The Basic Terms and Legal Aspects of The ESA from The Practical and Security Points of View

Ján Matejka
matejka@ilaw.cas.cz

The Institute of State and Law of the Czech Academy of Sciences

Pavel Vondruška
pavel.vondruska@uoou.cz

Office for the Personal Data Protection

Abstract

In this paper, the authors deal with the interpretation of some terms of the Electronic Signature Act (hereinafter referred to as the ESA) from the perspective of the security and legal impacts on those individuals who, are affected by this Act. In particular the following issues will be discussed:

- The relationship between Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures and the ESA.
- The legal methods of signing and the types of signatures (signature, handwritten signature, electronic signature, qualified signature, etc.).
- The differences between the types of certification service providers (CA, CSP, CSP-QC, A-CSP).
- The duties of the signatory arising out of the ESA.
- The problems of the application of the ESA in the context of the Czech legal system.

In this paper the relationship will also be described between handwritten signature and qualified electronic signature (advanced electronic signature using a qualified certificate and created via a secure signature creation device). The authors believe that it is exactly this crucial relationship which has not yet been determined in Czech writings and which is not correctly perceived by the public.

The authors in this paper will put emphasis on the explanation of some marginal aspects of the ESA and will outline the possible legal impact of some activities related to the application of electronic signatures in practice.

Keywords: signature, electronic signature, qualified signature, certification service providers, Electronic Signature Act.

1. Introduction

Electronic commerce is emerging as a way of doing business and communicating across public and private networks. An important requirement of electronic commerce is the ability to identify the originator of electronic information in the same way that documents are signed using a handwritten signature. This is commonly achieved by using electronic signatures which are supported by a certification-service-provider issuing certificates, commonly called a certification authority.

In this paper, the authors will deal with the interpretation of some terms of the **Electronic Signature Act** (hereinafter the **ESA**) from the position of the security and legal impacts on those individuals who are affected by this Act. In particular the following issues will be discussed:

Our objective is also to outline the systematic interpretation of some questions concerning the legal adaptations of electronic signing from **the private and public law points of view**. In this sense we would like to warn against several controversial and not very suitable adaptations in law.

In this paper the relationship will also be described **between handwritten signature and qualified electronic signature** (advanced electronic signature using a qualified certificate and created via a secure signature creation device). The authors believe that it is exactly this crucial relationship which has not yet been determined in Czech writings and which is not correctly perceived by the public.

2. The history and the legal framework of the ESA in the Czech Republic

In 2000 the Czech Electronic Signature Act was passed, approved and came into effect. Numerous laws relating to the ESA are in preparation. These laws are intended to codify digital signatures in law.

During its drafting the ESA evolved mainly from Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (hereinafter ”the Directive”) and also from the Draft of UNCITRAL on the uniform rules of electronic signatures (hereinafter ”the Draft of UNCITRAL”).

The approval of the ESA could be considered as a result of the legislative initiatives of the Association for the Information of Society (hereinafter ”SPIS”).

The ESA also contained amendments of relevant legal adaptation. In this case it is necessary to indicate that there are many more acts which were not amended. We may expect a lot of partial amendments. It appears to be necessary to point out that the legal adaptation of the ESA in the field of private law is now fully effective.

3. The legal methods of signing in the Czech legal system

The legal significance of a signature is based on the fact that a signature is a presumption of the validity of written legal transactions (§ 40 art. 3 of the Czech Civil Code). In this sense the signature certifies certain acts (for example the concluding of an agreement).

The written form of legal acts represents one of the pertinence where the existence of a relevant medium is necessary. This medium must have the character of a legal document. In this case it is quite important to discuss the term legal document. The Czech legal system does not contain the legal definition of the term legal document.

On the other hand, a lot of statutory provisions use this term, but the legal definitions are missing.

The absence of these legal definitions could not be considered the fault of the legislator [1]. Legal theory has solved this problem quite successfully. A legal document could be considered as *any material medium, which is capable of recording a matter in writing and perhaps similarly wherever the writing can be recorded* [2]. Here it is also important to point out *that it is immaterial what type of surface it has been recorded on or which substance has been used* [3]. It is possible to say that the theoretical disputes about the legal character of these documents are not practical ones [4].

