offence committed pursuant to paragraph (1) letters (b) and (c) can be fined up to 6 600 €.

(3) The offences committed in the electronic signature field shall be settled by the NSA.

(4) The generally binding legal regulation on offences[8a)] applies to offences and hearings thereof.

(5) Yields of fines shall be incomes of the State Budget of the Slovak Republic.

Article 26a)

Administrative Offences

(1) The NSA shall, for a breach of the obligations, impose a fine:

(a) up to 330 000 € on a natural person – entrepreneur or a legal entity that provides accredited certification services without an accreditation;

(b) up to 330 000 € on an accredited certification authority which:

1. does not provide certification services in accordance with this Act and with the security rules pursuant to Article 14 (2);
2. does not provide the revocation service for certificates;
3. does not release certificates revoked by it;
4. does not release its identification data or certificates used in providing certification services;
5. breaches the obligation to notify the NSA of the beginning of its activity pursuant

[8a)] The Slovak National Council Act No. 372/1990 Coll. on Offences as amended.

to Article 12 (6) letter (b);

6. conducts an activity which has been suspended for it temporarily.

(c) up to 165 000 € on an accredited certification authority, also repeatedly, if such accredited certification authority does not provide or conceals information concerning providing the accredited certification services;

(d) up to 33 000 €, also repeatedly, on a certification authority breaching the obligations of the certification authority pursuant to Article 14 (1) letter (c);

(e) up to 33 000 € on a certification authority breaching the obligation to revoke a certificate or to maintain the required documentation pursuant to Article15 (4);

(f) up to 33 000 € on 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 33 000 € on a physical person – entrepreneur or a legal entity misusing a private key of the signatory;

(h) up to 33 000 € on a deputized person who breaches the obligation to apply for the certificate revocation without any delay pursuant to Article 7 (6);

(i) up to 16 500 €, also repeatedly, on an accredited certification authority not meeting the obligations to get audited pursuant to Article 25 (1), or not presenting a final report on the outcomes of audit within the time period pursuant to Article 25 (2);

(j) up to 16 500 € on a certification authority that

1. does not meet the notification obligation pursuant to Article 14 (l) letter (d);
2. does not notify the NSA 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 obligation of maintaining the archive pursuant to Article 18 (1).

(2) In imposing a fine, seriousness, manner, duration, and consequences of the illegal

acting shall be taken into consideration by the NSA.

(3) The NSA may impose a fine pursuant to paragraph (1) within two years since the date when it finds out the breach of an obligation in the electronic signature field, but at latest within three years since the date when this breach of an obligation has occurred.

(4) The fine is payable within 30 days since the legal decision to impose a fine has entered into force.

(5) Yields of fines shall be incomes of the State Budget of the Slovak Republic.

Article 27

Authorization provision

The generally binding legal regulation issued by the NSA shall stipulate details concerning the method and procedure of using the electronic signature in business and administrative relations.

Article 28

Common provision

The generally binding legal regulation on the administration proceeding[9)] is applicable to the proceeding of the NSA pursuant to this Act, unless this Act stipulates otherwise.

Article 29

Interim provisions

(1) Public authorities are obliged to notify the NSA of the electronic address of the electronic registry which is used to receive submissions in the form of electronic documents signed by the electronic signature or electronic documents signed by the qualified electronic signature within 6 months since this Act has entered into force. A list of electronic addresses shall be published on the website of the NSA.

(2) An accredited certification authority is obliged to request the NSA to issue the

[9)] Act No. 71/1967 Coll. on Administration proceeding (Administration Code).

certificate for an accredited certification service of time stamp issuing till 31 January 2009.

(3) The accredited certification service of time stamp issuing and verification provided by the accredited certification authority may be provided till 31 January 2009 pursuant to existing rules.

Article 29

Final provision

This Act shall adopt the legal document of the European Community and the European Union specified in the annex.

Entry into force

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 paragraph (2) letters (a) to (e), letters (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 Article 26, which enter into effect since 1 September 2002.

The Act No. 679/2004 Coll. which amends and supplements the Slovak National Council Act No. 511/1992 Coll. on Administration of Fees and Taxes and on Changes in the System of Regional Financial Authorities as amended and on the amendment and supplementing of certain acts (Art. IV) entered into force on 1 January 2005.

The Act No. 25/2006 Coll. on Public Procurement and on the amendment and supplementing of certain acts (Art. II) entered into force on 1 February 2006.

The Act No. 275/2006 Coll. on Information Systems of Public Administration and on the amendment and supplementing of certain acts (Art. III) entered into force on 1 June 2006.

The Act No. 214/2008 Coll. which amends and supplements the Act No. 215/2002 Coll. on Electronic Signature and on the amendment and supplementing of certain acts (Art. I)

entered into force on 1 January 2009.

The Act No. 289/2012 Coll. which amends and supplements the Act No. 275/2006 Coll. on Information Systems of Public Administration and on the amendment and supplementing of certain acts as amended and which amends and supplements certain acts entered into force on 1 November 2012.

Pavol Paška

Annex to Act No. 215/2002 Coll.

A list of adopted legal documents of the European Community and the European Union

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ EC L 13, 19.1.2000; special edition of the EU OJ, chap. 13/volume 24).