ARTICLE:

CONTEMPORARY ENACTMENT OF THE ELECTRONIC SIGNATURE IN THE CZECH REPUBLIC

WRITTEN BY:
PROFESSOR VLADIMÍR SMEJKAL

Introduction

Following the activity of the United Nations Commission on International Trade Law (UNCITRAL),[1] as well as enactments of electronic signature laws in different countries across the world, such as the USA,[2] some European countries[3] decided to incorporate the electronic signature into their legislation. This activity resulted in relatively inconsistent legal regulations, which were united by the Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (EU Directive).[4]

After publishing the EU Directive, both Member States and, at that time, Candidate Countries began to update their existing legislation and published new laws concerning the electronic signature. The Czech Republic was one of the European countries which reacted quickly to the Directive, and on 29 June 2000 it adopted the Act No 227/2000 Coll., on electronic signatures and amendments to some related acts or otherwise, the Electronic Signature Act (ESA).[5] The Parliament of the Czech Republic passed the ESA on 29 June 2000, and it entered into force on 1 October 2000. The ESA was followed by additional implementation regulations, namely the Government Decree No 304/2001 Coll.,[6] implementing the Electronic Signature Act, and the Regulation of the Office of the Protection of Personal Data No 366/2001 Coll.,[7] on Specification of the Terms and Conditions Stipulated in Sections 6 and 17 of the Electronic Signature Act, and on Specification of the Requirements of Electronic Signature Devices.[8]

Since that time, both the Electronic Signature Act and the implementation regulations have been amended several times, but with the exception of the last extensive amendment, implemented by Act No 440/2004 Coll., which came into force on 26 July 2004, the modifications have been of a legislative and technical character. Other alterations were practically not necessary, for when the European Commission evaluated the implementation of the Directive in 2003, it was stated that necessary steps towards the acceptance of the electronic signature by courts and legislation were adopted almost in all countries and – with a few exceptions – the implementation was successful. Nevertheless, it was also stated that the methods of implementation differed between individual countries, and might be a source of certain incompatibilities. According to the report,[9] the Czech Republic is one of the countries that implemented the EU Directive into the national legislation in a standard way.

This article will not focus on the Electronic Signature Act in detail, although a number of basic provisions will be set out. The principal aim of this article is to describe the contemporary enactment of the ESA,

[1] *Model Law on Electronic Commerce, 1996.*

[2] *In 1995, in Utah, U.S.A., the Uniform Electronic Transactions Act, Utah Code Ann. §§ 46-4-101 was passed, followed by the other states that adopted similar laws. Federal laws concerning electronic signature: Uniform Electronic Transactions Act (UETA) and Uniform Computer Information Transaction Act (UCITA) of 1999, which were unified in 2000 by the Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 U.S.C. §§ 7001-7003.*

[3] *Two members of the European Union enacted legislation before the EU Directive was passed: Germany Signaturgesetz (1997) and Italy Legge 25 marzo 1997, n.59.*

[4] *(OJ L13/12 19 January 2000).*

[5] *Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů.*

[6] *Decree No 304/2001 Coll. implementing the Act No 227/2000 Coll., on electronic signatures and amendments to some related acts (Electronic Signature Act).*

[7] *The Regulation of the Office of the Protection of Personal Data No 366/2001 Coll., on Specification of the Terms and Conditions Stipulated in Sections 6 and 17 of the Electronic Signature Act and on Specification of the Requirements of Electronic Signature Devices.*

[8] *For information, Decree No 304/2001 Coll. was replaced by Decree No 495/2004 Coll. of 25 August 2004 that is in force from 1 January 2005.*

[9] *Dumortier, J. and others: Study on legal and market aspects of the application of Directive 1999/93/EC laying down a Community framework for electronic signatures and on practical applications of the electronic signature. K.U.Leuven, Belgium for the European Commission, Directorate General Information Society, Brussels, 2003.*

which is in many respects – from the legislative point of view – is both new, and broadens the original framework as laid out by the EU Directive.