Similarly to the term legal documents, the legal definition of the term ”signature” is not incorporated in the Czech legal system. However in this case there may be some discrepancies and theoretical and practical problems.

Firstly it is not sufficiently clear how many completed signatures are considered valid and which are not. For example there is almost no agreement on whether the signature ”Your father” or ”Your wife” are valid. Similarly it is not easy to answer the question, whether the mechanically created signature (printer letters ”Max Mayer”), followed by the handwritten signature, etc. may have the appropriate legal effects.

It is very difficult to give a clear answer regarding this matter. To give the appropriate answer to this question it is necessary to outline the classes of signature in the Czech legal system. From the strictly legal point of view it is necessary to differentiate between:

- **signature,**
- **handwritten signature,**
- **authenticated signature** (by a court, notary or administrative official),
- **electronic signature** (with its all enhanced forms).

It is an indisputable fact that every one of above-mentioned classes satisfies the requirements of a signature (§30 art. 3 of the Civil Code).

Legislators quite often demand that a signature is used, but in many cases a handwritten signature is required. In other cases an officially authenticated signature is required. A signature (without any other adjectives) must be considered in its widest sense, and it is possible to fulfil its pertinence via any other enhanced form (handwritten signature, authenticated signature (by a court, notary or administrative official) and electronic signature).

An authenticated signature (by a court, notary or administrative official) is sometimes compulsorily required as a result of legalization. It means that this kind of signature represents the most perfect class of signature. We do not intend to discuss these points at all.

Considering the fact that the Czech legal system clearly distinguishes between individual classes of signature, it is possible to state that in those cases where a handwritten signature (or authenticated signature) is not required a signature (without any other adjectives) may be used [5]. But also in this case it is necessary to respect the limitations of using mechanical signatures in normal cases [6].

As regards the last sentence [7] of § 40 art. 3 of the Civil Code and of other acts it is important to deal with the latest and newest class of signature – electronic signature.

4. The classes of electronic signature

The entire system of electronic signing according to the ESA and Amendments to Certain Other Legislation is based upon a few basic terms. The legal definitions of these terms are introduced in paragraph 2 of the ESA. There are:

- general electronic signature,
- advanced electronic signature,
- data message,
- signatory,
- certification-service-provider,
- accredited certification service-provider,
- certificate,
- qualified certificate,
- signature-creation data,
- signature-verification-data,
- signature-creation device,
- signature-verification device,
- secure-signature-creation device,
- secure-signature-verification device,

- electronic-signature product,
- accreditation.

In our paper we should firstly discuss the two main terms - electronic signature and certification-service-provider.

The term electronic signature did not perceived correctly by the public. Firstly, it is not very clear that there are different classes of electronic signature and secondly, ideas about the security and meaning are very confusing.

The above problems are based mainly on these statements:
- An electronic signature is 100x more secure than a handwritten signature.
- An electronic signature protects the text via coding.
- A signature at the end of an Email is not an electronic signature.
- The only secure signature is an advanced electronic signature.
- It is necessary to distinguish between an electronic signature and only an advanced electronic signature.

The source of these problems is the public statements of some individuals and also the absence of some legal definitions (for example qualified signature, etc.) The main aim of this part is to outline the exact differences and meaning of commonly - used electronic signatures.

For the exact definitions of these terms we need to use the following categories:
- Qualified Certificate Policy,
- Electronic Signature Format,
- Qualified Certificate Format,
- Time-stamping Protocol,
- Security Requirements for Trustworthy Systems,
- SSCD (Secure Signature Creation Device).

The above-mentioned differences between the individual classes of electronic signature may be defined only via the requirements for these classes of electronic signature:
- Electronic signature (general electronic signature),
- Advanced electronic signature,
- Electronic signature using qualified certificate,
- Electronic signature using qualified certificate issued by the accredited certification-service-provider,
- Qualified electronic signature,
- Qualified electronic signature with long-term validity.

These terms are often used in a different context not only in the Directive, but also in ETSI and ISSS/CEN documents.

4.1 General Electronic Signature

If we start with the common legal definition of an electronic signature in the ESA, the electronic signature means *information in electronic form which is attached to or logically associated with a data message and which allows the identity authentication of the signatory in relation to this data message.*

It appears to be important to compare this legal definition with the Directive´s definitions. In this Directive, the term electronic signature ”*... means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”* .

