Electronic signatures in Russian law

VICTOR NAUMOV AND TATIANA NIKIFOROVA

With the advent of global information technology, electronic documents are increasingly used in Russian business practice. Individual entrepreneurs and organizations enter transactions by exchanging e-mails, private users subscribe to e-mail services on the internet under contracts they sign electronically; banks introduce customer telebanking systems, and business make payments through electronic payment systems. These examples by no means exhaust the list of all potential uses of electronic documentation. In this context, it becomes necessary to determine the legal status of electronic documents in the system of Russian law.

The Russian Federation Civil Code[1] (Civil Code) addresses the electronic forms of documents on many occasions. A contract is considered to be made in writing if it is effected by the exchange of documents by postal mail, telegraph, teletype, telephone, electronic or other means of telecommunications which permit it to be ascertained that the document comes from the party to the contract.[2] Securities may be issued in a non-documentary form, that is, through electronic and computer technology.[3] The use of electronic digital signatures or other substitutes of handwritten signatures in transactions is permitted where their use is specified either in legislation, such as the Civil Code, but also other laws, such as the Federal Law on the Electronic Digital Signature, the Federal Law On Credit Histories and other statutes, or by agreement between the parties.[4]

A bank's agreement with a customer may provide that the customer's authority to control the money in their account and any electronic money may be proved by other documents using the substitutes of the customer's handwritten signature, such as a PIN, password and other means of providing evidence that the instructions of the customer have been given by the authorized person.[5]

It is important to note that the Russian law only recognizes the electronic digital signature as a legally valid substitute of a person's handwritten signature. Therefore, throughout the text of this article we shall use the terms 'digital signature' or 'electronic signature' meaning an electronic digital signature, namely, a method of encrypting text which allows for the identification of the origin of the text and the protection of the text from unauthorized changes.

The Federal Law on Information, Informatization and Protection of Information, passed in 1995 (Information Law),[6] contains the following definition of a document:

> 'documented information ([or] document) means information fixed on a material carrier [and] containing requisite details permitting it to be identified.' [7]

Under Article 5 of the Information Law, the legal force of a document that is stored, processed or transmitted by means of automated information and a digital signature may validate telecommunication systems. The legal force of a digital signature is recognized if the automated information system has hardware and software that permits the signature to be identified, subject to the observations of operational discipline.[8]

Law did not govern the use of electronic signatures for many years. Nevertheless, the legislation and other statutes of this period (in

[1] Russian Federation Civil Code Part One, No. 51-FZ of November 30, 1994, Part Two No. 14-FZ of January 26, 1996, and Part Three No. 146-FZ of November 26, 2001.
[2] Section 2 of Article 434 of the Civil Code.
[3] Section 1 of Article 149 of the Civil Code.
[4] Section 2 of Article 160 of the Civil Code.
[5] Section 3 of Article 847 of the Civil Code.
[6] Federal Law No. 24-FZ On Information, Informatization and Protection of Information of February 20, 1995, as amended on January 10, 2003.
[7] Article 2 of the Information Law.
[8] Article 5 of the Information Law.

particular, the regulations issued by the Central Bank of Russia)[9] mention electronic signatures. Even the case law from the last decade of the twentieth century occasionally recognized the validity of transactions concluded by way of exchange of documents by means of electronic telecommunications.[10]

The Federal Law on the Electronic Digital Signature

The Federal Law on the Electronic Digital Signature passed in 2002 (Electronic signature Law, or the Law),[11] sets forth the legal framework for the use of electronic signatures in electronic document flows. The Law is based on the following principles:

1. The electronic signature is recognized to be equivalent to the handwritten signature subject to the conditions provided in the Law;
2. The government supervises commerce in products and services involving electronic signatures, by way of certification of electronic signature means; and
3. Information systems are divided into common-use and corporate systems, differing in the degree of government supervision.

Under the Electronic signature Law, the electronic signature forms a part of an electronic document that is intended to protect the document against forgery. It is generated by cryptographic transformation of the information using a private key, permitting the holder of the electronic signature key certificate to be identified, and to ascertain the absence of distortion of information from the electronic document.[12]

The procedure of electronic signing provides that three components must be present: two keys, private and public, and the certificate of the signature key. The Law defines each as follows: [13]

- The private key is a unique series of symbols known only to the holder of the certificate of the signature key;
- The public key is a unique series of symbols corresponding to the private key available to any user of the information system and intended for the verification of the electronic signature in the electronic document; and
- The certificate of the signature key is a hard copy or soft copy document electronically signed by an authorized officer of a certification center, which contains the public key and is issued to the user of the information system to verify the electronic signature and the identity of the signatory.

