LAW

ON ELECTRONIC SIGNATURE

(Official Gazette of the Republic of Montenegro 55/03 and 31/05)

I GENERAL PROVISIONS

Article 1

This Law shall regulate the use of electronic signature in legal transactions, administrative, judicial and other proceedings, as well as rights, duties and liabilities of legal and natural persons related to electronic certificates, unless otherwise provided by special law.

Article 2

Certain terms used in this Law shall have the following definitions:

Electronic document - the document in electronic form that is used in legal transactions, administrative, judicial and other proceedings, and includes all forms of written and other text, data, images, drawings, charts, sound, music, speech, computer databases, etc;

Electronic signature - a set of data in electronic form that are attached to or logically associated with the electronic document and serve to identify the signatory;

Advanced electronic signature - electronic signature that reliably guarantees the identity of the signatory and the integrity of electronic documents and fulfils the conditions laid down by this Law;

Signatory - a person who has the means to create an electronic signature that is used to sign in his/her own name or on behalf of a natural or legal person that he/she is representing;

Data for creation of electronic signature - unique data, such as codes or private cryptographic keys used by a signatory for creation of electronic signature;

Means for creation of electronic signature - the appropriate computer equipment or computer program that signatory uses during creation of electronic signature, using data for creation of electronic signature;

Means for creation of advanced electronic signature - means for creation of electronic signature that fulfil the conditions laid down by this Law;

Data for verification of electronic signature - information such as codes or public cryptographic keys used for verification of electronic signature;

Means for verification of electronic signature - the appropriate computer equipment or programs that are used for verification of electronic signature;

Means for verification of advanced electronic signature - means for verification of electronic signatures that fulfil the conditions laid down by this Law;

Certificate - a certificate in electronic form, which connects the data for verification of electronic signature to a person and confirms the identity of that person;

Qualified certificate - a certificate that contains information provided for in this Law and that is issued by provider of services related to qualified certificates issuance;

Certification service provider - legal or natural person (entrepreneur), who issues certificates or provides other services related to electronic signature.

II ELECTRONIC DOCUMENT, ELECTRONIC SIGNATURE AND ADVANCED ELECTRONIC SIGNATURE

Article 3

The admission of an electronic document with electronic signature or advanced electronic signature may not be rejected only because it is in electronic form.

Provision of paragraph 1 of this Article shall not apply to:

1) Legal affairs that transfer immovable property rights or constitute other real rights on immovable property;
2) Probate processes;
3) Contracts regulating property relations between married or not married couples;
4) Contracts on the disposal of property of persons who have been deprived of ability to work;
5) Contracts on the assignment and allocation of lifetime property;
6) Contracts on the lifelong care and agreements relating to inheritance;
7) Gift contracts;
8) Other legal matters for which a special law expressly stipulates the use of manu propria signature in documents on paper or certified manu propria signature.

Article 4

If the law or other regulations stipulate that the document should be saved, it may be done in an electronic mode, provided that the electronic document is:

1) Accessible and available within the period established for its keeping;
2) Kept in the same form in which it was made or received;
3) Kept in a manner that allows identification of time and place of its origin or reception and person who has made it;
4) Kept by applying technologies and procedures that provide reliable method for detection of any amendment to the electronic document.

Obligation of keeping the document referred to in paragraph 1 of this Article shall not apply to communication or other data, which only objective is to enable sending or receiving of the electronic document.

Article 5

Persons, who keep electronic documents that are electronically signed, shall keep data and means for verification of electronic signature as long as these documents are kept.

Article 6

Electronic signature's validity may not be denied, nor may be rejected as the evidence solely because:

1) It is in electronic form;
2) It is not based on a qualified certificate;
3) It is not based on a qualified certificate issued by an accredited certification service provider;
4) It is not created by means for creation of advanced electronic signature.

Article 7

Advanced electronic signature, which can be verified on the basis of a qualified certificate, in relation to data in electronic form:

- Has the same legal force as manu propria signature, i.e. manu propria signature and stamp in relation to data in paper form;
- Is acceptable as evidence in legal affairs.