Some discrepancies between the Czech terminology and the European one are obvious. But the meaning is almost the same.

The requirements for our above-mentioned categories are minimal. No time stamp is needed; no format or standard is defined. No certificate or different way of publication is used. There are also no specific requirements for the system or for the signature-creation device (signature-verification device is not defined).

Therefore, the existing requirements will be described in this sheet. Similar sheets will also be used for a description of other classes of electronic signatures.

EESSI Standard	**Option Within Standard**		
Qualified Certificate Policy	Non-Public or Extend Policies	Public Use	Public Use with SSCD
Electronic Signature Format	Electronic Signature	Electronic Signature + Validation Data	Electronic Signature + Validation Data + Time Stamp
Qualified Certificate Format	Qualified Certificate Profile		
Time-stamping Protocol	Profile from IETF Timestamp Protocol		
Security Requirements for Trustworthy Systems	Lower Level	Qualified Level	
SSCD (Secure Signature Creation Device)	Lower Level	Qualified Level	Higher Level

This class of signature does not have very much value for the recipients. Confidence in this signature will be minimal, and should serve as information only – it does not represent a secure way of signing. As an example it is possible to point out that the classic signature at the end of a normal Email is this type of electronic signature.

4.2 Advanced Electronic Signature

Similarly to the term electronic signature, the term Advanced electronic signature is also almost compatible with the Directives.

The Czech legal system defines the term advanced electronic signature in paragraph 2 of the ESA. Advanced electronic signature means an electronic signature, which meets the following requirements:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory in relation to the data message;
- it is created and linked to the data message using devices that the signatory can maintain under his sole control;
- it is linked to the data message in such a manner that any subsequent change of the data is detectable.

The Directives define this term very similarly: Advanced electronic signature means an electronic signature, which meets the following requirements:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control;
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The requirements in relation to our categories are rapidly changing. There is no need of the time stamp and certificate. On the other hand the format for data creation and transmission of the electronic signatures is required. The basic document on this aspect is Electronic Signature Formats (ETSI TS 101 733 V1.2.2, 2000-12).

A new requirement for confidence in the operational system is being introduced. There are no specific requirements regarding signing devices. The security of these devices is the responsibility of the signatory.

The table below again sets out the differences.

EESSI Standard	**Option Within Standard**		
Qualified Certificate Policy	Non-Public or Extend Policies	Public Use	Public Use with SSCD
Electronic Signature Format	Electronic Signature	Electronic Signature + Validation Data	Electronic Signature + Validation Data + Time Stamp
Qualified Certificate Format	Qualified Certificate Profile		
Time-stamping Protocol	Profile from IETF Timestamp Protocol		
Security Requirements for Trustworthy Systems	Lower Level	Qualified Level	
SSCD (Secure Signature Creation Device)	Lower Level	Qualified Level	Higher Level

This class of signature represents for the recipient a really valuable source of information. Confidence in this class of signature is also high. It acts as communication between the sender and the recipient based on the agreement. The recipients must obtain signature-verification-data via a reliable method. Therefore this cannot be used for an anonymous communication. An example of this may be the use of the PGP system.

4.3 Electronic Signature Using Qualified Certificate

For the use of this term it is necessary to explain the following terms:

Certificate means data message, which is issued by the certification-service-provider, and is linked to the signature-verification-data with the signatory and which confirms the identity of that person.

Qualified certificate means a certificate, which meets the requirements laid down by the ESA and was issued by the certification-service-provider, which fulfils the requirements laid down for the certification-service-provider issuing the qualified certificates.

Certification-service-provider is an entity, which issues certificates and keeps regards and provides other services related to electronic signatures.

Accredited certification-service-provider is a certification-service-provider that has been awarded accreditation.

The requirements and duties of a certification-service-provider, which issues qualified certificates are laid down in paragraph 6 of the ESA and also in the forthcoming notice of the ÚOOÚ (Office for the Personal Data Protection). Every certification-service-provider is entitled to request the ÚOOÚ to award accreditation. The conditions are mentioned in paragraph 10 of the ESA. In the Directive voluntary accreditation is required.