Main principles of the Electronic Signature Act

When implementing the electronic signature into Czech legislation, it was necessary to adhere to the law regulating the form of legal acts, which is set out in the Civil Code.[10] The provisions of the Civil Code on the forms of written legal acts have been changed by the amendment implementing the ESA, and the contemporary statutory text is as follows:

"(3) Písemný právní úkon je platný, je-li podepsán jednající osobou; činí-li právní úkon více osob, nemusí být jejich podpisy na téže listině, ledaže právní předpis stanoví jinak. Podpis může být nahrazen mechanickými prostředky v případech, kdy je to obvyklé. Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.
(4) Písemná forma je zachována, je-li právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila".[11]

"(3) A written legal act shall be valid if it is signed by the acting person; if the legal act is done by more persons, their signatures shall not have to be on the same document unless a special regulation stipulates otherwise. If it is usual, the signature may be replaced with mechanic means. If the legal act is done by electronic means, it may be signed in an electronic way according to special regulations.
(4) The written form shall be kept if the legal act is done by telegraph, telex or electronic means that allow to record its content and determine the acting person."[12]

The electronic means mentioned above are represented by electronic documents to which an electronic signature has been attached in accordance with a special regulation: the ESA.

As for validation procedure (in trials and administrative procedures), it was not necessary to alter the law, because in all procedural regulations of the Czech Republic, free evidence examination is assumed and their form is not limited.[13] In accordance with the Czech laws, the court or administrative bodies are not limited by the form of evidence, in accordance with the provisions of the Civil Code, § 125. This section provides that evidence in any form (free evidence) may serve as evidence: in particular examination of witnesses, an expert's report, reports and statements of authorities, individuals or legal entities, notarial or executorial records and other documents, examining and cross-examination of the participants. Unless the method of adducing the evidence is prescribed, it shall be specified by the court. The provisions of § 132 determine it is for the court to weigh the evidence at its own discretion; the court shall weigh each proof individually and all proofs in their mutual connection; in doing so, the court shall take account all that was revealed in the proceedings including what was stated by the participants.[14]

The above mentioned amendment of the Civil Code, together with the principle of free assessment of evidence that enables the ability to introduce electronic evidence, means that the goal laid down by the Article 5 paragraph 1 of the Directive was reached, i.e. advanced electronic signatures based on qualified certification and created by devices allowing the generation of a safe electronic signature are equivalent to a handwritten signature on paper and are accepted as evidence in trials.

The section describes the electronic signature, defines the certification-service-provider (CSP) and other legal essentials related to the electronic signature, all of which were accomplished within the ESA.

The Act defines the concepts, procedures and subjects of law (individuals and legal entities) by which electronic signatures and advanced electronic signatures are formed, used and verified, to enable electronic documents to be used in a way that complies with the relevant rules of law. The ambition of the legislators was to make the Act as general and technologically independent as possible, otherwise it would be necessary to alter the wording of the Act each time the technology is changed. The definitions of the concepts used in the law follow the EC Directive, while the most important is the difference between various levels of signatures and certificates, which are defined

[10] *Civil Code, Act No. 40/1964 Coll. as Amended.*
[11] *Section 40 of Civil Code, Act No. 40/1964 Coll. as Amended.*
[12] *This translation is from the web of the Ministry of informatics. It is no longer available because it was replaced by the translation of the wording of the last amendment, but for an unknown reason, it was omitted in the new translation of the relevant acts.*
[13] *E.g. Act No. 141/1961 Coll., on Criminal Procedure (The Criminal Procedure Code), as Amended; Act No. 99/1963 Coll., on Civil Procedure (The Civil Procedure Code), as Amended; Act No. 71/1967 Coll., on Administrative Procedure (The Administrative Procedure Code), as Amended.*
[14] *The Civil Procedure Code, § 125 and § 132.*

as follows:

"§ 2 písm. (a) elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě;,
(b) zaručeným elektronickým podpisem se rozumí elektronický podpis, který splňuje následující požadavky
1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,

(k) certifikátem se rozumí datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,
§ 2 písm. l) kvalifikovaným certifikátem se rozumí certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb".