The certificate must contain, in particular, the period of its validity, the name of the issuing center, the full name or pseudonym of the holder of the certificate, the public key, other details as may be requested by the certificate holder, and the details of transactions in which electronically signed documents will be legally valid.[14] The latter provision does not appear to be entirely clear. The Law expressly states that it applies to relations arising "upon the execution of transactions under civil law and in other cases provided for by the laws of the Russian Federation".[15] This provision of the Law may presumably apply to the type of transaction under civil law as are provided for in the Civil Code. But the reference to "other cases opens" a wide scope of relations including various areas where public and private law apply.[16]

A substantial difference between the Electronic signature Law from a number of its foreign counterparts consists in an attempt to divide all information systems into corporate and common-use systems, and establish a different legal treatment for each system.

Information systems

A common-use information system is understood to be a system open for use by all individuals and legal entities and whose services cannot be denied to such users, while an information system is available to a restricted number of persons, as determined by its owner or by agreement of its users, is recognized to be a corporate information system. In a common-use system, signature keys are made by a user or by the certification center at the user's request. A corporate information system may have a different policy. If a corporate system provides the services of a certification center for common-use system

[9] For example, Provisional Regulations No. 17-P of the Bank of Russia *On the Procedure of Acceptance of Account Holders' Instructions Signed with Substitute of Handwritten Signatures in Making Non-Cash Payments by Credit Organizations* of February 10, 1998.
[10] Ruling No. 5347/98 of the Presidium of the Russian Federation Higher Arbitration Court of June 8, 1999.
[11] Federal Law No. 1-FZ On the *Electronic Digital Signature* of January 10, 2002.
[12] Article 3 of the Electronic signature Law.
[13] Article 3 of the Electronic signature Law.
[14] Article 6 of the Electronic signature Law.
[15] Section 2 of Article 1 of the Electronic signature Law.
[16] Bachilo, I.V., Semiletov, S.I. *A Commentary on the Federal Law* On the Electronic Digital Signature. Konsultant Plus Legal Database.

users, it must meet the requirements set forth for common-use systems.[17] The practical significance of this division is thus not great, for the Law does not provide for wide use of corporate systems.

All operations involved in the use of electronic signatures are performed using special hardware and software, which the Law terms as "the means of the electronic digital signature".[18]

Statutory certification

Applicable laws attach great importance to statutory certification of electronic signature technology. The Law states, for example, that only certified electronic signature technology must be used to create electronic signature keys. Government and municipal authorities may use neither uncertified technology nor keys generated by such technology in their corporate information systems.[19] Therefore, the only type of information systems where uncertified electronic signature technology may be used is unofficial corporate systems. On the other hand, the Law expressly states that an electronic signature may be recognized as equivalent to the handwritten signature only if certified technology has been used to generate it.[20]

Certification of electronic signature technology is a lengthy process in Russia and may require, among other things, decompiling the certifiable software. In the meantime, users often run foreign-made electronic signature technology, the certification of which is impracticable economically or organizationally. It should therefore be admitted that the statutorily required certification of electronic signature technology substantially limits user options offered to electronic document flow agents, and is a serious obstacle to wider use of electronic signatures in Russian business practice.

Until recently, there was another limitation to the expansion of the use of electronic signatures in Russia. Prior to July 2005, issuance of digital signature certificates, registration of digital signatories, provision of related services, and verification of digital signatures were subject to license by the government. In the meantime, there were no statutes which governed the procedure of such licensing. The Law thus did not apply for three years because there was no mechanism for licensing.

Federal Law No. 80-FZ of July 2, 2005 excluded these activities from the list of activities subject to statutory licensing. On the other hand, the requirement of licensing was not taken out from the Electronic signature Law,[21] though it does not apply in light of the recent changes in Russian laws.

Although the licensing of these activities was repealed, the government retained the power to regulate the activities in the sphere of protection of information. For example, activities related to the distribution and maintenance of the means of encryption, provision of encryption services, technical protection of information, and the development and production of protecting the information remains subject to licensing.[22]

Apart from licensing, the government's control over the use of digital signatures exists in other forms. In order to verify digital signature key certificates, the authorized officers of the certifying centers send information system users messages containing such officers' digital signature. Certifying centers must provide the authorized government body with the certificates of the digital signature keys of such persons in hard copies, with the handwritten signatures of such authorized officers verified by the signatures of the centers' directors and their official seals.[23]

At present, the authorized government body is the Federal Agency for Information Technology (FAIT) operating within the Russian Federation Ministry for Information Technology and Telecommunications.[24] FAIT maintains an official register of digital signature key certificates which the certifying centers verify the certificates they issue. The agency provides free access to this register and issued the key certificates of the digital signatures of respective authorized officers of the certifying centers.[25]