Article 8

Advanced electronic signature must:

1) Be exclusively associated with the signatory;
2) Clearly identify the signatory;
3) Be created using means that a signatory can manage independently and that are exclusively under his supervision;
4) Contain direct correlation with the data to which it refers in a manner that unambiguously provides an insight to any amendment to the original data.

Article 9

Electronic signature is made using means for electronic signature creation.

Advanced electronic signature is made using means for advanced electronic signature creation.

Article 10

Means for creation of advanced electronic signature must ensure that:

1) Data for creation of advanced electronic signature appear only once and that their safety is achieved;

2) From data for verification of advanced electronic signature, during validity period of certificate, data for formation of advanced electronic signature cannot be obtained with currently available means;

3) Advanced electronic signature is protected from forging using currently available technology;

4) Signatory may reliably protect data for creation of advanced electronic signature from unauthorised use.

Means for creation of advanced electronic signature shall not, during creation of advanced electronic signature, change the data that shall be signed or preclude the signatory to have an insight to the data before advanced electronic signature creation process.

Article 11

Means for verification of advanced electronic signature are means that provide:

1) Reliable determining that data used for verification of electronic signature correspond to data presented to a person who carries out verification;

2) Reliable verification of signature and correct displaying of the verification results;

3) Reliable insight into the content of signed data;

4) Reliable verification of authenticity and validity of signatory's certificate at the moment of signature verification;

5) Correct displaying of signatory's identity;

6) That any amendment to signed data can be reliably identified.

Article 12

Provisions of Article 3, paragraph 1 of this Law shall apply only when the protection of electronic signature and advanced electronic signature as well as verification of signatory's identity are carried out using existing technology by the signatory, or certification service provider.

Republic administration authority competent for information technology affairs (hereinafter referred to as "the competent administration authority"), shall regulate:

1) Electronic signature and advanced electronic signature protection measures;

2) Signatory's identity verification measures that shall be taken in accordance with paragraph 1 of this Article;

3) Technical-technological procedures for creation of advanced electronic signature;

4) Conditions that means for creation of advanced electronic signature shall fulfil.

III CERTIFICATES AND PROVISION OF CERTIFICATION SERVICE

Article 13

Qualified certificate must contain:

1) Label that it is a qualified certificate;
2) Identification data set on the person who issued the certificate;
3) Identification data set on the signatory;
4) Data for verification of electronic signatures that correspond to the data for creation of electronic signature and which are under control of the signatory;
5) Data on the validity period of the certificate;
6) Identification label of issued certificate;
7) Advanced electronic signature of provider of qualified certificates issuance services;
8) Restrictions related to the use of certificate, if any;
9) Restrictions related to the value of business events for which the certificate has been issued, if any.

Article 14

Certification service provider may perform certification service, if he has:

1) Established work organisation that guarantees the quality of providing certification service;
2) Financial and material resources that are sufficient for unobstructed provision of certification service, regardless of the number of service users and during the entire time of service provision;
3) Qualified personnel for carrying out adequate professional-technical tasks of certification service provider, keeping the register of signatories and protecting personal data;
4) Technical and program solutions that comply with international standards for performing certification service;
5) System of physical protection of devices, equipment and data;
6) Security solutions for protection against unauthorised access to and damage of information.

Article 15

Provider of qualified certificates issuance service, in addition to conditions under the Article 14 of this Law, must meet the following requirements, namely to:

1) Ensure safe performance of certification service, safe and timely keeping of register of signatories and implementation of safe and immediate certificate revocation;

2) Provide accurate determination of the date and time (hour and minute) of issuance or revocation of certificate;

3) Provide verification of signatory's identity, in an appropriate manner and in accordance with the regulations, and, if necessary, any additional characteristics of the person to whom the certificate has been issued;

4) Employ personnel with specialist knowledge, experience and professional qualifications necessary for providing certification service, particularly in relation to: competences at the management level, expertise in application of electronic signature technologies and appropriate safety procedures and safe application of appropriate administrative and management procedures that are harmonised with international standards;