"s2(a): electronic signature (ES) electronic signature shall mean data in electronic form which are attached to or logically associated with a data message and which serve as a method of unequivocal authentication of a signatory in relation to a data message;
(b): advanced electronic signature (AES) shall mean an electronic signature which meets the following requirements:
1. it is uniquely linked to the signatory;
2. it is capable of identifying the signatory in relation to a data message;
3. it has been created and attached to a data message using means that the signatory can maintain under his sole control;
4. it is linked to the data message to which it relates in such a manner that any subsequent change of the data is detectable;

(k) certificate shall mean a data message which is issued by the certificate service provider, links signature verification data to the signatory and is capable of authenticating the signatory; or links electronic mark verification data to the marking person and is capable of authenticating the marking person;
s2 (l) qualified certificate shall mean a certificate with the elements under Section 12 and has been issued by a qualified certification service provider;"

There are four possible variants of using signatures and certificates under the law, but only one of them gives such guarantees that it can be called an electronic form of autograph – advanced electronic signature (AES) in combination with a qualified certificate carried out as a so called qualified signature[15] – AES based on a qualified certificate and created by means of a device for secure signature creation.

The Electronic Signature Act defines the equality of electronic documents (data messages) with paper documents in the same way as the EU Directive, as follows:

"Compliance with the signature requirements (§ 3):
A data message shall be signed if it is furnished with an electronic signature. Unless proved otherwise it shall be assumed that the signatory has familiarised himself with the content of the data message before signing it.
The use of an electronic signature based on a qualified certificate and created using a secure signature creation device shall enable it to be verified that a data message has been signed by the person identified in the qualified certificate.
Integrity of the original (§ 4)[16]
The use of an advanced electronic signature shall guarantee that in the event of interference with the contents of the data message after it was signed such interference will be identifiable".

Thus the law first stipulates, in section 3, under what conditions the data message (the electronic document) is signed, while defining the conditions under which it is possible to check the signature reliably. The second provision, in section 4, guarantees the integrity of the signed message, strictly speaking, it states that the

[15] *See Dumortier, J.: Legal Status of Qualified Electronic Signatures in Europe. In: ISSE 2004 - Securing Electronic Business Processes, S.Paulus, N.Pohlmann, H.Reimer, uit., (Vieweg, 2004), pp. 281-289.*

[16] *The official translation of the Czech law uses the term "Integrity of the original", although in accordance the EU Directive it should be better "Compliance with the original".*

If the certification service provider is not accredited by the Ministry, he shall notify the Ministry at least 30 days prior to the commencement of provision of a qualified certification service that he is going to provide it, and of the moment the provision of it will commence.

integrity infringement can be detected should the authenticity of the electronic signature be checked.

> "Section 5 Obligations of the signatory
> (1) A signatory shall be obliged to
> a) handle advanced signature creation devices as well as data with due care so that no unauthorised use of those could occur;
> b) notify without delay the certification service provider who has issued the qualified certificate that there is a risk of abuse of his advanced signature creation data.
> (2) A signatory shall be liable, under special legal regulations 1a), for damage caused by a breach of obligations under paragraph 1. However, he shall be exempted from liability if he proves that the damaged person had not taken all the action necessary to verify that the advanced signature was valid and its qualified certificate had not been revoked".

The first duty of the signatory is, above all, focused on dealing with the private key, or as the case may be, with devices for signing. The second duty imposes the obligation to inform the certification service provider (CSP) when the key is compromised.[17] The third duty exempts the CSP of responsibility in case that he has been provably deceived by the certificate applicant.

A qualified certification service provider is not liable for damage he did not cause. It is a main principle of the private law, in this case strengthened by the provision of section 5(2) ESA. The signatory is accountable for the damage caused by breach of duty under the Civil Code Special legal regulations (1a) is Civil Code, Sec. 420 (1): "Everyone shall be liable for damage caused by violating a legal duty."[18]

The second apex of the triangle between the signatory and the verifier, e.g. the message recipient, is the certification-service-provider. This is the institution that issues certificates and keeps records, or provides further services relating to electronic signatures. The law imposes a range of duties on the CSP,[19] because the failure of this trustworthy third person would cast doubt upon the whole system of electronic signatures issued by this CSP, if not liquidate it completely.