The requirement of prior execution of the key certificates of the authorized officers' digital

[17] Section 1 of Article 17 of the Electronic signature Law.
[18] Article 3 of the Electronic signature Law.
[19] Article 5 of the Electronic signature Law.
[20] See the definition of "verification of the electronic digital signature in an electronic document" in Article 3 of the Electronic signature Law.
[21] Article 8 of the Electronic signature Law.
[22] Article 17 of Federal Law No. 128-FZ On Licensing of Certain Activities of August 8, 2001, as amended on March 13, 2002; March 21, 2002; December 9, 2002; January 10, 2003; February 27, 2003; March 11, 2003; March 26, 2003; December 23, 2003; November 2, 2004 and March 21, 2005.
[23] Section 1 of Article 10 of the Electronic signature Law.
[24] Resolution No. 319 of the Russian Federation Government *On Approval of the Regulations of the Federal Agency for Information Technology* of June 30, 2004. The web site of FAIT in Russian is located at http://www.minsvyaz.ru/site.shtml?id=2873. Information in English is only available in regard to the Ministry itself at http://english.minsvyaz.ru/enter.shtml.
[25] The register, in Russian, is available in electronic format at http://www.reestr-pki.ru.

signatures in hard copies, contained in the Electronic signature Law, appears to be redundant in corporate information systems, especially in bank systems, where banks act as the certifying centers.[26] Another flaw of the existing Electronic signature Law is a provision that stipulates that certifying centers may issue the certificates of digital signature keys to the holders only in hard copies executed on the centers' letterheads.[27] This provision rules out the electronic issuance of certificates to the holders even by hand delivery (on diskettes). In order to start using the digital signatures, the holders of the certificates must appear at the certifying center in person or, if they reside in different localities, spend time and money to sign the certificates and have them sent by mail or courier.

■ Foreign digital signature certificates

Foreign digital signature certificates, authenticated under the laws of foreign countries where such certificates are registered, are recognized in the Russian Federation, providing the statutory procedures under Russian law for the recognition of the legal effect of foreign documents have been observed.[28] The effect of a digital signature certificate may be suspended by the certifying center as may be directed by authorized persons or authorities having the power to do so by operation of law or under an agreement, and in corporate information systems, by operation of the policies established for them.[29] Certifying centers resume the effect of suspended certificates also as directed by authorized officials or authorities. If no direction is given to resume the effect of a suspended certificate within a specified period, the certificate must be cancelled.[30] The Law provides for other cases where digital signature key certificates may be cancelled.[31]

■ Liability for certificates

The Electronic signature Law, which sets forth the duties that certifying centers owe to the holders of digital signature key certificates, is silent on the centers' responsibility for the accuracy and validity of the certificates and the centers' liability for damages caused to any individuals, legal entities or organizations which have reasonably relied on such certificates.[32] The only sanction the Law provides is the possibility of placing liability for losses, caused in connection with the generation of digital signature keys using uncertified digital signature technology, on the producers and distributors of such technology. It should also be noted that the Law does not include among the duties which certifying centers owe to digital signature certificate holders, the substantial duty of keeping the private keys secret when the certifying centers generate such keys at the certificate holders' requests.[33]

■ Holders of certificates

Another substantial feature is that, according to the Electronic signature Law, only an individual may hold a digital signature key certificate, which limits the use of digital signatures in transactions between legal entities. The Law provides that where the legal force is given to a document by the signature of an authorized officer and the official seal of the organization, these two requisite details may be substituted by a digital signature under an agreement between the parties and in cases provided for by the laws or other statutes.[34]

In practice, the technical means which generate digital signatures are operated not by the executive officers of companies authorized by their articles of association to sign documents, but other company employees. When such authorized employees resign or are dismissed, it is necessary to follow the entire procedure of obtaining new digital signature certificates. There is a risk of misrepresentation of corporations by their extinguished signatories, who may send out electronic documents signed electronically, after they have ceased to be employed by the corporations.[35]

In practice, the technical means which generate digital signatures are operated not by the executive officers of companies authorized by their articles of association to sign documents, but other company employees