5) Use reliable systems and products that are protected from unauthorised changes and that provide technical and cryptographic security of the process;

6) Take measures against forging of certificates, and in cases where provider generates data for creation of electronic signature to guarantee the confidentiality of the process of generating such data;

7) Have financial resources for risk and liability insurance for possible damage caused by providing qualified certificates issuance service;

8) Have system for storing all relevant information relating to qualified certificates in a specific period of time, especially for providing evidence of those certificates for the purposes of legal proceedings, and those information can be stored in electronic form;

9) Have secure system that prevents saving and copying of data for creation of electronic signature for persons to whom certification services are provided;

10) Have systems for physical protection of devices, equipment and data, as well as security solutions for protection against unauthorised access;

11) Provide system for informing the persons seeking certification service about exact terms of using the service, including any restrictions, as well as procedures for resolving complaints, and information that can be delivered electronically must be written and prepared in understandable manner and relevant parts of that information must be available upon the request of third parties that use the certificate;

12) Use reliable system of keeping qualified certificate in a form that allows verification, in order to:

- Ensure that input and changes are done only by authorised persons,
- Enable verification of authenticity of information in the certificate,
- Make certificates available to public for browsing only in those cases for which the registered signatory had given authorisations,
- Make any technical change, which could harm safety requirements, known to the certification service provider.

Article 16

Certification services may be also preformed by administration authority, if they fulfil all the conditions laid down by this Law and regulations adopted under this Law.

The scope of work, content and certification service providers for administration authorities shall be regulated by the Government of the Republic of Montenegro.

Article 17

Certification services in the Republic of Montenegro (hereinafter referred to as “the Republic”) may be performed also by certification service providers that have head offices abroad.

Qualified certificates issued by certification service providers with head office in one of the Member States of the European Union have the same legal force as qualified certificates issued in the Republic.

Qualified certificates issued by certification service providers with head office abroad, outside the European Union, have the same legal force as qualified certificates issued in the Republic, provided that:

1) Certification service provider meets the requirements of this Law for issuing qualified certificates and if it has entered into the register of the competent authority in the Republic;
2) Local provider of qualified certificates issuance services guarantees for such qualified certificate;
3) It is stipulated by bilateral or multilateral agreement between the Republic and other countries or international organisations;
4) Qualified certificate or provider of qualified certificates issuance services is recognised on the basis of bilateral or multilateral agreement between the European Union and third countries or international organisations.

Article 18

Certification service provider does not need special permission to perform the services.

Article 19

Certification service provider has a duty to submit an application to the competent administration authority on beginning of performing certification services, at least eight days before work starts.

With the application referred to in paragraph 1 of this Article or in cases of changes in service delivery, certification service provider shall submit documentation about the internal rules of operation related to creation and verification of electronic signatures and internal organisation, as well as documentation proving that conditions under Article 14 and 15 of this Law have been fulfilled.

Article 20

Certification services in the Republic may be performed only by registered certification service providers.

Article 21

The competent administration authority shall enter certification service providers in records of certification service providers (hereinafter referred to as “records”), immediately after the service provider submits the application on the beginning of performing services.

Entry in records shall not be subject to administrative procedure conduction.

Records shall be public and kept also in electronic form.

Records in electronic form shall be signed by advanced electronic signature of the competent administration authority, which qualified certificate is published in the Official Gazette of the Republic of Montenegro".

The competent administration authority shall prescribe the content and manner of keeping records, forms of applications for entry in the records and applications for entry of changes, as well as type, content and manner of delivery of documentation necessary for entry in the records.

Article 22

Certification service provider who entered the records, if proves that all conditions for delivery of services prescribed by this Law and regulations adopted under this Law are fulfilled, may require from the competent administration authority to enter it in the Register of accredited certification service providers (hereinafter referred to as “the register”).

