Law

No. 9880, dated 25.02.2008, amended by the Normative Act no. 8, dated 30.09.2009

On Electronic Signature

Pursuant to articles 78 and 83 point 1 of the Constitution, upon proposal of the Council of Ministers

ASSEMBLY
OF THE REPUBLIC OF ALBANIA

DECIDED:

CHAPTER I

GENERAL PROVISIONS, DEFINITIONS

ARTICLE 1
Purpose

The purpose of this Law is to create the necessary conditions for the application and use of electronic signatures in Albania.

ARTICLE 2
Use of electronic signature

1. The use of electronic signatures is voluntary unless otherwise specified by law.

2. Legal provisions may require compliance with additional conditions for the use of qualified electronic signatures for public administrative activities.

ARTICLE 3
Definitions

For the purposes of this Law,

1. *"Electronic signatures"* shall mean all data in electronic form attached to other electronic data or logically linked to the data and used for authentication and the integrity of the signed document;

2. *"Advanced electronic signatures"* shall be electronic signatures which:

a) are exclusively assigned to the specific owner of the signature code;

b) enable the identification of the owner of the signature code;

c) are produced with secure means which the owner of the signature code can keep under his sole and exclusive control, and

d) are linked to the data in such a manner that enables any subsequent alteration of the data to be easily detected;

3. *"Qualified electronic signatures"* shall be electronic signatures which:

a) are based on a qqualified certificate that is valid at the time of the creation of the signature; and

b) have been produced with a secure device for the creation of signatures;

4. "*Signature codes"* shall be unique electronic data such as private cryptographic codes or algorithms that are used to create an electronic signature.

5. *"Signature test codes"* shall be any electronic data such as public cryptographic codes or algorithms that are used to test and verify an electronic signature.

6. "*Certificates*" shall mean electronic certificates assigning signature test codes to a person and confirming his or her identity.

7. "*Qualified certificates*" shall be certificates for natural persons that fulfill the requirements in article 12 and are issued by certification service providers which meet at least the requirements pursuant to articles 9 to 19 or article 23 of this Law and bylaws pursuant to article 24 that are based on this Law.

CHAPTER II

LEGAL VALIDITY OF THE ELECTRONIC SIGNATURES, EXCEPTIONS

ARTICLE 4
Legal validity of electronic signatures

A legal action which has to be made through a written document and a handwritten signature can also be made by an electronic document in conjunction with a qualified electronic signature. The electronic document, which bears the signatory's name and his qualified electronic signature, has the same legal validity as the simple written form.

ARTICLE 5
Electronically signed contract

If the legal action is a contract then each of the parties has to sign the same document with each respective qualified electronic signature.

ARTICLE 6
Waiver of rights

The parties can agree to waive of the rights granted in this chapter.

ARTICLE 7
Exceptions

The electronic signature will not have any effect in the following cases:

1. legal action in the area of family law and law of legacy, which are subjected to special legal requirements;
2. other legal actions which require the public legalization, a written notarized act or official confirmation by a court;
3. legal actions that refer to assets as a guarantee of bail ; and
4. always when the law does not allow the use of electronic signature.

ARTICLE 8
Authenticity of document's content

If a document is signed with a valid electronic signature it is deemed that the content of the document is true and has not been modified.

ARTICLE 9
Invalidity of electronic signatures

The electronic signatures are considered invalid if it can be proven that the security requirements of this Law or bylaws have not been met.

CHAPTER III

COMPETENT AUTHORITY, REGISTRATION, SUPERVISION

ARTICLE 10
National Authority for Electronic Certification

1. The National Authority for Electronic Certification, hereafter the Authority is the institution that supervises the enforcement of this Law and bylaws issued to its pursuance;
2. Authority shall be the central public institution, of legal character, *dependent on the respective minister, specified by the Decision of Council of Ministers*[(1)]*;*
3. The Authority's residency shall be Tirana;
4. The Authority shall be financed by the State's budget and from revenues derived from its activity;
5. Pursuant to this law and bylaws the Authority has the full integrity to enforce its law and other provisions;
6. The Director of Authority is assigned by the minister and operates by the procedures provided in law nr.8549, date 11.11.1999, "Status of Civil Servants ";

(1) Normative Act Nr. 8, dated 30.09.2009, for an amendment of Law no. 9880, dated 25.02.2008, "For Electronic Signature"

7. The employees of the Authority shall enjoy the status of civil servants. Working relations for authority employees, which cover supporting duties shall be regulated by labor law; and

8. The structure of the Authority shall be approved by Prime Minister after the Minster proposal. The Ordinance on functioning of the Authority shall be approved by Minister.