[26] Khalikov, R. *Particular Features of the Subjective Composition in the Use of Electronic Digital Signatures in Banking*, 2005, available in Russian in electronic format at http://www.russianlaw.net/law/doc/a185.htm.
[27] Section 3 of Article 9 of the Electronic signature Law.
[28] Article 18 of the Information Law. For more details of recognition of foreign electronic signature key certificates, see Dmitruk, N. *The Legal Mechanisms of Recognition of Foreign Electronic Signatures.* In: *Informatsionnoe pravo* No. 3 2005, available in Russian in electronic format at http://www.infolaw.ru/lib/2005-3-foreign-electronic signatures.
[29] Section 1 of Article 13 of the Electronic signature Law.
[30] Section 3 of Article 13 of the Electronic signature Law.
[31] Section 1 of Article 14 of the Electronic signature Law.
[32] The obligation to provide such liability is established for the European countries, for example, by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures Official Journal L 013, 19/01/2000 p. 0012 – 0020 available in electronic format at http://www.ict.etsi.org/EESSI/Documents/e-sign-directive.pdf.
[33] Article 11 of the Electronic signature Law.
[34] Article 19 of the Electronic signature Law.
[35] Khalikov, R. *Particular Features of the Subjective Composition in the Use of Electronic Digital Signatures in Banking*, 2005, available in electronic format at http://www.russianlaw.net/law/doc/a185.htm.

Also, the following practice often emerges in relations: a legal entity acts as the owner of the digital signature while its users are authorized individuals. In a case like this, the owner of the digital signature (the chief executive of the legal entity) provides the entity's counterparty (its bank, for example) with a list of authorized digital signatories to electronic documents. This practice is widespread, though it is not permitted legislatively.[36]

Summary

To summarize, it should be noted that the existing legislation in Russia provides that electronic documents can be used and that the digital signature can serve as a requisite identifier. On the other hand, there exist certain flaws that hamper the use of electronic document flow in business practice. Among such flaws there are, in particular, the requirement to use only certified electronic signature technology, the impossibility of using digital signatures to identify legal entities, the requirement to use hard copies in the procedures of issuance of digital signature key certificates, and the absence of provisions for the liability of certifying centers'.

As a result of these flaws, the practice of using digital signature technology by non-government corporate structures is rarely based on observance of the requirements of the Electronic signature Law. In this case, the agents of electronic document flow are denied government support in the application and protection of their electronic documents; specifically, they run the risk of refusal by government authorities and courts to recognize the validity of their electronic documents. It could therefore be concluded that the Electronic signature Law does not entirely protect the interests of the users of non-government corporate information systems.

On the other hand, we should note the increasingly important role of digital signature technology in relations governed by public law. New laws have been adopted where the legislators use the notion of electronic document and electronic signature. For example, the Federal Law On Credit Histories assigns a significant role to electronic document flow in the functions of credit bureaus.[37] Information is supplied to credit bureaus, credit history subjects and credit information users in electronic document form, the legal validity of which is verified by digital signatures in accordance with the laws of the Russian Federation, or by different substitutes of handwritten signatures.[38] Moreover, starting early 2005, a program of introduction of electronic declaration is being implemented by Russian customs authorities.[39]

It should thus be noted that in the area of regulation where the state can mandate observance of the provisions of the Electronic signature Law, specifically, observance of the requirement to use certified digital signature technology, there are good prospects for further use and development of the digital signature tools.

On the other hand, government regulation is not free of odd inconsistencies. It is reported that model rules were adopted in July 2005 for the internal structural organization of the federal executive authorities, together with model policies for interaction between federal executive authorities.[40] These models established the procedure of processing applications from members of the general public only in hard-copy form. Thus another annoying obstacle was put in place to limit the implementation of paper-free document flow in the functioning of public authorities, which, we trust, will be overcome in the near future. ■

Victor Naumov is Head of Intellectual Property Protection Group with DLA Piper Rudnick Gray Cary, St.Petersburg, Russia, an Associate Professor of the St.Petersburg State University and a fellow of the Russian Internet Academy. He practices information law and intellectual property, e-commerce and Internet regulation and other related matters.

victor.naumov@dlapiper.com

Tatiana Nikiforova is an Associate with DLA Piper Rudnick Gray Cary St.Petersburg, Russia and a member of the Intellectual Property and International Technology Group. She has a degree in law from St.Petersburg State University, Russia and an LLM from Oxford University.

tatiana.nikiforova@dlapiper.com
http://www.dlapiper.com

[36] Khalikov, R. *Particular Features of the Subjective Composition in the Use of Electronic Digital Signatures in Banking* available in Russian in electronic format at http://www.russianlaw.net/law/doc/a186.htm.
[37] Federal Law No. 218-FZ *On Credit Histories* of December 30, 2004, as amended on July 21, 2005.
[38] Articles 5 and 6 of the Federal Law On Credit Histories.
[39] Order No. 64 of the Federal Customs Service *On the Decision of the Board of the Collegium of the Federal Customs Service of Russia* On the Program for Development and Introduction in the Customs Authorities of the Russian Federation of the Electronic Form of Declaration of Goods and Vehicles *of December 17, 2004* of January 21, 2005.
[40] See news item by CNews Magazine, October 27, 2005 in Russian at http://www.cnews.ru/news/top/index.shtml?2005/10/27/190727.