THE LAW OF THE REPUBLIC OF ABKHAZIA

On digital signature in the banking system

Chapter I. General provisions

Article 1. The purpose and scope of this Law

1. The purpose of this Law is to provide legal conditions for the use of digital signature in electronic documents, following which the digital signature in electronic documents is considered equivalent to a handwritten signature on a paper document.
2. This law applies to relations arising in the course of banking transactions on the accounts of individuals and legal entities, interbank settlements and other banking services.
   This law does not apply to relations arising when other types of handwritten signature are used.

Article 2. Legal regulation of relations in the field of digital signature

Legal regulation of relations in the field of digital signature in the banking system is carried out in accordance with this Law, other laws, and with normative legal acts adopted in accordance with these laws. It is also implemented by an agreement between the parties.

Article 3. Basic concepts used in this Law

For the purposes of this Law, the following basic concepts are used:

- electronic document – a document in which information is presented in an electronic and digital form;
- digital signature – a detail of an electronic document designed to protect the electronic document from forgery and obtained as a result of cryptographic information conversion by using a private key of digital signature which allows to identify the owner of the signature key certificate and to establish the absence of information distortion in the electronic document;
- owner of the signature key certificate – an individual, in whose name the verification centre issues a signature key certificate and who owns a corresponding private key of digital signature, which allows to create a personal digital signature in electronic documents (to sign electronic documents) using the tools of digital signature;
- tools of digital signature – hardware and (or) software tools, which provide for the implementation of at least one of the following functions – creation of a digital signature in an electronic document by using a private key of digital signature, confirmation of the authenticity of a digital signature in an electronic document by using a public key of digital signature, creation of private and public keys of digital signatures;
- certificate of digital signature – a paper document issued in accordance with the rules of the certification system to confirm the compliance of the tools of digital signature with the established requirements;

- private key of digital signature – a unique sequence of characters known only to the owner of the signature key certificate and designed to create a digital signature in electronic documents using the tools of digital signature;
- public key of digital signature – a unique sequence of characters corresponding to the private key of digital signature, which is accessible to the user of the banking information system and designed to confirm the authenticity of a digital signature in an electronic document by using the tools of digital signature;
- signature key certificate – a paper document or an electronic document with a digital signature of the authorised person of the verification centre, which contains the public key of digital signature and which is issued by the verification centre to the participant in the banking information system to confirm the authenticity of the digital signature and identify the owner of the signature key certificate;
- confirmation of the authenticity of the digital signature in an electronic document – a positive result of verification, by an appropriate certified tool of digital signature and by using the signature key certificate, of the ownership of digital signature in an electronic document by the owner of the signature key certificate and the absence of distortions in an electronic document signed by this digital signature;
- user of signature key certificate – an individual who uses information about the signature key certificate obtained from the verification centre, in order to verify the ownership of a digital signature by the owner of the signature key certificate;
- banking information system – an information system for the use of credit institutions and their clients, the participants in which may include credit and other institutions;
- corporate banking information system – an information system, the participants in which may include a limited circle of credit institutions, determined by the owner of the information system with consent from participants in this information system.

Chapter II. Terms of use of digital signature

Article 4. Conditions for recognising the equivalence of a digital signature and a handwritten signature

1. Digital signature in an electronic document is equivalent to a handwritten signature on a paper document, if the following conditions are met all at once:
   - signature key certificate related to this digital signature has not lost force (is valid) at the time of verification or at the time of signing the electronic document if there is evidence that determines the time of signing;
   - the authenticity of digital signature in an electronic document is confirmed;
   - the digital signature is used in accordance with the information specified in the signature key certificate.

2. A participant in the banking information system may be the owner of any number of signature key certificates at once. Moreover, an electronic document with digital signature has legal significant in the conduct of relations specified in the signature key certificate.

Article 5. The use of digital signature

1. The creation of digital signature keys is for use in:
- banking information system;
- corporate banking information system in the manner established by that system.
2. When creating digital signature keys for use in banking information systems, only certified tools of digital signature should be used. Compensation for losses caused by the creation of digital signature keys by non-certified digital signature tools may be imposed on the creators and distributors of these tools in accordance with the legislation.