> "Section 7 Liability for damage
> (1) A qualified certification service provider shall be liable under special legal regulations (1a) for damage caused by a breach of obligations laid down in the present act.[20]
> (2) A qualified certification service provider shall not be liable for damage resulting from the use of a certificate issued as qualified that was due to violation of limits for its use under Section 12 paragraph 2 (i) and (j) and Section 12a (h)".

The law recognises three categories of CSP: a common CSP (Sec. 2 (h) ESA), a qualified CSP issuing qualified certificates (Sec. 2 (i) ESA), and a CSP accredited by the supervisory body (the Ministry of Informatics, hereafter MI www.micr.cz) (Sec. 2 (j) ESA). If the certification service provider is not accredited by the Ministry, he shall notify the Ministry at least 30 days prior to the commencement of provision of a qualified certification service that he is going to provide it, and of the moment the provision of it will commence. At the same time, he shall submit to the Ministry his qualified system certificate referred to in paragraph 1 (a) for verification. (Sec. 6 (2) ESA) The MI is required to be informed that someone intends to issue qualified certificates, even if they have not been accredited.

To ensure a high degree of credibility for documents filed electronically and for electronic communication by the public authority against individuals and legal entities, a requirement formulated in §11 of the ESA,

[17] *Such cases have already occurred in the Czech Republic such as in the area of electronic banking.*
[18] *Civil code § 420, paragraph 1, in accordance with that everybody is liable for damage he caused by breaking of legal duty.*
[19] *See Sec. 6 and 7 ESA.*
[20] *Special legal regulations (1a) is Civil Code, Sec. 420 (1).*

Accreditation is voluntary: every CSP may apply for accreditation with the MI.

has been included in the law - in compliance with Article 3 Section 2 and 7 of the EC Directive in the following wording:

"For the purpose of signing in the sphere of public authorities, it shall be possible to use only advanced electronic signatures and qualified certificates issued by accredited certification service providers. Furthermore, if the AES based on a qualified certificate is used in the area of public authority bodies, the qualified certificate must include such data that would identify the person unambiguously."[21]

An accredited CSP is a CSP that has been accredited under the law. Accreditation is voluntary: every CSP may apply for accreditation with the MI. The Ministry considers whether the applicant meets material, personal and organisational requirements for the qualified CSP's activity under the law,[22] and whether the applicant meets all the legal requirements for accreditation, as set out below:

"Conditions for granting accreditation to provide certification services

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

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

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

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

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

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

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

f) a proof of payment of the administrative fee".

The Ministry renders a decision of accreditation in due course. It is a voluntary accreditation, not subject to any limitation by quota or fee.[23]

At present there are, in the Czech Republic, three accredited certification service providers[24] and several tens of thousands of these certificates have been issued, and their number is rising sharply. In 2005 altogether 12,941 qualified certificates, 167,002 commercial certificates and 980,473 time stamps were issued.[25] Several thousands of common, and particularly so-called commercial (non-qualified) certificates, have already been issued, especially for banking applications. Citizens use the advanced

[21] *Unfortunately, due to the disputes between particular resorts (Ministry of Finance, Ministry of Labour and Social Affairs and Ministry of Interior of the Czech Republic) the long-term dispute about such an unambiguous identification has still not been solved. Whether the so called birth number assigned to every person after birth, or the number of social insurance, or any other new, completely flawless identification should be used.*

[22] *Sec. 9 and 10 ESA.*

[23] *Administrative fee is 100 000 Koruna, i. e. cca 3 300 EUR.*

[24] *První certifikační autorita, a.s. (www.ica.cz), Česká pošta, s.p. (qca.postsignum.cz), eIdentity, a.s. (www.ie.cz)*

[25] *Source: http://www.micr.cz/files/3051/Elektronick__podpis_20060119.pdf.*

electronic signature mainly in the area of tax administration and administration procedures.