ARTICLE 11
Registry of Certification Service Providers

The authority shall register the names of the certification service providers and of the certification service providers that have ceased to operate pursuant to article 13 and 46 of this law. This register is updated and published online.

ARTICLE 12
Supervision

The Authority may conclude agreements with public or private entities to perform the supervision. In all cases, the activity should be related to particular duties or activities that cannot be performed by Authority.

ARTICLE 13
Interruption of the Service Provider activity

The Authority shall interrupt a certification service provider to operate temporarily, entirely or partly in cases when it:

a) has not the reliability necessary to operate as certification service provider;

b) has not the specialized knowledge necessary for its operations, pursuant to article 19 of this law;

c) has not the necessary financial guarantee, pursuant to article 19 of this law;

d) is using unsuitable products for electronic signatures;

e) does not fulfill the other conditions to operate as certification service provider pursuant to this Law and bylaws.

ARTICLE 14
Invalidation of qualified certificates by the Authority

1. The Authority may order qualified certificates to be invalidated if:

a) forged or are not sufficiently secure against forgery; and

b) secure signature-creation devices of the electronic signature have security defects that would enable qualified electronic signatures or data related to this signature to be forged without detection.

2. The Authority verifies the invalidity of qualified certificates, which are forged.

3. The invalidation procedures and information of third parties are regulated by other bylaws issued to pursuance of this law.

ARTICLE 15
Validity of qualified certificates

The validity of qualified certificates issued by a certification service provider shall not be impaired by measures taken against the service provider, pursuant to article 13 of this law.

ARTICLE 16
Inspection and information

1. The Authority, while exercising its rights, reserves the right to inspect or request information from the certificate service providers periodically or anytime that it judges as necessary.

2. The Authority inspects or requests information anytime when:

a) it has information on violation of provisions of the Law or other relevant bylaws;

b) it submits complaints from certificate applicants or certificate holders.

ARTICLE 17
Cooperation

1. Certification service providers and the third parties working for them shall permit the Authority and persons operating on its behalf to enter their premises, during normal working hours, with no prior notice.

2. Certificate service provider and third parties working for them are obliged to provide information and the necessary support making available all the paperwork's and electronic documentation.

3. To exercise its rights pursuant to this law, when appropriate, the Authority shall be supported by central, local public authorities and the police forces.

CHAPTER IV CERTIFICATION SERVICE PROVIDERS

ARTICLE 18
Certification service provider's operation

The certification service provider does not require prior approval to begin its operation.

ARTICLE 19
Requirements for operation

1. The Certificate service provider can be any legal or natural person who can prove that he:

a. has the necessary reliability and specialized knowledge to operate as a certification service providers;

b. has the necessary financial guarantees to cover damages, pursuant to article 41 of this Law.

2. The requirements and criteria that a certification service provider has to meet, including those pursuant to article 1 of this Law, are to be specified by other bylaws in pursuance of this law.

ARTICLE 20
Registration of certification service activity

Anyone commencing to operate a certification service shall report this to the competent authority once it starts the operation. During the registration, the service provider shall submit the necessary evidences proving that all conditions under article 19 of this law have been met.

ARTICLE 21
Reporting on lack of ability to meet the criteria

The Certification service provider has to ensure that criteria pursuant to article 19 of this Law are fulfilled throughout the entire duration of his operation. Circumstances that render this impossible must be reported to the Authority immediately.

ARTICLE 22
Transferring the tasks of certification services

The certification service provider may transfer the tasks, pursuant to this Law and bylaws, to third parties if they fulfill conditions specified pursuant to article 19 of this Law. The transfer does not exclude the service provider from any legal responsibilities.

ARTICLE 23
Periodical report

Every Service Provider must submit an annual detailed report of its operations to the Authority no later than the 31st march of the following year. The structure and content of this report is specified by the Authority.

CHAPTER V

ISSUANCE OF QUALIFIED CERTIFICATES

ARTICLE 24
Identification of the applicant of qualified certificate

1. The certification service provider shall, reliably identify any person who applies for a qualified certificate, and upon consent of the applicant shall be entitled to use the personal data collected, to guarantee reliably the identity of the applicant pursuant to this article.

2. The Certification-service provider shall confirm the assignment of a signature-test code to an identified person with a qualified certificate, ensuring that this can be verifiable electronically by anyone using public electronic links.

