

ARTICLE:

# THE USE OF ELECTRONIC DIGITAL SIGNATURES IN BANKING RELATIONSHIPS IN THE RUSSIAN FEDERATION

By **Olga I. Kudryavtseva**

**The amount of cases on claims for damages caused by an unfounded charge-off by a bank has greatly increased in Russia over the past few years. This is because the parties to banking relationships have become used to operate electronic payment systems based on the electronic digital signature, but the security risks associated with the use of an electronic digital signature are not widely understood. In addition, the existing legal framework does not provide enough guarantees for the parties involved in electronic data documentation. This article is focused on the main difficulties that face those that use electronic payment systems in Russia.**

## **The legal basis**

The definition of an electronic digital signature (EDS) is specified in Article 3 of Federal Law No. 1-FZ on Electronic Digital Signature (the Law on EDS):

An electronic document detail intended for protecting the electronic document against forgery, obtained as the result of cryptographic data transformation through the use of the secret key of the electronic digital signature and allowing identification of the owner of a signature key certificate and also making sure no information distortion has occurred in the electronic document

All operations relating to electronic digital signatures are connected to information systems. According to the provisions of Article 2 of the Federal Law of 27 July 2006 N 149-FZ 'On Information, Information Technologies and

the Protection of Information' (the Law on Information), information systems comprise a complex mix of information contained in data bases, information technologies and technical devices providing the processing of the information.

The Law on EDS provides for two types of information systems in Article 3:

'public information system' is an information system open for use by all and any natural persons and juridical persons the services of which cannot be refused to such persons;

'corporate information system' is an information system in which participation is limited to a specific group of people determined by the owner of the information system or by agreement of its participants.

The difference between these two types of systems is clear: the systems of common use are open and intended for use by all natural persons and legal entities, while a corporate system is an information system which may be a distinct circle of persons defined by its owner or by an agreement concluded between the participants of the information system. Owners of an information system are specified in Article 6 of the Law on Information, in that they may be owned by the state and by private individuals or legal entities, and, as an element of property, may be in the ownership of citizens, organs of state power, organs of local self-government, organizations and public bodies.

The type of an information system matters in determining a number of issues, including the order of

*The agreement on participation in the corporate information system usually includes elements of different types of contract.*

the creation of the EDS keys; the issuance and use of the signature key certificates, including the information to be indicated in the certificates, the order of the certificate register keeping, suspension, annulment and keeping of the certificates; the status of the certification center providing the functions of the information system, and the termination of the certification center activities.<sup>1</sup>

All banking services and operations are completed within corporate information systems. As the interaction between the participants of corporate information systems is exercised on the basis of an agreement, the following agreement models are usually used between commercial banks and their clients:

1. The bank and the client conclude an agreement on electronic data documentation. In this agreement, the parties determine the exchange data procedure, terms of use of the EDS, authorization procedure and verification of the document integrity, rules and terms of the keeping the key certificates, dispute resolution procedure, and such like. The contract may cover all legal relations between the bank and the client, or only a determined relationship in respect of specific banking services (for example, on the disposal of money on the client's account).
2. The bank and the client conclude a bank account agreement with a supplement to the agreement regulating use of the 'Bank-Client' system which allows the performance of banking transactions by means of electronic documents.
3. The bank develops a special document - electronic data documentation regulation - which determines all the terms of the data exchange and the application of the electronic digital signature. The regulation is to be found in a public place open for general use (for example, the bank's official

internet site) or in the client's department of the bank. The client expresses his agreement to the terms of the regulation when concluding the agreement. The parties also determine the range of relationships that are covered by the regulation.

The agreement on participation in the corporate information system usually includes elements of different types of contract. It would therefore be regarded as a mixed contract. Concluding such contracts, the parties (especially the banks) ought to consider the authoritative rulings of the High Arbitration Court of the Russian Federation, in particular Article 2 of the Resolution of the Plenum of the High Arbitration Court of the Russian Federation of 19 April 1999 \_ 5 'On Certain Aspects of Practice on Resolution of Disputes on Concluding, Execution and Termination of Bank Account Contracts' which reads as follows:

Unless otherwise provided by the law or a contract, the bank is responsible for the consequences of the execution of an order, where it is initiated by unauthorized persons, even where the bank could not establish the fact of instruction by an unauthorized person using procedures provided by the banking rules and the contract.

