

Legal aspects of electronic signatures in Bulgaria

GEORGE G DIMITROV

Legal Framework

The contemporary Bulgarian law provides a thorough regulation of electronic signatures by a set of primary and secondary normative acts.¹

The Electronic Document and Electronic Signature Act² (EDESA) is the main legislative instrument that regulates the legal regime of electronic documents and electronic signatures, the status of the certification-service-providers and the rules for provision of certification services.³ The law regulates the usage of e-signatures in both the private and public sectors. Usage of e-signatures in the judicial system, the National Bank, the Parliament and some other state bodies should be regulated by separate laws. In the private sector, the law does not apply to contracts for which other laws require qualified written form, or to cases in which the keeping of a document or a copy has a specific legal meaning, such as for bills of exchange, securities and bills of lading. The law was elaborated on the basis of EU Directive 1999/93/EC⁴ (The Directive) and the UNCITRAL Model Law on Electronic Commerce.

The regulation of particular usage of e-signatures and e-documents can be also found in other primary acts such as the Labour Code, the Tax Procedure Code, and the Public Procurements Act, amongst others.

Certain acts of secondary legislation hold rules implementing the EDESA

The Ordinance on the activities of certification-service-providers, the terms and procedures of

termination, and the requirements for provision of certification services⁵ establishes a particular legal framework of the activity of the certification-service-providers and the order and manner for waiving down their activity: the requirements to the qualified certificates profiles; the requirements relating to the information storage for the purposes of provision of services by the certification-service-providers; the requirements with respect to the content, the format and the sources related to data disclosure by the certification-service-providers; the order and manner for directory keeping; the requirements to the certification bodies and auditors and the procedure for accreditation of such persons by the Communications Regulation Commission (CRC).

The Ordinance on the requirements in relation to the algorithms for qualified electronic signatures⁶ establishes statutory requirements to the algorithms for qualified electronic signatures.

The Ordinance on the procedure for registration of certification-service-providers⁷ lays down the order and the conditions, pursuant to which the CRC shall perform a special procedure for registration of certification-service-providers, issuing qualified certificates for universal e-signatures.

Definitions

The law introduces a number of new terms unknown so far to the Bulgarian legal system that should be clarified.

The 'electronic document' is defined by the term 'electronic statement'. Under the law, an

The regulation of particular usage of e-signatures and e-documents can be also found in other primary acts such as the Labour Code, the Tax Procedure Code, and the Public Procurements Act, amongst others

¹ In view of the real necessity of a contemporary legislative framework for the development of electronic commerce, on the one hand, and the strategic emphasis on the harmonization of Bulgarian legislation with that of the European Union, on the other, the Bulgarian Council of Ministers adopted, by its Decision 679 of 29 October 1999, a Strategy for the Development of the Information Society and a National Program for the Information Society. One of the most important elements in this strategy is the development of electronic signatures and the security of information exchange and data protection.

² Promulgated in State Gazette i. 34/06.04.2001, enacted on 07.10.2001, amended SG i. 112/2002, enacted on 05.02.2002.

³ The English version of the act and the implementing ordinances can be found at <http://www.orac.bg/en/resources-links>.

⁴ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 19.1.2000 L13/12).

⁵ Promulgated in State Gazette i. 15/08.02.2002, enacted on 12.02.2002.

⁶ Promulgated in State Gazette i. 15/08.02.2002, enacted on 12.02.2002.

⁷ Promulgated in State Gazette i. 15/08.02.2002, enacted on 12.02.2002.

electronic statement shall be considered any verbal statement, or a statement containing also non-verbal information, presented in a digital form through a generally accepted standard for the transformation, deciphering and visualization of information. An electronic document shall be any electronic statement stored magnetically, optically or in any other manner that provides the capability of being reproduced. The written form shall be considered observed if an electronic document has been created.

The law regulates two main types of electronic signatures 'basic' and 'qualified' as well as a variety of the qualified type of electronic signature, called 'universal'.

Under Article 13, paragraph 1, i.1 of the Bulgarian Law, an electronic signature (basic) shall be considered any information bound to the electronic statement in a manner consented to by the signatory and the addressee, secure enough with a view to the needs of the market exchange, which reveals the identity of the signatory and the consent of the signatory to the electronic statement, and which protects the contents of the electronic statement from subsequent changes.