ARTICLE 25
Data contained in the qualified certificate requested by the applicant

1. If requested by an applicant, a qualified certificate may contain data on his authorization to act for a third party, occupational or other data on individual attributes.

2. Data on the authorization to act for a third party may only be included if proof of this party's approval is given; occupational or other data on the person must be confirmed by the offices responsible for occupational or other data.

3. Other personal data may only be included in a qualified certificate with the approval of the person concerned.

ARTICLE 26
Use of pseudonym

1. If requested by the applicant the certification-service provider shall use a pseudonym instead of his name in the qualified certificate.

2. According to article 25, pseudonym can be used for the data of qualified certificate, but the approval of the third party or the responsible office is required.

ARTICLE 27
Data protection from fraud and assurance of the secrecy of codes

1. The certification service provider shall make arrangements to ensure that data contained in the qualified certificates cannot be forged without being detected.

2. The certification service provider shall ensure that the signature codes are kept completely secret. Signature codes may not be stored outside the secure signature creation device and shall not be accessible directly by the applicant.

ARTICLE 28
Personnel and products credibility

For the purposes of certified qualified electronic signatures, the certification service provider shall employ credible personnel and products that meet the requirements pursuant to this Law. Other legal provisions shall specify the security criteria for the personnel and devices.

ARTICLE 29

Secure signature creation device

The certification service provider shall obtain suitable proof that the applicant owns the relevant secure signature creation device.

ARTICLE 30
Information obligations on security measures

1. The certification service provider shall inform the applicant on the measures needed to increase the security of a qualified electronic signature, and test them reliably.

2. The certification service provider shall inform the applicant that data contained on a qualified electronic signature may need to be signed again if the security of the current signature is reduced with the passing of time.

ARTICLE 31
Information obligations on legal validity

The certification service provider shall inform the applicant that a qualified electronic signature has the same effect in legal actions as a handwritten signature unless otherwise specified by article 7 of this Law.

ARTICLE 32
Information in written form

To fulfill the information obligations pursuant to articles 30 and 31, the applicant shall be given a written information sheet, acknowledgement of which shall be confirmed by signing, in order to be issued a qualified certificate.

ARTICLE 33
Contents of qualified certificates

A qualified certificate shall bear a qualified electronic signature and contain the following data:

a) name of the signature-code owner; a supplement shall be added to the name if there is a possibility of confusion with another name, or an unmistakable pseudonym assigned to the signature-code owner so he can be recognized as such;

b) assigned signature-test code;

c) designation of the algorithms with which the signature-test code of the signature-code owner and the signature-test code of the certification service provider may be used;

ç) current serial number of the certificate;

d) commencement and termination of its validity;

dh)name of the certification service provider and the country in which he is domiciled;

e) information on whether the use of the signature code is limited to certain applications by nature or extent;

ë) Information that the certificate is a qualified one; and

f) If necessary, special attributes of the signature-code owner.

ARTICLE 34
Special attributes

1. Special Attributes may also be included in a separate qualified certificate (qualified certificate with special attributes).

2. In a qualified certificate with special attributes, the data provided for in article 33 of this Law may be replaced, referring clearly to qualified certificate's data from which it refers, in case that the use of the qualified certificate with special attributes is not needed.

ARTICLE 35
Invalidation of qualified certificates

1. The certification-service provider shall invalidate a qualified certificate immediately:

a) if a signature-code owner or his representative so demands,

b) if the certificate was issued on the basis of false data other than those specified pursuant to article 33 of this Law,

c) if the certification service provider has ceased to operate and the operation is not being continued by another certification service provider;

ç) if the competent authority orders the certificate invalidated in accordance with article 14 of this Law.;

2. Further reasons for invalidation can be specified in contracts between parts, including cases provided in nos.1 of this article.

3. The invalidation must state the time from which it applies.

4. Invalidation does not have backdated effect.

ARTICLE 36
Revocation on behalf of the code-owner

The certification-service provider must provide a non-stop certificate revocation service, which is operated so that authorized revocations can be executed immediately, at any time it is requested.

ARTICLE 37
Invalidation of certificate after special conditions on attributes cease to apply

If a qualified certificate contains data pursuant to article 25 of this Law, the third party or the office responsible for the occupational or other data on the person may demand invalidation of the certificate in question, if the conditions for the occupational or other data on the person cease to apply after being included in the qualified certificate.

ARTICLE 38
Issuance of qualified time stamps

The issuance of qualified time stamps by a certification service provider shall meet the same requirements as specified pursuant to article 28 of this Law.