The Decision on fulfilment of the conditions referred to in paragraph 1 of this Article shall be adopted by the competent administration authority on the basis of insight in documentation submitted with the application for entry in the register and, if necessary, on the basis of direct insight.

The Decision shall be issued within 15 days after the day of proper application submission.

The administrative procedure for entry into the register, on issues that are not regulated by this Law, the provisions of the Law on General Administrative Procedure shall be applied.

Article 23

The competent administration authority, based on the Decision establishing that the applicant fulfils all prescribed conditions, in terms of Article 22, paragraph 1 of this Law, shall immediately enter the applicant in the register.

The register shall be public and kept also in electronic form.

The register shall be signed by advanced electronic signature of the competent administration authority, which qualified certificate is published in the Official Gazette of the Republic of Montenegro".

The competent administration authority shall prescribe the content and manner of keeping records, forms of applications for entry in the register and list of documentation that is submitted with the application, as well as the amount and manner of payment of registration costs.

Article 24

Certification service provider who entered the register (the accredited service provider) may indicate that fact in issued certificates.

IV RIGHTS, OBLIGATIONS AND RESPONSIBILITIES OF SIGNATORIES AND CERTIFICATION SERVICE PROVIDERS

Article 25

Legal or natural person shall independently select certification service provider.

Signatory may use certification services of one or more certification service providers.

Signatory shall use certification services pursuant to contract with selected certification service provider.

Article 26

Qualified certificate may be issued to any person upon his/her request, based on determined identity and other data about the person to who qualified certificate shall be issued.

Article 27

Signatory has duty to protect carefully means and data for creation of electronic signature from unauthorised access and use and to use them in accordance with the provisions of this Law.

Article 28

Signatory has duty to submit all necessary data and information about changes that affect or may affect the accuracy of immediate determining of signatory's identity to certification service provider no later than 48 hours after the change occurred.

Signatory has duty to seek the revocation of his/her certificate in all cases of loss or damage of means or data for creation of own electronic signature.

Article 29

Signatory shall be liable for irregularities that have occurred due to failure to meet the obligations regulated by the provisions of Article 27 and 28 of this Law.

Signatory shall not be liable for irregularities in cases when he/she proves that the party whom suffered the damage had not taken, or had wrongly taken the actions related to verification of electronic signature.

Article 30

Certification service provider has duty to:

1) Ensure that every qualified certificate contains all necessary information regulated by Article 13 of this Law;
2) Conduct full verification of signatory's identity;
3) Ensure accuracy and integrity of data entered in records of issued certificates;
4) Enter basic information about own identity in each certificate;
5) Allow any interested person to have insight into own identification data;
6) Keep timely, accurate and with security measures protected records of certificates that must be publicly available;
7) Keep timely, accurate and with security measures protected records of invalid certificates;
8) Provide visible information about the exact date and time (hour and minute) of issuance or revocation of certificate;
9) Keep all data and documentation about issued and revoked certificates as a proof and verification mean in judicial, administrative and other proceedings, for at least 10 years since their expiration, where data and accompanying documentation may be in electronic form;
10) Apply provisions of the Law and other regulations governing the protection of personal data.

Article 31

Certification service provider, before the conclusion of the contract referred to in Article 25, paragraph 3 of this Law, shall notify the person who submitted the request for certification issuance about all relevant circumstances for its use.

Notification under paragraph 1 of this Article shall contain:

1) Excerpt from existing regulations, internal rules and other conditions related to the use of certificates;
2) Information on possible restrictions that apply to the use of certificates and the value of business events for which the certificate is issued;
3) Information on appropriate legal remedies when dispute arises;
4) Information on measures that shall be implemented by signatories and on technology necessary for safe creation and verification of electronic signatures.