By contrast, under Article 2, paragraph 1 of the Directive, the 'basic' e-signature shall mean any data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. At the same time, the advanced e-signature is defined by the Directive as an electronic signature that complies with the following requirements: it shall be related in a unique manner to the signatory; it shall be capable of authenticating the signatory; it shall be created by using means in the sole control of the signatory; and it shall be related to the information in such a manner that any subsequent change can be detected.

Improper translation of the definitions provided for by the Bulgarian act might lead to misunderstanding of the regime of the e-signatures and the analysis on the transposition of the Directive into the Bulgarian law.

The Bulgarian law regulates the basic e-signature in the same way as the Directive regulates the advanced electronic signature, without explicitly naming it this way.

The qualified electronic signature (as it is known under the Directive) in Bulgarian law is named as 'advanced' e-signature (literal translation). It is defined to be a transformed electronic statement

attached to, included, or logically associated to the electronic statement. The transformation is to be accomplished through definite algorithms by the use of a private key of an asymmetric cryptosystem. The signature should be created by a secure signature-creation device and it should be supported by a qualified certificate issued by a certification-service-provider.

Furthermore, the Electronic Documents and Electronic Signatures Act introduces different legal consequences for using e-signatures than those provided by the EU Directive and by other national jurisdictions. Article 5, paragraph 1 of the Directive provides that Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure signature creation device satisfy the legal requirements of a signature in relation to data in electronic form, in the same manner as a manuscript signature satisfies those requirements in relation to paper-based data, and that they are admissible as evidence in legal proceedings.⁸ The Directive does not recognize the same legal power of the basic e-signature. Paragraph 2 of Article 5 provides only that Member States shall ensure that an electronic signature is not denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature creation device.

Therefore, the electronic signature as defined under the Directive cannot always be considered an e-signature under the Bulgarian Law. Provided the electronic statement is followed by a basic signature under the meaning of the Directive, under the Bulgarian Law it shall be considered as a kind of authentication information, but the statement shall not be considered signed at all. However, the person that is willing to prove the authorship of such a statement is entitled to do that by means provided for by under the provisions of the Bulgarian Civil Procedure Code. Therefore, the requirements of Article 5 (2) of the Directive shall be considered met.⁹

Under the Electronic Documents and Electronic Signatures Act, all types of electronic signatures are treated legally in the same manner as manuscript signatures with some exceptions. Both main types ('basic' and 'qualified') are equal as regards their legal consequences relative to a

⁸ On the legal effects of e-signatures see Dumortier, J., Nilsson, H., Kelm, S., Van Eecke, P., Skouma, G., *Legal and Market Aspects of E-signatures: A Survey to the European Commission*, September 2003, available in electronic format at http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

⁹ See Kalaydjiev, A., Belaselkov, B., Dimitrov, G., Iordanova, M., Markov, D., Stancheva, V., *Electronic Document and Electronic Signature. Legal Regime*, Sofia: 2004, Ciela Publishing/CSD, p 274.

manuscript signature, except for cases where the signatory or addressee of the electronic statement is the state, a state body or a local government body. A universal e-signature has the meaning of a manuscript signature in respect to everyone.¹⁰

As noted above, the Electronic Documents and Electronic Signatures Act introduces the universal electronic signature as a special type of qualified electronic signature supported by a qualified certificate, issued by a certification-service-provider registered under a special procedure at the Communication Regulation Commission. All citizens and organizations may sign communications directed to state and municipal authorities only with a universal e-signature, and vice versa, in order for such signatures to be considered and legally effected as manuscript signatures. The universal e-signature shall be used by the CRC, the registered certification-service-providers, and all state authorities.¹¹

A particular approach was chosen by the Bulgarian legislator in respect to the actors relating to electronic signatures. The Bulgarian law provides two definitions that are relevant to the electronic signatures – owner and signatory.¹²

An 'owner' of the electronic signature shall be considered the person on behalf of whom the electronic statement has been performed. He is the 'owner' of the e-signature. He could be either a legal or a natural person.

The 'signatory' is the person that is authorized to make electronic statements on behalf of the owner of the electronic signature. Under the law no one but the signatory shall have the right of access to the signature-creation data. The signatory can only be a natural person.

Qualified Certificates

Pursuant to the Electronic Documents and Electronic Signatures Act, similarly to Annex I of the Directive, the qualified certificate shall be an electronic document, issued and signed by a certification-service-provider, that contains certain data for: the identification of the certification-service-provider (CSP) and the State in which it is established; the name of the signatory, which shall be identified as such and specific attributes of the signatory to be included if relevant, depending on the purpose for which the certificate is intended; the public key which corresponds to the private key under the control of the signatory; an indication of the beginning and end of the period of validity of the certificate; the identity code of

the certificate; the qualified electronic signature of the CSP issuing it; any limitations on the scope of use of the certificate, and of the value of the transactions.