ARTICLE 39
Documentation of the security measures and qualified certificates

1. The certification service provider shall document all security measures taken in order to meet the requirements specified in this Law and bylaws as well as document the qualified certificates issued so that the data and their correctness can be confirmed at any time.

2. The documentation shall be made without delay and in such a manner that it cannot subsequently be altered without detection. This shall particularly apply to the issuance and invalidation of qualified certificates.

ARTICLE 40
Right of information on the data stored by the service provider

Upon request, the signature-code owner shall be given access to the data and the procedural steps concerning him which are stored from the certification service provider.

CHAPTER VI

Liability

ARTICLE 41
Reimbursement

1. A certification service provider shall reimburse a third party for any damage caused from relying on the data in a qualified certificate or a qualified time stamp or on any information given in accordance with Article 24 of this law when:

a) he infringes the requirements pursuant to this Law and bylaws;

b) his products for qualified electronic signatures or other technical security services fail to operate properly.

2. Damages shall not be payable, if the third party had prior knowledge on the causes pursuant to point 1 of this article.

ARTICLE 42
Exclusion from payment obligations

The certification service provider is excluded from obligation of reimbursement if he proves to be innocent in his actions.

ARTICLE 43
Restrictions on damage reimbursement

If a qualified certificate restricts the use of the signature code to certain applications by type or extent, damages shall be payable only within the limits of these restrictions.

ARTICLE 44
Liability in the cases of transfer of tasks

The certification service provider shall be liable for transfer of obligation to offer services, pursuant to article 22 of the Law.

ARTICLE 45
Assets Guarantees

The certification service provider shall be obliged to take appropriate financial measures to ensure that it can meet its statutory obligations for reimbursement of damages caused by:

a) Infringement of the requirements of the Law and bylaws.

b) Lack of proper function of his products for qualified electronic signatures or other technical security services.

ARTICLE 46
Actions after cessation of certification service of certification service providers

1. A certification service provider has to report the cessation of its operation immediately to the competent authority.

2. In the possible case of cessation:

a) It has to invalidate all valid certificates.

b) or has to take care that the valid certificates will be taken over by another certification-service provider. It has to support the succeeding certification service provider in the best way possible and provide it with all the necessary data.

c) It shall inform the signature-code owners concerned that it will be ceasing operations and that the certificates are being taken over by another certification service provider.

3. Even in the case of the cessation of operations, the certification service provider has to continue the revocation services. If it is not able to fulfill this it has to report this fact to the competent authority, which will then take care of the respective revocation services.

CHAPTER VII

PROTECTION OF PERSONAL DATA

ARTICLE 47
Data usage

1. The certification-service provider shall only use the personal data that is necessary to fulfill the certification services and only insofar as it is necessary for the purposes of issuing and maintaining the certificate.

2. This data shall only be obtained from the person directly. Obtaining personal data from a third party shall only be permitted with the consent of the person concerned.

ARTICLE 48
Data handover

1. The certification-service provider shall hand the data on the identity of a signature-code owner to the competent authority upon request:

a) where this is necessary for the prosecution of criminal acts or infringement of regulations, and in the case when investigative institutions require the above;

b) to avoid risk to national security or order;

c) to fulfill the tasks legally required of the government, customs, military defense or the fiscal authorities;

ç) after a court order.

2. The Authority after asking for information, shall inform the signature code owner whose pseudonym has been revealed as long as this will not restrict the performance of its legal duties, or if the interests of the signature code owner for information outweigh the other reasons.

CHAPTER VIII

TECHNICAL SECURITY

ARTICLE 49
Security of signature creation devices

1. To store signature codes and to produce qualified electronic signatures, secure signature-creation devices shall be used that will reliably identify forged signatures and false signed data and offer protection against unauthorized use of the signature codes.

2. If the signature codes are themselves produced on a secure signature-creation device, the requirements of article 51 of this Law shall be applied

ARTICLE 50
Components of signature application

1. The presentation of data to be signed requires signature-application components that will clearly indicate the production of a qualified electronic signature and enable the data to which the signature refers to be identified.

2. To check signed data, signature-application components are needed which will show:

a) which data the signature refers to,

b) whether the signed data are unchanged,

c) which signature-code owner the signature is to be assigned to,

ç) contents of the qualified certificate on which the signature is based, and of the appropriate qualified attribute certificates, and

d) results of the subsequent check of certificates pursuant to article 24.2

3. Signature-application components also shall, if necessary, make the contents of the data to be signed or already signed sufficiently evident.

4. The signature-code owners should use these signature application components or take other suitable steps to secure qualified electronic signatures.