The supervisory body in the field of electronic signature is the Ministry of Informatics of the Czech Republic, which is obliged, in accordance with section 9 of the Electronic Signature Act, to:

- award accreditation to those who become accredited providers of certification services,
- assess the conformity of electronic signature devices with requirements stipulated by the Electronic Signature Act on and the relevant regulation,
- verify the qualified certificates of certification service providers having applied for an accreditation,
- supervise whether the Electronic Signature Act is observed.

In accordance with the Regulation No 366/2001 Coll. the Ministry sets the requirements in relation to:

- overall security policy and system security policy of certificate services providers issuing qualified certificates,
- cryptographic modules being used by the providers issuing qualified certificates.

Personal data

As for the protection of personal data, this is not subject to the supervision of the Ministry of Informatics because it is regulated by a special Act, Act No 101 of 4 April 2000 on Protection of the Personal Data and on Amendments to Some Related Acts as Amended (Personal Data Protection Act), which deals with this issue. Supervision over personal data protection is performed by the Office for Personal Data Protection. The Act also stipulates the legal essentials of a qualified certificate, cancellation of a qualified certificate, duties of a qualified certificate services provider at the termination of activity, and defines the means for secure creation and verification of an electronic signature.[26]

Amendment to the Electronic Signature Act from 2004

The amendment to the Electronic Signature Act, implemented in 2004 (effective from 26 July 2004), also included several legislative and technological adjustments, for instance those in connection with the entry of the Czech Republic into the European Union; its substance was, however, different, as described below. Except for the time stamping which is used, but has not yet been codified, the amendment has introduced two important innovations into the Czech legislation that are related to the activities of public authority bodies. They are the so-called electronic sign and electronic public deed.

Electronic mark

The electronic mark is actually an electronic signature created by a technical device. By electronic mark is understood to be data in electronic form attached to the data message or logically connected with it, and to meet the following requirements:

1. they are unequivocally linked to the marking person and are capable of identifying that person by means of a qualified system certificate;
2. they have been created and attached to a data message using an electronic mark creation device that the marking person can maintain under their sole control;
3. they are linked to the data message to which they relate in such a manner that any subsequent change of the data is detectable. [27]

The qualified system certificate is analogous to a qualified certificate in accordance with the Regulation. The qualified system certificate, however, can be issued to a natural person and to a legal entity.

The difference between the signature and the mark is the fact that the mark is not a signature in legal terms because it is created by a technical device, in an automated way.[28] It is not a signature in the sense of the Civil Code because it has not been created by a physical person but a "non-person". But from the perspective of its function, it is the same. The person performing the signature will be replaced by a so-called marking person that is a natural person, legal entity or an organisational unit of a country possessing a means for electronic marks creation and marks data message

[26] *Smejkal, V. a kol.: Právo informačních a telekomunikačních systémů. 2nd edition. Praha, C.H.Beck 2004, ISBN 80-7179-765-0, or Smejkal, V., Bachrachová, H.: Das tschechische Gesetz über die elektronische Signatur. International conference "Internationalen Salzburger Rechtsinformatik Symposions 2002", Salzburg 20–24 February 2002. In: Schweighofer, E., Menzel., T., Kreuzbauer, G.: IT in Recht und Staat. Aktuelle Fragen der Rechtsinformatik. Wien, Verlag Österreich 2002, pp. 329 – 337.*

[27] *Sec. 2(c) ESA.*

[28] *According to the Civil Code, a legal act accompanied by a signature can be performed solely by a physical person. Legal acts of legal entities can be performed by persons authorized to it by a contract on institution of legal entity, founding deed or law (statutory bodies), or other persons if it is stated in the internal regulations of a legal entity or it is usual with respect to their working position. In other words, performing a signature, even in an electronic way, is impossible for legal entities (e.g. a bank or a state) but neither a technical device without any human operator cannot perform a signature.*

with an electronic mark by means of a device for electronic marks creation. It must be set in such a way to be able, without any further control of a marking person, to label only those data message being selected for marking by the marking person. It is not the execution of the operation by a natural person relating to each data message as it is the case of an electronic signature, but it is the setting of certain rules – an algorithm that would control the device. The electronic mark creation device, i.e. a computer, must be protected against unauthorised change and must guarantee that any change will be obvious to the marking person.[29]