In divergence to the Directive, under Bulgarian law the certificate should contain the full name of the signatory but not their pseudonym. However, such could be envisaged as complementary information. Furthermore, the certificate must also contain: the identification of the owner of the e-signature, the grounds of the representative power granted by the owner to the signatory to sign on his behalf and when the authorization of the author originates from other authorized persons, the certificate must contain data for these persons as well; the signature algorithms to be used by the signatory and by the CSP; the liability and the guarantees of the CSP; a reference (by way of a hyperlink) to the certificate list holding the certificate of the CSP, as well as to the registration of the provider in the CRC, if the CSP is registered.

The law does not explicitly provide that the certificate must contain an indication that it is issued as a qualified certificate, but the interpretation of the statutory rules lead to a conclusion that such indication should be present. Strict requirements are provided in respect of the organization and maintenance of the registers of the certificates issued by the providers of certification services.

Certification-service-providers

Chapter II of the law regulates in detail the requirements, activities, rights and obligations of certification-service-providers in issuing certificates, providing access to published certificates to any third person and the provision of services for the creation of private and public keys for qualified electronic signatures.

There are two types of certification-service-providers under the Electronic Documents and Electronic Signatures Act: those that are unregistered, and those that are registered with the CRC register. Unregistered certification-service-providers shall be obliged to notify the CRC only upon the commencement of their business activities as such. No prior authorization is required. These certification-service-providers are not entitled to issue certificates for universal e-signatures. As noted, such certificates can be issued by certification-service-providers registered by the CRC under a special procedure only. Nevertheless, as there is no legal requirement for

¹⁰ Art.13, para.3 EDESA.

¹¹ Art. 33, para.2 EDESA.

¹² Art. 4 EDESA.

Under Bulgarian law, the CSP shall be liable in all cases when the signature-creation data and the signature-verification data cannot be used in a complimentary manner even when the signatory has generated them

authorization, for practical purposes the CRC shall determine whether the applicants meet the stricter requirements of the Electronic Documents and Electronic Signatures Act and hence whether they could be registered or not. The acts of the CRC are subject to administrative and court review.

The law provides that the Council of Ministers shall adopt regulations providing greater detail as to the requirements for the activities of certification-service-providers regarding the following: maintaining sufficient funds for securing their activities in compliance with the requirements of the law; their insurance for liability, arising of non-performance of their obligations; providing necessary technical equipment, and so forth.¹³

Liability

In respect of establishing trust in electronic signatures, the Electronic Documents and Electronic Signatures Act provides particular rules for the liability of the certification-service-providers to the signature owner and to all third parties for damages caused by the non-fulfillment of the statutory requirements for their activities and duties.¹⁴

Similarly to the Directive, the CSP shall be liable as regards the accuracy of all information contained in the qualified certificate at the time of its issuance and as regards the fact that the certificate contains all the details prescribed for a qualified certificate. It shall be liable for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate, and for failure to register revocation.

However, in divergence to the Directive, the CSP shall be liable for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both. Under Bulgarian law, the CSP shall be liable in all cases when the signature-creation data and the signature-verification data cannot be used in a complimentary manner even when the signatory has generated them. This is due to the fact that the CSP is obliged to check the correspondence of the key pair at the time of issuance of the certificate. Furthermore, under Bulgarian law the special liability grounds encompass all cases of non-performance of the statutory duties by the CSP as defined in Article 21

(the requirements for its activity, such as: maintaining sufficient financial resources, usage of trustworthy systems, employment of qualified personnel), Article 22 (general obligations of the CSP: to issue certificate, to publish the certificate, to perform prompt suspension, revocation and restoration of the certificate, to provide the customers with certain information), and Article 25 (specific duties in respect to certificate issuance process).

Similarly with the approaches of the other jurisdictions, under the national liability rules the certification-service-provider shall not be held liable for damages, caused by the certificate usage and for the value of transactions exceeding the indicated limits of the certificate. The rule is imperative.