### **Electronic digital signatures in practice**

In case N A33-31683/05, a company initiated legal proceeding against its bank, seeking damages caused by an unfounded charge-off in the amount of 519,605.51 roubles, consisting of 423,303.88 roubles of damages and 96,301.63 roubles of penalties. In the period between 27 November 2003 and 28 January 2004, 423,303.88 roubles were written off the client's account by a number of electronic payment orders signed with the electronic digital signature belonging to the general director of the plaintiff. The plaintiff asserted that since 3 October 2003 a new person had unlawfully exercised the powers of the general director of the company under

<sup>1</sup> N. Solovyanenko, 'Commentary on the Federal Law On Electronic Digital Signature', (2003) 5 *Economy and Law* 22.

forged documents that were produced to the bank.

Rejecting the claim, the court observed as follows:

1. Despite the forged documents setting out the status of the new person as a general director that had been produced to the bank, the electronic digital signature of the general director of the company had not been changed by the plaintiff;
2. The plaintiff had not informed the bank of the loss of the electronic digital signature belonging to the general director of the company;
3. The plaintiff had not undertaken other security measures to prevent unlawful use of the general director's electronic digital signature;
4. In accordance with the term of the contract concluded between the parties, the bank (the defendant) is not responsible for the consequences of the execution of the order, given by unauthorized persons in cases when the bank could not establish the fact of instruction by unauthorized persons using procedures provided by the banking rules and the contract. The parties had agreed the bank's limitation of liability under the bank account contract. Under the circumstances, the bank could not establish the fact of instruction by unauthorized person using all available procedures provided by the banking rules and the contract.<sup>2</sup>

The guidelines when using electronic digital signatures in legal relations between commercial banks and the Central Bank of the Russian Federation (RF) is specified in by-laws issued by the Central Bank of the RF, and agreements on electronic document exchange based on these by-laws.<sup>3</sup>

It is important to note that, in accordance with the definition set out in Article 3 of the Law on Electronic

Digital Signature, that the owner of a signature key certificate is a natural person. Some scholars<sup>4</sup> assert that this provision restricts the sphere of the application of electronic digital signatures in the banking sphere. They refer to the Federal Law of 21 November 1996 No. 129-FZ 'On Accountancy', which prescribes that the chief accountant's signature is required on all financial documents of a company otherwise the financial obligations of a company are void. They also refer to paragraph 2.14 of The Ruling of the Central Bank of the Russian Federation No. 2-II of 3 October 2002 'On Written Orders in Russian Federation', which prescribes that payment orders are executed by banks provided these orders bear two signatures (the first and the second) of the persons entitled to sign the payment orders, or one signature (in case there is no person in the staff of a company who is entitled to put the second signature) and under the seal of a company. Taking these requirements into consideration, they suggest that electronic digital signatures should be capable of belonging to legal entities as well as to natural persons.

In the overwhelming majority of cases, companies use only one electronic digital signature of an authorized person when authorizing the payment orders to the bank, and the decisions of judges support this practice, giving preference to the terms of the agreement concluded between the bank and the client. Furthermore, in accordance with the provisions of Article 53 of the Civil Code of the RF, a legal entity acquires its rights and obligations through its agencies acting in accordance with the law, other legal acts and constituent documents.<sup>5</sup> Pursuant to the civil legislature, a chief accountant is not an agency of a legal entity.<sup>6</sup> This means the absence of a chief accountant's signature on the financial documents of a legal entity is not sufficient to consider such documents to be void.

Suggestions to introduce the concept of the corporate electronic digital signature into the legislation is not greatly supported by the majority of scholars, due to the risks of unauthorized use of the EDS and the difficulties

<sup>2</sup> Resolution of the Federal Arbitration Court of East-Siberian Region of 16 August 2006 N A33-31683/05-Φ02-4097/06-C2 (case N A33-31683/05).

<sup>3</sup> Regulations on the Rules of Electronic Documents Exchange between the Bank of the RF, Credit Organizations (Branches) and Other RF Bank's Clients when Performing Payments Through Accounting System of the Bank of the RF as of 12.03.1998 No. 20-II; Letter of the Central Bank of the RF as of 02.06.1998 N 122-T 'On the List of Contractual Terms on the Exchange of Electronic Documents'.