Another difference is that in case of an electronic signature, if not proved otherwise, the person performing the signature is supposed to have become acquainted with the content of the data message before signing it.[30] As to the mark, the legal fiction is different. The marking person is presumed to have signed the data message without any previous control of its content.[31] This difference is substantial from the perspective of liability: in the case of an electronic signature the signatory can not argue that they do not know what they signed because they are obliged by law to acquaint themselves with the content of the message; in comparison, in the case of an electronic mark, the knowledge of the marked content is not assumed, hence the marking person can refuse responsibility for the content of the message and they will be obliged to prove who is responsible for the content of the message.

The use of electronic marks is beneficial in such cases when it is necessary, in accordance with the law, to mark trustfully enormous amounts of data messages within a relatively short time (for instance, to acknowledge an electronic data message having been filed from the server of a public authority – tax returns, for example), and the creation of an advanced electronic signature for each data message would be extremely demanding (as to time, people and money), and also in such cases when it is not possible to use qualified certificates. It is expected that electronic marks will be used for customs administration, for issuing of electronic extracts from official databases, to acknowledge receipts of electronic message as stipulated by the law (reports to social security bodies), such as for electronic invoicing.

Regulation § 11 section 2 states that "Documents of public authorities in electronic form marked by an electronic mark based on a qualified system certificate issued by an accredited provider of certification services or signed using a recognised electronic signature shall have the same legal effect as public deeds issued by those authorities."[32] This can be considered to be the most revolutionary moment of the Czech amendment of the Electronic Signature Act. Up until now, public instruments in classic "paper" form were only admitted. The law now enables the public authorities to issue and hand over among themselves electronic public instruments.

In practice, the discreet text means electronic marks based on qualified system certificates as well as recognised electronic signatures are able to ensure the non repudiation of the origin and originality of the data content in electronic form, to which they are attached.[33] They can be therefore full-value parts of electronic documents issued by public authorities only if the law presumes that an advanced electronic signature has been sent by the person whose signature it is, whether they sent it or not – since they have the same function as the official stamp and signature of an authorized person attached to the document. Documents issued by these authorities are called authentic deeds and their content does not have to be proved at formal dealings or legal proceedings, unlike private documents.[34] As soon as technological and organisational conditions are created according to the Act, or other Acts, it will be possible to obtain – now exclusively in electronic form – extracts from various records administered by public authorities, for instance, a copy of the Criminal Record, or an extract from the Land or Commercial Register.

To enable such extracts to be issued in paper form at given places, Parliament is presently discussing an amendment to the Act number 365/2000 Coll., on information systems of public administration; the Act is, by its nature, an act regulating the activity of the Ministry of Informatics, and stipulates the duties of providers of information systems to public administration. The amendment, among others, introduces the possibility of issuing authenticated outputs of information systems of public administration

[29] *Sec. 17a ESA.*
[30] *Sec. 3 (1) ESA.*
[31] *Sec. 3a (2) ESA.*
[32] *Sec. 11 (2). in accordance with sec. 11 (1) recognised electronic signature is advanced electronic signatures and qualified certificates issued by accredited certification service providers.*
[33] *Czech ESA, § 2/b, § 3/2 a § 5/1/a.*
[34] *Documents issued by courts of the Czech Republic or by another state authorities within the scope of their competence as well as documents declared public by special regulations shall certify that they are an order or statement of the authority that issued the document and, unless a contrary has been proved, the truthfulness of what is verified or certified therein. (Sec. 134 of the Civil Procedure Code).*

in the form of documents that would be issued by local authorities, municipalities, notary public, Post Offices and Chamber of Commerce. These authorities will be able to issue documents that would normally be issued by other government departments, only if they will be authorised to do so. An Act on data sharing in public administration by individual public administration information systems is also currently being prepared and should enable the above mentioned issuance of public instruments by authorised persons.