An accredited certification-service-provider should be regarded as a trustworthy certification-service-provider.

The principle of voluntary accreditation is touched upon in one provision of the ESA. Paragraph 11 requires the public power sector to use only qualified certificates issued by an accredited certification-service-provider. Therefore the voluntary effect is in this case a necessity.

As regards the different categories, the requirements are more exacting again. The time stamp is also not needed, but an exact format is required. This is mostly regulated in the ETSI document Qualified Certificates Profile (ETSI TS 101 862 V1.1.1, 2000-12).

EESSI Standard	Option Within Standard		
Qualified Certificate Policy	Non-Public or Extend Policies	Public Use	Public Use with SSCD
Electronic Signature Format	Electronic Signature	Electronic Signature + Validation Data	Electronic Signature + Validation Data + Time Stamp
Qualified Certificate Format	Qualified Certificate Profile		
Time-stamping Protocol	Profile from IETF Time-stamp Protocol		
Security Requirements for Trustworthy Systems	Lower Level	Qualified Level	
SSCD (Secure Signature Creation Device)	Lower Level	Qualified Level	Higher Level

The security system requirement is on the same level as in the class above. The requirements for qualified certificates issued by the certification-service-provider are regulated in the forthcoming notice of the ÚOOÚ. In the EC (EU) this problem is solved in the document Policy Requirements for CSPs Issuing Qualified Certificates (ETSI TS 101 456 V1.1.1, 2000 -12).

In this class of electronic signature there is also no need to use the secure-signature-creation device and the secure-signature-verification device.

It is possible to say that this class of electronic signature represents the basic class of electronic signing. Confidence in this class is really high. The recipient does not have to know the sender, the legal certainty of the validity is provided by the ESA. Therefore the above-mentioned agreement is not needed.

Confidence in the certificate is provided via the confidence in the certification-service-provider based upon the ESA. The use of this class is required under the provision of paragraph 11 of the ESA for communication in the public power sector.

Generally we may claim that this class is suitable for direct communication between the parties, but not for long-term validity.

4.4 Qualified Electronic Signature

Now we should discuss the very important term qualified electronic signatures. This term is not directly incorporated in the Czech legal system. In spite of this fact it is quite important to explain this term. The reason for this may be seen in its wide practical and theoretical use.

This term is described in paragraph 3 of the ESA:

The use of an advanced electronic signature based upon the qualified certificate which has been created via a secure-signature-creation device makes it possible to confirm that the data message has been signed by the person named on this qualified certificate.

The difference of this class is based on the fact that here there is the requirement for the use of the secure-signature-creation device. In the ESA this requirement is regulated in paragraph 17. In the EC (EU) many documents deal with this topic. For example these CEN/ISSS documents:

- Secure Signature-Creation Devices (EAL 4 and EAL 4+), (CWA Draft on Area F).
- Security Requirements for Signature Creation Systems (CWA Draft on Area G1).
- Procedures for Electronic Signature Verification V1.0.3 (2001-01-25,CWA Draft on Area G2).
- EESSI Conformity Assessment Guidance; Version 2.0 (2001-01-22, CWA Draft on Area V).

EESSI Standard	Option Within Standard		
Qualified Certificate Policy	Non-Public or Extend Policies	Public Use	Public Use with SSCD
Electronic Signature Format	Electronic Signature	Electronic Signature + Validation Data	Electronic Signature + Validation Data + Time Stamp
Qualified Certificate Format	Qualified Certificate Profile		
Time-stamping Protocol	Profile from IETF Time-stamp Protocol		
Security Requirements for Trustworthy Systems	Lower Level	Qualified Level	
SSCD (Secure Signature Creation Device)	Lower Level	Qualified Level	Higher Level

Exactly the term secure-signature-creation and verification device is one of the most complicated terms in the whole system of electronic autographing (signaturing). The exact requirements have not yet been formulated.

Generally, we may claim that it is possible to divide these requirements into the following three areas:

- Technical – crypto logical requirements.
- Requirements which are essential for the integration of these devices into the operating system.
- Legislative requirements.

Within the limits of this paper it is almost impossible to discuss this wide topic.

