BULGARIA'S NEW LAW ON ELECTRONIC DOCUMENTS AND ELECTRONIC SIGNATURES

This Feature Report was written by George G. Dimitrov, LL.M., Managing Partner of the O.R.A.C. Dimitrov, Petrov & Co., Bulgarian Law Firm, Sofia. The author, a member of the working group drafting the implementing regulations for the Law on Electronic Documents and Electronic Signatures, may be contacted by telephone at (359 2) 987-7096 and 987-8641 or by E-mail at george.dimitrov@orac.bg.

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.

On 6 April 2001 the new Law on Electronic Documents and Electronic Signatures was promulgated in the State Gazette. The law was enacted under a special *vocatio legis* term and will enter into force six months after the date of its promulgation *(see BEER, May 2001, page 11)*.

The law was elaborated on the basis of EU Directive 1999/93/EC (hereinafter "The Directive") and the UNCITRAL Model Law on Electronic Commerce. The implementing regulations for the law are expected to be adopted by the end of September.

Objectives Of The Law

The Law on Electronic Documents and Electronic Signatures aims to provide legal regulation of electronic documents and electronic signatures and the rules and conditions for providing certification services. The law does not apply to contracts for which other laws require qualified written form, or to cases in which keeping a document or a copy of a document has specific legal meaning, such as for bills of exchange, securities, bills of lading etc.

Terms

The law provides a number of new terms for Bulgarian law that are clarified:

"Electronic document" is defined through the term "electronic statement". Under the law, an electronic statement (communication) shall be any verbal statement, or a statement containing non-verbal information, presented in 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—"regular" and "advanced"—as well as a variety of the advanced type of electronic signature, called "universal". Both main types are equal as regards their legal consequences relative to a hand-written 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 hand-written signature in respect to everyone.

A regular electronic signature shall be any information relating to an 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.

Under Article 2, paragraph 1 of the Directive, an e-signature means any data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

Hence, in comparison with the Directive, the Bulgarian law provides stricter treatment of a regular electronic signature: Such a signature shall protect the contents of the electronic statement from subsequent changes and the connection between the electronic signature and the electronic statement shall be consented to in advance by the signatory and the addressee. The definition of a regular electronic signature also includes another subjective element: The electronic signature shall reveal the consent of the signatory to the electronic statement.

An advanced electronic signature is defined in the Law on Electronic Documents and Electronic Signatures as a transformed electronic statement included, added, or logically related to the electronic statement. The transformation is to be accomplished through algorithms, including the use of a private key of an asymmetric cryptosystem.

By contrast, the Directive defines an advanced electronic signature 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;

10/01 Copyright © 2001 The Bureau of National Affairs, Inc. BEER ISSN 1058-7365

- 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.

Although the Law on Electronic Documents and Electronic Signatures' definition of advanced electronic signature differs from the one in the Directive, in general the same effect is reached.

Furthermore, the Law on Electronic Documents and Electronic Signatures introduces different legal consequences of using e-signatures than those provided by the EU Directive and by other 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 hand-written signature satisfies those requirements in relation to paper-based data, and that they are admissible as evidence in legal proceedings. The Directive does not recognize the same legal power of the regular 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.

Under the Law on Electronic Documents and Electronic Signatures, all types of electronic signatures are treated legally in same manner as hand-written signatures with some exceptions.

As noted above, the Law on Electronic Documents and Electronic Signatures provides for a universal electronic signature—a special type of advanced electronic signature that is certified by a certification service provider registered under a special procedure by the State Telecommunications Commission (the "STC"). All citizens and organizations may sign communications 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 hand-written. Universal e-signature shall be used by the STC, registered certification service providers, all state authorities, etc.

Certificates

Pursuant to the Law on Electronic Documents and Electronic Signatures, a certificate shall be an electronic document, issued and signed by a certification service provider, that contains certain data for the certification service provider, the signatory of the advanced electronic signature, the natural person (author) authorized by the signatory holder to perform electronic statements, the public key, the identificators of the algorithms, the term of issuance, suspension and termination, the term of validity, restrictions, the identification code of the certificate, the liability and guarantees of the supplier of certification services, etc.