Time stamp

Finally, the item of greatest interest of the Czech legislation is the amendment to the Electronic Signature Act in respect to the time stamp. The time stamp is an instrument that aims to ensure the matching of a relevant time entry to an electronic document in a reliable way. In other words, there is some evidence of the fact that a certain electronic document (a data message) existed at a given time, in accordance with the time stamp that is used. This can be very important in many cases: when filling in the so-called electronic advice of delivery (confirming the delivery of a letter to an addressee), when submitting an income-tax return, or offers in public tenders, and in case of disputes concerning copyright or other rights of intellectual property.

The Act stipulates, in s6b, that the Time Stamp Authority (www.ica.cz) signs the document in an electronic way, including the attached time data and other identification data.[35] The time stamp does not include any identification of a claimant, which means it cannot be used as evidence of the fact that the document was kept by a certain person immediately before the time stamping, but this can be easily solved in a way that the document will be stamped after the holder has attached an electronic signature to the document.

The amendment introduces the so-called "qualified time stamp"[36] which is a data information issued by a qualified certification-service-provider (QCSP) and which joins, in a trustworthy way, data in electronic form with time details, and ensures that the given data in electronic form existed before the given time moment. The stamping must, according to the provisions of s6b contain:

a) the number of a qualified time stamp unique for the given QCSP,
b) an identification of rules under which the QCSP issued the qualified time stamp,
c) specification of the QCSP,
d) time value corresponding to the co-ordinated universal time at the time of creation of the qualified time stamp,
e) data in electronic form for which the qualified time stamp has been issued,
f) electronic mark of the QCSP who issued the qualified time stamp.

Thus the time stamp is again protected against forgery or modification, based on the assumption that the time indicated in the time stamp is correct without any doubt because the QCSP and the user, who sends the document for stamping, guarantees the correct time and the user cannot influence the actions of the QCSP, just as they cannot influence the actions of a notary.

The term "qualified certification-service-provider" sounds new, but in fact it is a legislative abbreviation inserted into the Act for a person issuing qualified certificates, or qualified system certificates, or a qualified time stamp, or means for safe creation of electronic signatures (qualified certification services) and who fulfilled the disclosure requirements to the Ministry of Informatics according to the § 6 of the Act.

It is necessary to mention at this point the existence of a certain trap of a literal interpretation of the definition of a qualified time stamp, which probably comes from a document created by technologists, not by lawyers.[37] One issue will relate to the length of time the data in electronic form for which the qualified time stamping was issued, existed before the given time moment – an hour, a week, a year, a decade? It may be more precise to use another definition, legally more exact, such as "the data existed at the moment of hash creation of the document (for which the time stamping is needed)", or in a simpler way "at the moment of delivery of the document to the QCSP". But this must be solved in its interpretation, and obviously other issues concerning time correlation and relevant risks are also relevant.[38]

The Electronic Signature Act states, in the new s6b(2), that the QCSP shall issue a qualified time

[35] *In fact it is not the document but its sample or hash, which is signed.*
[36] *sec. 2 (r) ESA.*
[37] *RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), Part. 1. Introduction: A time-stamping service supports assertions of proof that a datum existed before a particular time. Similarly ETSI TS 102 023 V1.2.1 (2003-01), part 3.1.*
[38] *Smejkal V.: Novela zákona o elektronickém podpisu a časové razítko (Amendment to the Electronic Signature Act and Time Stamping). Crypto-World, VI., No. 4, pp.2-3.*

However, the important question from the year 2000 still remains: will the public authority endorse and create applications that will work with those new elements?

stamp without delay after receiving an application for its issuance. The question then arises as to what "immediately" means. "Immediately", in a legal interpretation, means "as soon as possible" for which, see the above observation about the moment of the existence of "stamped" data above. The provider of a qualified time stamp is obliged, according to the amendment (Sec. 6b ESA):

"a) ensure that the time stamps issued by him as qualified contain all the elements specified under the present act;
b) ensure that the time data included in a qualified time stamp correspond to the value of the coordinated universal time at the time of creation of the qualified time stamp;
c) ensure that the data in electronic form which are the subject of application for issuance of a qualified time stamp, unequivocally correspond to the data in electronic form contained in the issued qualified time stamp;
d) take appropriate measures against forgery of qualified time stamps;
e) provide upon request to third parties essential information on terms and conditions regarding the use of qualified time stamps, including limitations on their use and information on whether he is accredited by the Ministry or not; such information may be provided electronically".