<sup>4</sup> F. Gudkov and O. Ivanov, 'Electronic Document – the Beginning is Started', (2002) 18 EL – Lawyer.

<sup>5</sup> Article 53. The Legal Entity's Bodies

1. The legal entity shall acquire the civil rights and shall assume upon itself the civil duties through its bodies, acting in conformity with the law, with the other legal acts and with the constituent documents. The procedure for the appointment or the election of the legal entity's bodies shall be laid down by the law and by the constituent documents.

2. In the law-stipulated cases, the legal entity shall have the right to acquire the civil rights and to assume upon itself the civil duties through its participants.

3. The person, who by force of the law or of the legal entity's constituent documents comes out on its behalf, shall act in the interests of the legal

entity it represents honestly and wisely. He shall be obliged, upon the demand of the founders (the participants) of the legal entity, to recompense the losses he has inflicted upon the legal entity, unless otherwise stipulated by the law or by the agreement. Translation from <http://www.russian-civil-code.com/>.

<sup>6</sup> There are in the region of ten Federal Laws regulating the status of different types of legal entities (joint-stock companies, limited liability companies, partnerships, institutions). Each law establishes the system of the particular legal entity's agencies. None of the laws provides for a chief accountant to be an agency of a legal entity.

with identifying a specific individual to sign an electronic document.<sup>7</sup> A. V. Shamraev suggests identifying two subjects: the owner of the EDS (the legal entity) and the user of the EDS (an authorized person).<sup>8</sup> In this case, the director of a company should give to the counterparty (for example, the bank) a list of persons authorized to use the EDS when signing documents. R. O. Kchalikov notes that such practice is now wide-spread in Russia, despite it not being directly defined in law.<sup>9</sup>

The peculiarity of using electronic digital signatures in the banking relationship is that the bank, being the owner of the corporate information system, usually functions as a certification center and the user of the key certificate simultaneously. There are occasions when the bank and the client will obtain certification center services from an independent third party. In such cases, the bank and the client conclude an agreement with the certification center according to which the certification center receives electronic documents from the bank's clients, verifies the validity and integrity of the data and identifies the key certificate owner. After completion of these procedures, the electronic documents are sent to the bank.

Pursuant to Article 17 of the Law on EDS, the use of electronic digital signatures in corporate information systems is established by the decision of the owner of the corporate information system or by the agreement between the members of the system. This legal provision provides the members of corporate information systems with ample opportunity to lay down all necessary conditions in the agreement, as is made clear in the provisions of the article:

Article 17. The Uses of Electronic Digital Signatures in a Corporate Information System

1. A corporate information system that provides participants in a public information system the services of the authentication centre of a corporate information system shall meet the qualifications set by the present Federal Law for public information systems.
2. The procedure for using electronic digital signatures in a corporate information system shall be established by the decision of the owner of the

corporate information system or agreement of participants in the system.

3. The content of information in signature key certificates, the procedure for keeping a register of signature key certificates, the procedure for custody of annulled signature key certificates and cases when said certificates lose their legal effect in a corporate information system shall be governed by the decision of the owner of the system or agreement of participants in the corporate information system.

Unfortunately, the Law on EDS does not provide for special rules on the liability of the certification centers. The provisions of Article 8 states:

Article 8. The Status of an Authentication Centre

1. An authentication centre that issues signature key certificates to be used in public information systems shall be a legal entity performing the functions specified in the present Federal Law. Furthermore, the authentication centre shall possess the necessary material and financial capabilities allowing it to bear civil liability to the users of signature key certificates for losses they might incur as a result of unreliability of information contained in the signature key certificates.

The criteria applicable to the material and financial capabilities of authentication centres shall be set by the Government of the Russian Federation on the proposal of the authorised federal executive governmental body.

The status of an authentication centre supporting the operation of a corporate information system shall be defined by its owner or by agreement of the participants in such a system.

2. The activity of an authentication centre shall be subject to licensing under the Russian legislation on licensing specific types of activity.