From the point of view of the reliability, a qualified electronic signature is considered to be the most perfect. According to this it is possible to discuss the legal framework of this class of signature in relation to the handwritten signature.

In the Czech legal system a handwritten signature is in many cases directly and explicitly required, and therefore it is impossible to use an electronic one, or any of its other higher forms (including a qualified electronic signature). It would be necessary to amend the relevant legislation to change the present legal implementation.

4.5 Enhanced electronic signature

This class is commonly used with any of above-mentioned electronic signatures. The difference is based on the fact that some requirements are added (for example time stamp, additional requirements for signing devices, etc.).

4.6 Qualified electronic signature with long-term validity

The most important class of electronic signature formed as an enhanced electronic signature is the qualified electronic signature with long-term validity. This class will be widely described in the forthcoming ETSI document Policy requirements for CSPs issuing trusted time stamps.

Here the minimum requirements in the area of security and quality of the secure reliable verification of the electronic signature with long-term validity will be regulated. The new term in this area is the term of time stamping. This requirement is specified in the ETSI document Time Stamping Profile (draft ETSI TS 101 861 V.1.1.4).

EESSI Standard	**Option Within Standard**		
Qualified Certificate Policy	Non-Public or Extend Policies	Public Use	Public Use with SSCD
Electronic Signature Format	Electronic Signature	Electronic Signature + Validation Data	Electronic Signature + Validation Data + Time Stamp
Qualified Certificate Format	Qualified Certificate Profile		
Time-stamping Protocol	Profile from IETF Time-stamp Protocol		
Security Requirements for Trustworthy Systems	Lower Level	Qualified Level	
SSCD (Secure Signature Creation Device)	Lower Level	Qualified Level	Higher Level

In accordance with this, it must be ensured the records are kept secure for the whole term of validity. Therefore long-term preservation of the saved data must also rely upon the software, which has been used during these operations.

5. Conclusion

The authors in this paper put emphasis on the explanation of some marginal aspects of the ESA and outlined the possible legal impact of some activities related to the application of electronic signature in practice.

The main contribution of this article should be seen in the systematic interpretation of the individual classes of electronic signature in the Czech legal system. Our objective was also to outline the systematic interpretation of some questions concerning the legal adaptation of electronic signing with the private and public law points of view. One of the main aims of this work was also to compare some terms in the Directives and the ESA.

The authors also tried to discuss several controversial and not very appropriate legal implementations in the Czech Republic.

6. References

[1] Eliáš, K.: Právní úkony na soukromých listinách se zvláštním zretelem k jejich podepisování. AD NOTAM, 1996, c. 3, s.53

[2] Planková, O., in Knapp, V., Luby, Š.: Ceskoslovenské obcanské právo, díl II, Orbis, Praha, 1974, s.593

[3] Krcmár, J.: Právo obcanské, díl V. – Právo dedické, Všehrd, Praha, 1930, s.22

[4] As stated in the commentary for the Civil Judicial Order

[5] Differently the interpretation of Eliáš, K., Právní úkony na soukromých listinách se zvláštním zretelem k jejich podepisování. AD NOTAM, 1996, c. 3, s.54,

[6] § 40 art. 3 of the Civil Code - If the legal transaction is made via electronic devices, it may be electronically signed under special regulation /ESA/

[7] Directive EU: Evropská komise DG XV - Directive 1999/93/EC of 13 December 1999 on a community framework for electronic signatures, http://www.ict.etsi.org/eessi/e-sign_directive.pdf

[8] ETSI, European Telecommunication Standards Institute, http://www.etsi.org/sec/el-sign.htm

[9] CEN/ISSS: http://www.ni.din.de, http://www.cenorm.be/isss/workshop/e-sign

[10] EESSI: European Electronic Signature Standardization Initiative, http://www.ict.etsi.org/eessi/EESSI-homepage.htm, http://www.ni.din.de

[11] ESA : Zákon o elektronickém podpisu c. 227/2000, http://www.uoou.cz

[12] Vondruška, P.: Typy elektronických podpisu, Sborník konference ”Bezpecnost dát 2001”, Bratislava, Slovak Republic

[13] Vondruška, P.: Typy elektronických podpisu, Crypto-World 3/2001 (e-zin), http://www.mujweb.cz/veda/gcucmp