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 advanced electronic signatures.

There are two types of certification service providers under the Law on Electronic Documents and Electronic Signatures—those that are unregistered, and those that are registered with the STC register. Unregistered certification service providers shall notify the STC only on the beginning 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 STC under a special procedure. Nevertheless, as there is no legal requirement for authorization, for practical purposes the STC shall determine whether the applicants meet the stricter requirements of the Law on Electronic Documents and Electronic Signatures and hence whether they are to be registered or not. The acts of the STC 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 from non-performance of their obligations under the law; and
- providing themselves with the necessary technical and technological equipment, etc.

Liability

In respect of public security, the Law on Electronic Documents and Electronic Signatures provides for the liability of the certification service provider to the signature holder and to all third parties for damages from non-fulfillment of the statutory requirements for its activities and duties, caused by:

- untrue data or the absence of required data in the certificate;
- cases where the signatory mentioned in the certificate does not possess the private key corresponding to the public key; and
- damage caused by incompatibility of the data for determination of the use of the private key with the data made available to the user of the public key.

The law provides further liability of the signatory before *bona fide* third parties when, for the generation of the public and private keys, he has used an algorithm that does not fit the statutory requirements.

The signature holder incurs liability to *bona fide* third parties in cases where:

- the signatory does not follow strictly the security requirements 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 its 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, etc.

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.

Security

An electronic signature shall meet certain legislative requirements for technical security in order to be granted legal validity. For a regular electronic signature, the contents of the electronic statement must be protected against subsequent changes. To be granted legal validity as an advanced electronic signature, it is necessary a certificate by certification service provider to have been issued and the e-signature to meet not only the security requirements for a regular electronic signature, but also those concerning the process of "signing"—which shall be done through algorithms providing for the use of the private key of an asymmetrical cryptosystem. The requirements for these algorithms will be determined in a Regulation of the Council of Ministers.

In relation to legal security, Chapter II of the Law on Electronic Documents and Electronic Signatures regulates in detail the requirements, activities, rights and obligations of certification service providers with respect to issuing certificates, providing access to the published certificates to any third person and providing services for the creation of private and public key pair for advanced (and hence universal) electronic signatures. All of these requirements will be spelled out in the implementing regulations.

The law guarantees the protection of personal data collected by certification service providers and prohibits the use of such data apart from the needs of keeping the registry, unless such use is explicitly agreed to by the person in question or it is allowed under a special statutory order. It should be noted that a new Law on the Protection of Personal Data is expected to be adopted. Therefore, at present, it is not possible to predict the nature of future regulations concerning other possible cases for the use of personal data.

Government Regulation

The state body authorized to perform oversight and to regulate the activities of certification service providers in Bulgaria is the State Telecommunications Commission. The STC drafts, coordinates and proposes to the Council of Ministers the adoption of secondary legislation. It supervises and controls the activities of certification service providers in general, the form of the certificates to be issued, the preservation of information on the services provided by certification service providers, etc.

Use Of Electronic Documents And Universal Electronic Signatures By The State And Municipalities

Under the Law on Electronic Documents and Electronic Signatures, state and municipal authorities shall be obliged to accept and issue electronic documents. The exact state authorities shall be determined either by the Council of Ministers, if they are subordinated to it, or by the law, in respect of judicial and other authorities. 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.

Recognition Of Certificates Issued By Foreign Certification Service Providers

With regard to the possibility for recognizing in Bulgaria the legality of certificates issued by foreign certification service providers, the Law on Electronic Documents and Electronic Signatures establishes on the basis of Article 3 (2) of the Directive the legal opportunity for the establishment of organizations for voluntary accreditation.

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 that one of the following requirements is met:

- the obligations of the certification service provider that issued the certificate and the requirements for its activities fulfill the requirements envisaged by the law, and the certification service provider has been recognized in his home country; or
- 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
- 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 STC, 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 fines are introduced. For natural persons, these fines range from BGN100 (US$46) to BGN10,000 (US$4,600), provided that an act does not constitute a crime. Legal entities shall be subject to fines ranging from BGN500 (US$230) to BGN50,000 (US$23,000).