That the certification center should have at its disposal

<sup>7</sup> K. Leontiev, *Commentary on the Federal Law 'On Electronic Digital Signature'* (Moscow, 2003) 23; A. Sergo 'Electronic Documents Circulation' (2003) 5 *Russian Justice Journal* 70.

<sup>8</sup> A. Shamraev, *Legal Regulation of Information Technologies* (2003) 57.

<sup>9</sup> R. Kchalikov, 'On Peculiarities of Using Electronic Digital Signature in Banking Relationship' (2006) 1

*Legislation.*

enough financial and pecuniary assets to carry the responsibility for any damages caused because of the inaccuracy of information contained in the key certificates is very vague and inaccurate, and when the careless mistakes of banks are added to the equation when concluding agreements, disputes tend to be complex as a result.

### Case law arising out of the use of electronic digital signatures

Most of the disputes arising of the banking relationship in connection with the use of electronic digital signatures are resolved in favour of the bank. This is because it is for the customer to prevent unlawful access to the signature, and the bank is not liable for the charge-off executed against a valid signature. In most of the cases that have been the subject of litigation, it was the bank that supplied the pairs of private and public EDS keys to the customer, generated by the bank with a view of facilitating the installation and use of the electronic digital signature. This leads to the situation that the bank has the technical capability to use the customer's EDS while the customer does not have any legal remedies to defend and to prove the unlawful use of its electronic digital signature.

A typical example is that of case N A40-75611/06-47-564.<sup>10</sup> A company initiated legal proceedings against the bank before the Arbitration Court for the City of Moscow. The plaintiff sought damages caused by an unfounded charge-off in the amount of 62,989,427.44 roubles and 12,337,778 roubles of penalties. The customer (the plaintiff) and the bank (the defendant) concluded a bank account contract dated 28 April 2003. Within the period between 17 January 2005 and 31 August 2005, 62,989,427.44 roubles were written off the client's account by a number of electronic payment orders. All disputed payment orders were received by the bank through the 'Bank-Client' system and signed by a duly authorized person. Meanwhile, in accordance with the provisions to paragraph 1.1 of the contract, the bank carried out equipment and software adjustments and performed all other necessary actions to start up the system.

Dismissing the claim the courts observed as follows:

1. Paragraph 2.2 of the Contract established that a payment order signed with identified electronic signatures and received by the bank from the customer provided the grounds for the bank to

write off the sums from the client's account, in case the digital signature on the payment order has been duly checked (the public key and the private key correspond to each other).

2. Paragraph 3.3.4 of the Contract provides that it is for the customer to provide for the security of the electronic digital signature and defend it from unlawful or unauthorized use, and to inform the bank of any attempt to gain unauthorized access to the system not later than the next day after the disclosure.
3. In accordance with the provisions of paragraph 3.3.5 of the Contract, the customer is obliged to ensure that only persons duly authorized by the customer are permitted to use each electronic digital signature for the purpose of giving instructions to the bank.

However, sometimes a court will award damages to the customer which are caused by an unfounded charge-off by referring to the fact that it was for the bank to prevent unlawful access to the bank electronic payment system. In Resolution of the Federal Arbitration Court of Central Region of 24 December 2007 N A08-10822/05-4, the company initiated litigation against the bank, claiming 5,975,000 roubles of damages caused by improper performance by the bank of the obligations under the contract on rendering the service 'electronic bank'. The terms of the contract provided that the customer was given the opportunity to make payments using electronic payment documents by sending to the bank and receiving from the bank groups of electronic documents through an open data channel. On 22 July 2005, 5,975,000 roubles were written off from the customer's account through the 'Client-Bank' system by sending to the bank on behalf of the customer electronic payment order No. 3358, signed with the EDS belonging to the directors of the customer. The company affirmed that it never instructed the bank to write off the money from its bank account, and that the unlawful actions of third parties became possible due to a deficiency in the service of 'electronic bank' service provided by the bank.