Article 32

Certification service provider has duty to terminate certification service, i.e. revoke a certificate in cases when:

1) Revocation of a certificate is required by a signatory or his/her authorised legal representative;
2) Determines that the information in the certificate is incorrect or that the certificate is issued on the basis of erroneous data;
3) Receives official notice that the signatory had lost the capacity to exercise rights, ceased to exist or that circumstances that significantly affect the validity of the certificate had changed;
4) Determines that data for creation of electronic signature or information system of signatory are threatened in a manner that affects reliability and safety of creation of electronic signature;
5) Determines that data for verification of electronic signature or information system of certification service provider are threatened in a manner that affects reliability and safety of certificates;
6) Ceases to work or his work is banned, but validity period of issued certificates has not expired yet.

Certification service provider has duty to keep records of all revoked certificates up to date.

Certification service provider has duty to notify the signatory about the revocation of the certificate within 24 hours after received request or notification, i.e. arise of circumstances that caused revocation of the certificate.

Article 33

Certification service provider has duty to:

1) Apply organisational and technical measures of protection of certificates and data related to signatories;
2) Establish and apply a system of protection of access to records of certificates and revoked certificates, which shall allow access only to authorised persons and ensure verification of data transfer accuracy and timely insight into possible errors of technical assets,

Measures and procedures referred to in paragraph 1 of this Article shall be prescribed by the competent administration authority.

Article 34

In case that certification service provider, due to potential bankruptcy or need, i.e. intent to terminate business activity, has the intention to terminate the contract, it shall notify each signatory and the competent administration authority about that, at least three months before the date scheduled for termination of the contract.

Certification service provider has duty to ensure continued performance of certification services for signatories, to whom it has issued the certificates, by other service provider and to deliver it all documentation related to performed certification services.

If the certification service provider does not provide continued performance of services by other provider, it shall revoke all issued certificates and immediately, at the latest

within 48 hours, notify the competent administration authority and submit all documentation related to performed services.

The competent administration authority shall immediately revoke all certificates issued by the service provider that for any reason has not revoked issued certificates, at the expense of the service provider.

Article 35

Certification service provider shall ensure connection of its records of issued and revoked certificates with other certification service providers by using available information technology and technical and program means, which operation is in accordance with applicable international standards.

The competent administration authority shall stipulate technical rules for ensuring the connection between records of issued and revoked certificates of certification service providers in the Republic.

Technical rules referred to in paragraph 2 of this Article shall include currently available scientific and technological achievements, as well as internationally accepted standards and they cannot be set for a period longer than two years.

Article 36

Provider of qualified certificates issuance services has duty to insure the risk of liability for damages arising from performing certification services.

The competent administration authority shall prescribe the lowest amount of insurance referred to in paragraph 1 of this Article.

Article 37

Certification service provider that issues qualified certificates or guarantees for qualified certificates issued by other provider is liable for damage caused to the party who relied on that certificate, if:

1) Information that qualified certificate contains is not valid at the moment of its issuance;
2) The certificate does not contain all elements prescribed for qualified certificate;
3) The provider did not enable a signatory to, at the moment of issuance of the certificate, have data for creation of electronic signature that correspond to data for verification of electronic signature that are given, i.e. identified in the certificate;
4) The provider does not ensure that data for creation and data for verification of electronic signature may be used complementary, when they are generated by the provider;
5) The provider fails to revoke the certificate in accordance with the provisions of Article 32 of this Law;
6) The certificate does not contain information on restrictions regarding the use or the value of business events for which the certificate is issued.

Certification service provider is not liable for damage referred to in paragraph 1 of this Article, if he proves that he acted with the diligence of a good businessmen.

Certification service provider is not liable for the damage caused by the use of the certificate beyond restrictions, if these restrictions are clearly stated in the certificate.

Article 38

Certification service provider may collect personal data that are necessary for the issuance and maintenance of the certificate, directly from the signatory or indirectly with his/her clearly expressed consent.

Personal information collected in accordance with paragraph 1 of this Article cannot be processed or used for other purposes without clearly expressed consent of the signatory.

Certification service provider, upon the request of the signatory, may enter signatory's pseudonym in the certificate, instead of full name of the signatory.

V SUPERVISION

Article 39

Supervision of the certification service providers shall be done by the competent administration authority.