Article 6. Signature key certificate

1. The signature key certificate should contain the following information:
   - the unique registration number of the signature key certificate, the start and end date of the validity of the signature key certificate, which is in the register of the verification centre;
   - surname, first name and patronymic of the owner of the signature key certificate or the owner's alias. In case of using an alias, the verification centre shall write an entry about it in the signature key certificate;
   - public key of digital signature
   - the name of digital signature tools with which this public key of digital signature is used;
   - the name and location of the verification centre that issued the signature key certificate;
   - information about the relations in the implementation of which an electronic document with a digital signature will be of legal significance.

2. If necessary, on the basis of supporting documents, the position (with indication of the name and location of the organisation in which this position is established) and qualification of the owner of the signature key certificate is indicated in the signature key certificate, and according to his application in writing – other information supported by corresponding documents.
3. The signature key certificate should be included by the verification centre into the register of signature key certificates not later than the date the signature key certificate becomes valid.
4. To verify whether the digital signature belongs to its owner, the signature key certificate is issued to its users with an indication of the time and date it was issued, information about the validity of the signature key certificate (valid, suspended, terms of suspension, cancelled, time and date of the cancellation of the signature key certificate) and information about the register of signature key certificates. If the signature key certificate is issued as a paper document, this certificate is issued on the letterhead of the verification centre and certified by the personal signature of the authorised person and seal of the verification centre. If the signature key certificate is issued as an

electronic document, this certificate should be signed with a digital signature by the authorised person of the verification centre.

Article 7. The term and procedure for storing the signature key certificate in the verification centre

1. The term and procedure for storing the signature key certificate as an electronic document in the verification centre is defined by a contract between the verification centre and the owner of the signature key certificate. In this case, access to the verification centre is ensured for the participants of the information system to receive the signature key certificate.
2. The term and procedure for storing the signature key certificate as an electronic document in the verification centre after cancellation of the signature key certificate should be no less than the statutory limitation period for the relations specified in the signature key certificate.
   At the end of the specified period, the signature key certificate is deleted from the register of signature key certificates and is transferred to the archive. The archival storage period is not less than five years. The procedure for issuing copies of signature key certificates during this period is established in accordance with the law.
3. A signature key certificate as a paper document is stored in the manner prescribed by the legislation on archives and archiving.

Chapter III. The verification centre

Article 8. Status of the verification centre

1. A state verification centre under the National Bank of the Republic of Abkhazia has been created in the Republic of Abkhazia. It issues signature key certificates to be used in banking information systems. Moreover, the verification centre should possess the necessary material and financial capabilities allowing it to bear civil liability before the users of signature key certificates for losses that may be incurred by them because of unreliable information contained in the signature key certificates.
2. The state verification centre under the National Bank of the Republic of Abkhazia is designed to certify signature key certificates during an exchange of electronic documents in the banking system of the Republic of Abkhazia.
3. The state verification centre under the National Bank of the Republic of Abkhazia keeps a register of digital signature key certificates.

Article 9. The activity of the verification centre

1. The verification centre
   - makes signature key certificates;
   - creates digital signature keys at the request of the information system’s participants with a guarantee of keeping secret the private key of the digital signature;

- suspends and resumes signature key certificates and also cancels them;
- keeps the register of signature key certificates, keeping it updated and freely accessible to the members of the information systems;
- checks the uniqueness of public keys of digital signatures in the register of signature key certificates and the archive of the verification center;
- issues signature key certificates in the form of paper and (or) electronic documents with information about their validity;
- upon users' requests, performs authentication of digital signatures in the electronic document with respect to signature key certificates issued to them.

2. The making of signature key certificates is carried out on the basis of an application of a participant in the information system, which contains information indicated in Article 6 of this Law, necessary for identifying the owner of the signature key certificate and to send him messages. The application is signed personally by the owner of the signature key certificate. The information contained in the application is supported by appropriate documents.
3. When making signature key certificates, the verification centre creates two paper documents containing two copies of signature key certificates, which are certified by handwritten signatures of the owner of the signature key certificate and a stamp of the verification centre. One copy of the signature key certificate is issued to the owner of the signature key certificate, another stays in the verification centre.
4. Services for the issue or cancellation of signature key certificates for the members of the information systems registered by the verification centre, together with information on their work in the form of electronic documents, are rendered free of charge.

Article 10. Obligations of the verification centre in relation to the owners of signature key certificates

When making signature key certificates, the verification centre assumes the following responsibilities in relation to the owners of signature key certificates:

- to include the signature key certificate in the register of signature key certificates;
- to provide for the issue of the signature key certificate at the request of participants in the information systems;
- to suspend the signature key certificate at the request of its owner;
- to notify the owner of the signature key certificate about the facts that became known to the verification centre and which can significantly affect the possibility of further use of the signature key certificate;
- any other obligations determined by normative legal acts and agreements between the parties.