Satisfying the claim, the court observed as follows:

1. Under the parties' agreement, a conciliation commission including representatives of both the

<sup>10</sup> Resolution of the Federal Arbitration Court of Moscow Region of 29 October 2007 N KT-A40/10952-07 (case NA40-75611/06-47-564).

claimant and the defendant was called. The commission ascertained that on 22 July 2005 at 11:57, 9 files, including a file containing disputed payment order N 3358, were sent during the exchange session with the bank. Meanwhile, the payment order was found neither in the system, nor in the program 'BS-Client 3' data base. An excerpt from the customer's bank account as of 22 July 2005 was found, containing information on the charge-off in the sum of 5,975,000 roubles from the company account in the list of excerpts. The 'Client-Bank' system had not informed the customer that the excerpt contains a payment order that is absent in the system, in the list of sent payment orders and in the system data base. The commission also ascertained that the file containing the disputed payment order was found neither among electronic documents given to the bank, nor on the customer's computer hard disc. This fact is also confirmed by the expert opinion performed within the criminal proceedings.

2. The fictitious payment order was given number 3358. However, on this banking day, only payments under payment orders between N 3328 to N 3349 were performed. Authentic payment order N 3358 containing instruction on the transfer of 4,200,000 roubles was sent on 26 June 2005. However, the program installed by the bank had proceeded to issue two payment orders on 22 July 2005 and 26 June 2005 with the same numbers and belonging to the same company.
3. The very transport module of the software 'BS-Client 3' provided by the bank to the customer was described by the experts as the one intended for the transfer of files of any kind (including electronic payment orders) under the system 'Client-Bank', despite of its format and the place of creation, and the program did not generate any information of possible danger connected with the transfer of outside files.
4. According to the expert opinions, the complex software 'BS-Client 3' did not provide the necessary information relating to safety standards preventing the payment information from being distorted, falsified, destroyed, or copying the electronic digital signature.
5. The bank did not produce any evidence of the fact

that the charge-off had been performed through the customer's fault. The bank did not produce evidence of the fact that the customer had not verified the excerpt of its account in a timely fashion.

6. Paragraph 2 of the Resolution of the Plenum of the High Arbitration Court of the RF of 19 April 1999 No. 5 'On Certain Aspects of Practice on Resolution of Disputes on Concluding, Execution and Termination of Bank Account Contracts' provides as follows: 'If otherwise it is not stipulated by the law or the contract, the bank is responsible for the consequences of the execution of the order given by unauthorized persons, even where the bank could not establish the fact of instruction by unauthorized persons using procedures provided by the banking rules and the contract'. In this instance, there was no limitation of the bank liability established in the Contract between the bank and the customer.

### Concluding remarks

This second case is the most interesting, because the court decision contradicts the other court decisions in similar cases. The court awarded the customer damages caused by the unfounded charge-off, because it was for the bank to prevent unlawful access to the bank electronic payment system. In this case, the plaintiff proved the bank failed to fulfill its contractual commitments, and the bank failed to produce enough evidence to demonstrate it was the customer's fault. The significance of such evidence as an expert opinion should also be noted when analyzing such cases. As a rule, the courts refer to the results of the report of an expert performed within criminal proceedings, treating it as written evidence, and do not have a new expert report for arbitration proceedings.

Due to the complexity and long time it takes to bring criminal proceedings to court in such cases, the results of an expert report are not usually known to the arbitration court considering the case, so the case reports do not indicate how people obtained use of the electronic digital signatures. The case reports may occasionally indicate that the money was transferred to third parties. In such cases, the aggrieved party has an opportunity to sue the third parties, referring to the provisions on unjustified enrichment (Article 1102 of the Civil Code of the Russian Federation) unless the unjustified enrichment is repayable under the provisions

of Article 1109 of the Civil Code of the Russian Federation ('Unjustified enrichment which is not to be repayable'). Such claims are commonly satisfied by the courts, but the aggrieved party usually faces the situation when the disputed money has already been transferred to different parties through a succession of payments and, therefore, the recovery becomes much more difficult, if not impossible.

Nonetheless, it should be noted that the legislation currently in force in the Russian Federation provides members of the information systems with the opportunity to assert their rights in court by referring to the payment documents signed with an electronic digital signature. The difficulties which the parties face in protecting the electronic digital signature from unlawful use and the vague provisions of the law, as well as the novelty of the electronic digital signature institution in the Russian Federation, increases the importance of court decisions in eliminating the gaps in the legislation and the collisions of laws.

© Olga I. Kudryavtseva, 2008

*Olga I. Kudryavtseva is the correspondent for the Russian Federation*