In respect to the types of the fault within the limits of the liability exposure, under the general Bulgarian civil law likewise the laws in many other jurisdictions, exemption of liability can be agreed upon between the parties by contract. Releasing of liability cannot be agreed for willful misconduct or gross negligence (Article 94 of the Law on Obligations and Contracts). For the CSPs there are further limitations. Under Article 29, paragraph 3, apart from willful misconduct, parties cannot agree upon exemption of liability of the CSP for any type of negligence.

When speaking of liability, the provision of an insurance against the liability risk is mandatory for a CSP established or operating in Bulgaria. The CSP shall be obliged to have minimum insurance coverage for damages it might cause as follows: i) 100,000 BGL (ca 50,000 EUR) for damages caused to any person in any single case for the CSP issuing qualified certificates with limitation of the scope of the usage of the certificate or the value of the transactions; ii) 500,000 BGL (ca 250,000 EUR) for damages caused to any person in any single case for the CSP issuing qualified certificates without limitation of their usage; and iii) 600,000 BGL (ca 300,000 EUR) for damages caused to any person in any single case for the CSP issuing universal certificates.

Considering the above, it becomes obvious, that the scope of the special liability grounds under Bulgarian EDESA is broader than the one of Article 6 of the Directive.

Another issue of interest seems to be the approach of the Bulgarian legislator to explicitly establish binding value of the Certification Practice Statements (CPS) and the Certificate Policy (CP)

¹³ The Ordinance on the Activities of Certification-service-providers, the Terms and Procedures of Termination Thereof, and the Requirements for Provision of Certification Services. See *supra* note 4.

¹⁴ For thorough analysis on the transposition of Article 29 of EDESA see Dumortier, J., et al., *ibid*, p 244.

employed by the certification-service-provider. Under the Bulgarian Law the CPS and the CP jointly constitute General Terms, binding to the CSP and to the owner on contractual grounds. Therefore any acts, omissions or failures to comply with the provisions of the CPS and the CP would engage the liability of the CSP on a common civil liability grounds. The general rules could be found in the Commercial Act, the Law on Obligations and Contracts (especially the provision of Article 16).

In respect to the relying party, under Bulgarian law the CPS/CP is not binding. Therefore any acts or omissions or failures to comply with the CPS/CP could entail the liability of the CSP on a general tort grounds only by using the CPS/CP as a measure and criterion for the due care of the CSP to act. It should be proved that the negligent behavior of the CSP in discrepancy with the prescriptions of the CPS/CP has caused the damage to the relying party.¹⁵

The law provides further rules for the liability of the signatory of utmost good faith towards parties when, for the generation of the public and private keys, he has used an algorithm that does not fit the statutory requirements.

For the signature holder also incurs liability to third parties in cases where: the signatory does not follow the security requirements as strictly defined by the certification-service-provider; he fails to request that the certification-service-provider terminate the certificate if he becomes aware that the private key has been used unlawfully or that there is a risk of it being used unlawfully; the signatory is not authorized to hold the private key corresponding to the one identified in the certificate public key; and he makes untrue statements before the certification-service-provider relating to the contents of the certificate.

The signature holder and the signatory shall always be liable to the certification-service-provider when they provide untrue data or fail to provide the data required.

Supervision

The Bulgarian law has provided for an adequate supervisory scheme for provision of certification services. The state body authorized to perform supervision on the activities of the certification-service-providers in Bulgaria is the Communications Regulation Commission.

The Communications Regulation Commission (CRC), is an independent specialized state

authority, a legal person with its head-office in Sofia and its own budget. The CRC comprises five members and has its own administration. It implements the telecommunications sector policy and the postal sector policy adopted by the Council of Ministers, taking due account of public interests, state sovereignty and national security. The CRC regulates and supervises the telecommunication activities under the terms provided for in the Telecommunications Act, and the postal services provision under the terms provided for in the Postal Services Act.

Further to the above functions in the area of e-signatures, the CRC exclusively drafts, coordinates and proposes to the Council of Ministers the adoption of secondary legislation. It also supervises and controls the activities of certification-service-providers in general, the form of the certificates to be issued, and the preservation of information on the services provided by certification-service-providers amongst other things.¹⁶

Those CSPs that operate under the meaning of the Bulgarian law, and provide services on the territory of Republic of Bulgaria, despite of their nationality or place of establishment are also subject to supervision.¹⁷ The controls constitute regular or incidental method of supervision. They could be carried out at any time even after a complaint as a repressive measure. However, there is no explicit provision where the Commission shall be obliged to perform repressive control upon the placing of a complaint. The control could be initiated by the Commission itself at any time, despite the submission of external complaints or by performing a regular check. The controls could be carried by the officials employed by CRC or by designated external persons such as auditors, bodies and laboratories. The Commission keeps and maintains a list of such designated persons.