Cross-border relations

The amendment also responded to the entry of the Czech Republic into the European Union. It is, in particular, possible to acknowledge qualified certificates in EU Member States, to obtain accreditation to act as accredited certification service provider for providers having a seat in a different country, and to issue qualified certificates in accordance with Czech law and the EU Directive.

As to the recognition of foreign qualified certificates, the following is valid:

"(1) A certificate that is issued as qualified by a certification service provider established in a Member State of the European Union shall be a qualified certificate under the present act.
(2) A certificate issued in a state other than a Member State of the European Union as qualified as defined under the present act, shall be a qualified certificate under the present act if
a) the certification service provider complies with conditions of European Community law and has been accredited to operate as an accredited certification service provider in a Member State of the European Union, or
b) a certification service provider established in a Member State of the European Union complying with conditions of European Community law takes over responsibility for the validity and correctness of the certificate in the same extent as with his qualified certificates, or
c) it arises out of an international treaty".[39]

In most cases other Electronic Signature Act amendments are connected with the above mentioned issues. Only some specifications of interpretation result from its application in practice, and from the new conception of an administrative crime, make an exception.

Conclusion

By amending the Electronic Signature Act, it will enable faster development in the transition to the maximum electronic exercise of public authority (e-government) than the provisions of the original version of the Electronic Signature Act. However, the important

[39] *s16 ESA.*

Millions of transactions are entered across the world every day using the typed name in an e-mail, which is a form of electronic signature, but it is not – as far as the Czech understanding is – the most reliable form.

question from the year 2000 still remains: will the public authority endorse and create applications that will work with those new elements? Will they be looking for reasons why it is not possible? To put this into context, Article 2 paragraph 3 of the Czech Constitution reads "The state power serves all citizens and may be applied only in cases, to the extent and in ways stipulated by law." In other words, if it is not stipulated in the law, the state authority is not obliged and cannot even use an electronic instrument if a paper instrument is required by law. Unfortunately in cases when the neutral term "document" – in technological sense – is used, the Czech state authorities are not very active in using electronic documents signed by electronic signature.

The Czech legislation is starting slowly but surely to count on both alternatives: paper and electronic documents. Nonetheless, it means to permanently control the existing legislation and exert pressure on new legal regulations presenters, which is also the long-term effort of the author of this article. It is a never-ending work because public law regulations necessitate explicit legal regulations. However, another solution is not possible. Legal regulations themselves will not increase the use of the electronic signature – at least digital or cryptographic electronic signatures. Millions of transactions are entered across the world every day using the typed name in an e-mail, which is a form of electronic signature, but it is not – as far as the Czech understanding is – the most reliable form.

Certain impetus towards mass introduction of the digital signature is expected, and it is probably only the state, which has been (for a long time already) considering the introduction of chip cards for civil service employees, group identity cards, access passes and digital signature certificates, could do so. Key objectives relating to electronic communications security is to issue smart cards to managing and expert staff of the public administration.[40] Another alternative would be cards of social security and health insurance companies although, even with those, the state plays the crucial and decisive role.

Professor Vladimír Smejkal is a Member of the Government Legislative Council of the Czech Republic and Rector of the Institute of Finance and Administration, Prague, Czech Republic.

http://www.vsfs.cz
smejkal@znalci.cz

[40] *State Information and Communications Policy e-Czech 2006. Ministry of Informatics of the Czech Republic, http://www.micr.cz/files/1288/ENG-SIKP.pdf*