Article 11. Obligations of the owner of the signature key certificate

1. The owner of the signature key certificate shall:

- not use for digital signature the public or private digital signature keys, if he is aware that these keys are being used or have been used before;
- keep secret the private key of digital signature;
- immediately require the suspension of the signature key certificate if there are grounds to believe that the secret of the private key of the digital signature is compromised.

2. In case of non-compliance with the obligations stipulated in this Article, compensation for the losses resulting from this is the responsibility of the owner of the signature key certificate.

Article 12. Suspension of the signature key certificate

1. The validity of the signature key certificate may be suspended by the verification centre on the basis of an indication by persons or bodies having such a right by virtue of a law or contract, and in the corporate information system by virtue of the rules of use established for it.
2. The period between the reception of instructions by the verification centre about the suspension of the validity of the signature key certificate and the entering of the relevant information into the register of signature key certificates should be established in accordance with a rule common to all holders of signature key certificates. Upon agreement between the verification centre and the owner of the signature key certificate, this period may be shortened.
3. The validity of the signature key certificate upon the instruction of the authorised person shall be suspended for a period calculated in days, unless otherwise established by normative legal acts or by an agreement. The verification centre resumes the validity of the signature key certificate as directed by the authorised person. In case there is no instruction to resume the validity of the signature key certificate within the specified period, it is subject to cancellation.
4. In accordance with the instruction of the authorised person to suspend the validity of the signature key certificate, the verification centre informs about this the users of signature key certificates by entering into the register of signature key certificates with an indication of the date, time and the period of suspension of the validity of the signature key certificate. The verification centre also informs about this the owner of the signature key certificate and the authorised person from whom the instruction was received to suspend the validity of the signature key certificate.

Article 13. Cancellation of the signature key certificate

1. The verification centre that issued the signature key certificate shall cancel it:
   - upon expiry of its validity period;
   - with the loss of legal force of the certificate of the corresponding tools of digital signature used in the public information systems;

- if the verification centre came to know for certain that the validity of the document, on the basis of which the signature key certificate was issued, has expired;
- upon application in writing of the owner of the signature key certificate;
- in other cases established by normative legal acts or an agreement between the parties.

2. If the signature key certificate is cancelled, the verification centre informs about this the users of signature key certificates by entering into the register of signature key certificates of an appropriate information with an indication of the date and time of the cancellation of the signature key certificate, with the exception of cases where the signature key certificate is canceled after the expiration of its validity period, and also informs about this the owner of the signature key certificate and the authorised person (body) from whom the instruction was received to cancel the signature key certificate.

Chapter IV. Features of use of digital signature

Article 14. The use of digital signature in a corporate information system

1. The manner of use of digital signature in a corporate banking information system is determined by the decision of the owner of the corporate information system or by an agreement between the participants in this system.
2. The cases when the abovementioned certificates lose legal force in the corporate banking information system are determined by the owner of that system or by an agreement of the participants in the corporate banking information system.

Article 15. Recognition of a foreign signature key certificate

A foreign signature key certificate, certified in accordance with the legislation of a foreign state in which this signature key certificate is registered, is recognised on the territory of the Republic of Abkhazia in case of compliance with the procedures established by law for recognising the legal significance of foreign documents.

Article 16. Cases of substitution of seals

1. The contents of a paper document, certified by a seal and changed into an electronic document, may be certified by a digital signature of the authorised person in accordance with normative legal acts and an agreement between the parties.
2. In cases established by law and other normative legal acts or an agreement between the parties, a digital signature in an electronic document, the certificate of which contains the information about the powers of its owner, which is necessary to implement these relations, is recognised as equivalent to a handwritten signature of a person in a paper document certified by a seal.

Chapter V. Final and transitional provisions

Article 17. The bringing of normative legal acts into conformity with this Act

1. Normative legal acts of the Republic of Abkhazia shall be brought into conformity with this Law within three months from the date of entry into force of this Law.

Adopted by the National Assembly –

Parliament of the Republic of Abkhazia

on July 28, 2006

PRESIDENT S. BAGAPSH

OF THE REPUBLIC OF ABKHAZIA

Sukhum

August 2, 2006

No. 1442-c-XIV