Supervision of the certification service providers in domain of collection, use and protection of personal data of signatories may be performed both state and other authorities defined by the Law and other regulations governing the protection of personal data.

Article 40

Within the supervision of work of registered, i.e. recorded certification service providers, the competent administration authority shall:

1) Determine whether they fulfil the conditions prescribed by this Law and regulations adopted under this Law;
2) Control the regularity of implementation of prescribed procedures and organisational-technical measures, the application of internal rules regarding the conditions stipulated in this Law and regulations adopted under this Law.

Article 41

Certification service provider has duty to enable authorised persons of authorities referred to in Article 39, paragraph 1 and 2 of this Law access to its business premises and insight into business information, insight into business documents, access to the register of signatories and computer equipment and devices that it uses, in order to conduct surveillance.

If certification service provider does not fulfil the conditions prescribed by this Law and regulations adopted under this Law, the authorised person of the competent

administration authority shall render a Decision on administrative procedure, which shall temporarily prohibit the provision of certification services and that fact shall be entered in the records, i.e. the register.

The competent administration authority, after enforceability of the Decision referred to in paragraph 2 of this Article, shall delete certification service provider from records, i.e. the register.

VI PENALTY PROVISIONS

Article 42

A fine amounting from 3 to 15 minimum wages in the Republic shall be imposed on a natural person, who without authorisation accesses and uses data and means for creation of electronic signature and advanced electronic signature for misdemeanour.

Article 43

A fine amounting from 10 to 20 minimum wages in the Republic shall be imposed on a signatory, i.e. natural person or responsible person of legal person who represents the signatory for misdemeanour, if:

1) He/she carelessly and irresponsibly uses the means and data for creation of electronic signature (Article 27);

2) Certification service provider fails to submit required data and information about changes that affect or may affect the accuracy of the electronic signature within the time limit set out in Article 28, paragraph 1 of this Law;

3) Certification service provider fails to submit timely the request for revocation of the certificate (Article 28, paragraph 2).

Article 44

A fine amounting from 20 to 150 minimum wages in the Republic shall be imposed on certification service provider for misdemeanour, if it:

1) Issues a qualified certificate that does not contain all the necessary information (Article 13, paragraph 1);
2) Does not report to the competent administration authority the beginning of performing certification services within prescribed period (Article 19, paragraph 1);
3) Does not implement appropriate protective measures to prevent unauthorised saving and copying of data for creation of electronic signature (Article 15, paragraph 1, item 9);
4) Does not inform the signatory to whom it issues the certificate on all relevant conditions of issued certificate use (Article 15, paragraph 1, item 11);
5) Does not determine validly the identity of natural or legal person for whom a qualified certificate is being issued (Article 30, paragraph 1, item 2);

6) Does not keep updated and security measures protected records of certificates and does not allow their public accessibility (Article 30, paragraph 1, item 6);

7) Does not keep updated records of all revoked certificates (Article 32, paragraph 2);

8) Does not inform the signatory about completed certificate revocation within prescribed period (Article 32, paragraph 3);

9) Does not timely inform signatories to whom the certificates have been issued and the competent authority about possible bankruptcy or other circumstances that may terminate the performance of certification services (Article 34, paragraph 1);

10) Does not allow authorised persons of the competent authority access to its business premises and insight into business information, business documentation, access to the register of signatories, computer equipment and devices (article 41, paragraph 1).

Article 45

A fine amounting from 20 to 100 minimum wages in the Republic shall be imposed on a legal person for misdemeanour, if it:

1) Refuses admission of an electronic document with electronic signature or advanced electronic signature, only because it is in electronic form (Article 3, paragraph 1);

2) Does not store data and means for verification of electronic signature for as long as electronic documents are kept (Article 5).

VII TRANSITIONAL AND FINAL PROVISIONS

Article 46

Secondary legislation, on the basis of competences referred to in this Law, shall be passed within four months from the day of entry into force of this Law by the competent administration authority.

Article 47

This Law shall enter into force on the eighth day following that of its publication in the Official Gazette of the Republic of Montenegro.