ARTICLE 51
Technical components for certification services

The technical components for certification services shall contain provisions to:

1. Ensure that signature codes produced and transferred are unique and secret and exclude storage outside the secure signature-creation device;

2. Protect qualified certificates that are available to be tested or downloaded in accordance with article 24.1 from unauthorized alteration and unauthorized downloading, and

3. Exclude the possibility of forgery and falsification in the production of qualified time stamps.

ARTICLE 52
Testing and confirmation body

1. Any legal or natural person who, by his request, is recognized as the Testing and Confirmation Body by the National Authority for Electronic Signatures, only if it can prove it has the reliability, independence, and specialized knowledge needed to exercise these functions.

2. The recognition may be:

a) limited in content,

b) be given for a limited period of time;

c) conditions may also be attached.

3. The Testing and Confirmation Body shall perform their tasks impartially, free of instruction, and conscientiously.

4. They shall document the tests and confirmations and hand over this documentation to the competent authority if they cease to operate.

5. Bylaws and other legal provisions shall specify the conditions, criteria and obligations pursuant to which the Testing and Confirmation Body must operate.

ARTICLE 53
Fulfillment of legal requirements

1. Confirmation on legal requirements, pursuant to articles 49, 50, 51 of this Law and bylaws, shall come from the Testing and Confirmation Body.
2. The manufacturer shall at the time of launching the product on the market at the latest, deposit a copy of his declaration in writing with the competent authority.
3. Declarations of manufacturers which comply with the requirements of the Law and other provisions on electronic signatures shall be made available to the public.

ARTICLE 54
Acceptance and use of foreign products and electronic signatures

1. Electronic signature and foreign products of electronic signatures are recognized and applied in conformity with agreements concluded by the Republic of Albania and foreign states for their acceptance and exchange of data
2. Procedures on establishing the security level for foreign electronic signatures and foreign products are regulated by other bylaws.

CHAPTER IX

COSTS AND FEES

ARTICLE 55
Fees

With the proposal of the respective Minister, the Council of Ministers shall approve the measures and the types of fees to be paid to the Authority, by the certification service provider or other subjects that are liable according to this law. Fees cannot be higher than the costs of service conducted by the Authority.

CHAPTER X ADMINISTRATIVE

MEASURES

ARTICLE 56
Violations

The following violations, whenever they do not constitute a penal offence, they constitute an administrative offence and shall be punishable to fines as follows:
1. With a 2.000.000 (Lek) whenever:

a) The service provider does not report immediately on beginning of operations, pursuant to article 20.

b) The correct identification of the applicant is not performed, pursuant to point 1, of article 24.

c) The requests, pursuant to point 2, article 25, for taking the necessary evidences proving the authorization to act for a third party, are not executed.

ç) the service provider acts without prior approval of a third party, pursuant to point 2, article 26.

d) The service provider does not undertake the necessary actions after the cessation of activity, pursuant to article 46.

2. With a 1.000.000 (Lek) fine whenever:

a) The certification service is offered in contradiction with what is specified pursuant to article 19.

b) The security measures are not implemented as required pursuant to article 27.

c) The documentation is not compiled pursuant to article 39.

ç) The service provider does not collaborate with the Authority, as required pursuant to articles 17 and 48.

ARTICLE 57
Other Sanctions

Regardless of the sanctions defined pursuant to article 56, and the circumstances specified in article 13, whenever the Authority reasonably considers that violations are to the extent that impair the integrity and credibility of the service provider, temporarily suspends the activity of the service provider, entirely or partially.

ARTICLE 58
Complaints and execution

1. The complaints, against the decision to penalize by fine or suspension of the activity, must be submitted to the Minister, not later than 10 days from the date of its imposition.

2. The Minister shall take a decision within 30 day period of time. Against this decision a complaint shall be made within 30 days following its proclamation or the notification from the court.

3. The processing of the administrative infringements, complaints and the execution of decisions are performed in accordance with the law: “On administrative violations”. The fine is an executive title, which is collected by the Authority and deposited with the State’s Budget.

CHAPTER XI FINAL

PROVISIONS

ARTICLE 59
Bylaws

The Council of Ministers shall be charged with issuance of bylaws pursuant to articles 14, 19, 28, 52, 54 and 55 of this Law.

ARTICLE 60
Entry into force

This law shall enter into force 15 days after being published in the Official Journal.

Announced by decree nr. 5655, dated 11.03.2008 of the President of the Republic of Albania, Bamir Topi.