Use of Electronic Signatures by the State and the Municipalities

Under the Electronic Documents and Electronic Signatures Act, state and municipal authorities shall be obliged to accept and issue electronic documents. The exact state authorities shall be determined by the Council of Ministers, when they are subordinated to the Council. Usage of e-signatures by state bodies that do not fall within this scope, like the National Assembly, the Bulgarian National Bank, and the Constitutional Court, for instance, shall be regulated by a special

The signature holder and the signatory shall always be liable to the certification-service-provider when they provide untrue data or fail to provide the data required

¹⁵ As general grounds for tort (delictual) liability could be referred art.45 of the Law on Obligations and Contracts.

¹⁶ The scope of CRC duties and powers could be found in Chapter IV and V of EDESA.

¹⁷ As a 'place of establishment' is meant jurisdiction under which the entity is registered or established and recognized as such.

law. The usage of e-signatures in the judicial system will also be regulated by a separate law. There are no such laws adopted so far. The obligations of municipal authorities and other state authorities shall be regulated by their own by-laws. The procedure and manner in which electronic documents shall be recorded shall be set by internal rules.¹⁸

The Council of Ministers has recently adopted a regulation¹⁹ by which it obliged all Ministries, State Agencies, District Governors, and some other national state authorities as of 1 January 2005 will be required to accept and issue documents in electronic form signed with a universal e-signature. Thus, any interested citizen shall be entitled to communicate electronically with the state authorities and to request the issuance of licenses and certificates electronically.

Furthermore, a set of draft amendments to certain normative acts is expected to be enforced to make possible the usage of e-signatures in the judiciary for the purposes of civil and criminal procedure. That would provide the courts with the possibility to issue verdicts and court decisions in electronic form, signed with a universal e-signature, and will enable the citizen to submit applications and claims electronically.

International Aspects

With regard to the possibility for recognizing in Bulgaria the legality of certificates issued by foreign certification-service-providers, the Electronic Documents and Electronic Signatures Act establishes particular rules.

Under the law, all certificates issued by foreign certification-service-providers in accordance with their home country legislation shall be recognized as fully effective on the territory of Bulgaria, provided one of the following requirements is met: i) the obligations of the certification-service-provider that issued the certificate and the requirements for its activities meet the requirements envisaged by the law, and the certification-service-provider has been recognized in his home country; or ii) a local certification-service-provider accredited by the respective accreditation organization or a duly registered certification-service-provider undertakes an obligation to be responsible for the acts and the omissions of a foreign certification-service-provider;

or iii) the certificate or the certification-service-provider that issued the certificate are recognized pursuant to a legally enforced international contract.

The first two requirements shall be certified by the CRC, which has to enter in a special register data for foreign certification-service-providers regarding the certificates for their public keys, as well as for a Bulgarian certification-service-provider that has undertaken responsibility for a foreign certification-service-provider.

Penalties

To ensure observance of the provisions of the law by its addressees, certain administrative fines are introduced. For natural persons, these fines range from BGN 100 (ca EUR 50) to BGN 10,000 (ca EUR 5,000), provided that an act does not constitute a crime. Legal entities shall be subject to fines ranging from BGN 500 (ca EUR 250) to BGN 50,000 (ca EUR 25,000). ■

© George G Dimitrov, 2004
George G Dimitrov, LL.M., is the Managing Partner of Dimitrov, Petrov & Co (ORAC), a Bulgarian Law Firm in Sofia. The author is a member of the working group drafting the implementing regulations for the Electronic Documents and Electronic Signatures Act and Chairman of the Bulgarian Center for ICT law.

george.dimitrov@orac.bg
<http://www.orac.bg>

¹⁸ Presently certain state authorities provide for possibility for electronic communication with citizen and provision of e-government services by using e-signatures. Such authorities are the Ministry of Transport and Communications, the General Tax Directorate for submission of VAT tax declarations through web interface, the National Social Security Institute for the purposes of registration of labour contract, the Ministry of Finance for the purposes of provision of small public procurements through Internet, etc.

¹⁹ Regulation 153 of the Council of Ministers of 5 June 2004 for Specification of the State Authorities under Art.41, para.1 of EDESA, promulgated in State Gazette i. 61/13.07.2004.