**LAW No. 107/2015**
**ON ELECTRONIC IDENTIFICATION AND TRUST SERVICES**

Pursuant to article 78 and 83, paragraph 1 of the Constitution, upon the proposal of the Council of Ministers,

**THE ASSEMBLY OF**
**THE REPUBLIC OF ALBANIA**

**DECIDED:**

## CHAPTER I
## GENERAL PROVISIONS

### Article 1
### Objective

The objective of this law is to establish the necessary legal framework for electronic identification, electronic seals, electronic registered delivery services and certificate services for website authentication in the Republic of Albania.

### Article 2
### Scope

1. This law applies to trust services especially electronic transactions and electronic identification schemes.
2. The provisions of this law do not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants and also to the cases foreseen otherwise by the legislation in force.

### Article 3
### Definitions

For the purposes of this law, the following definitions apply:
1. "Authentication" means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed[1]
2. "National Authority for Electronic Certification", here and after the Authority, is the public institution as per the law no. 9880, dated 25.2.2008, "On electronic signature".
3. "Certificate for website authentication" means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued

[1] This law is partially aligned with the Regulation (EU) no.910/2014 of the European Parliament and of the Council, of 23 July 2014 "On electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC", CELEX number 32014R0910, Official Journal of European Union, L Series, no. L257, dated 28.8.2014, pages 73-114.

4. “Qualified certificate for website authentication” means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in law.
5. “Certificate for electronic seal” means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person.
6. “Qualified certificate for electronic seal” means a certificate for an electronic seal that is issued by a qualified trust service provider and meets the requirements laid down in this law.
7. “Safe electronic identification” means the electronic identification of a natural person and certification of authenticity of his/her identity, by using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.
8. “Initial identification” means the verification of the identity of the applicant to be provided with the electronic identification means.
9. “Creator of a seal” means a legal person who creates an electronic seal;
10. “Holder of the identification means” is the natural person, who has been provided with the identification means by the identification service provider based on agreement recognized by the parties.
11. “Electronic seal creation device” means configured software or hardware used to create an electronic seal;
12. “Qualified electronic seal creation device” means an electronic seal creation device that meets mutatis mutandis the requirements laid down in this law.
13. “Electronic identification means” means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service.
14. “Trust service provider” means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.
15. “Qualified trust service provider” means a trust service provider as per the law no. 9880 dated 25.2.2008 “On electronic signature” which in addition to the services laid down in this law, may provide other trust services.
16. “Conformity assessment body” means a natural or legal body according to law “On electronic signature” which carries out conformity assessment of a qualified trust service provider, in addition to the provision of qualified trust services.
17. “Relying party” means a natural or legal person that relies upon an electronic identification or a trust service;
18. “Electronic identification scheme” means the set of electronic identification means and systems which are necessary for the electronic identification;
19. "Trust service"’ means an electronic service which consists of: the creation, verification, and validation of electronic seals, electronic registered delivery services and certificates related to those services, or the creation, verification and validation of certificates for website authentication; or electronic identification through electronic identification means used within the electronic identification scheme, the preservation of seals or certificates related to those services.
20. “Qualified trust service” means a trust service, providing qualified electronic signature and qualified time stamps, according to law no. 9880, dated 25.2.2008, “On electronic signature”, qualified time stamps, qualified electronic registered delivery service, qualified certificate for website authentication, electronic identification through electronic identification means used within the electronic identification scheme, as laid down in this law.

21. “Electronic registered delivery service” means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;
22. “Qualified electronic registered delivery service” means an electronic registered delivery service which meets the requirements laid down in this law;
23. “Person identification data” means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;
24. “Electronic seal creation data” means unique data, which is used by the creator of the electronic seal to create an electronic seal;
25. “Validation data” means data that is used to validate an electronic signature or an electronic seal.
26. “Electronic transaction” means purchase or sale of goods or services, carried out by natural persons, legal persons, public or private, through computer networks.
27. “Validation” means the process of verifying and confirming that an electronic signature or a seal is valid.28. “Electronic seal’ means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity;
29. “Qualified electronic seal” means an electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.

## CHAPTER II
## SAFE ELECTRONIC IDENTIFICATION

### Article 4
### Legal validity of safe electronic certification

Safe electronic identification is made possible through electronic identification means issued according to the electronic identification scheme by qualified trust service providers for the purpose of providing electronic services. Personal data created through the safe electronic identification shall be considered true and taken for granted and they shall have same legal value as the data obtained from identification of a natural person through the official identification document.

### Article 5
### Guarantee provided by the electronic identification scheme

The electronic identification scheme ensures high level of credibility as regards the claimed or asserted identity of the person and it is characterized by technical specifications, standards and related procedures, including technical checks which aim is to lower the risk of identity misuse or change. Technical specifications, standards and procedures for the levels of credibility of electronic identification shall be established by subordinate legal acts of the Council of Ministers.

### Article 6
### Requirements for the identification procedures

The procedures of safe identification meet the following requirements:
1. Initial identification must meet the requirements defined in article 7 of this law, where related data must be verifiable at any time.
2. ensure identity of the holder of the identification means.
3. guarantee use by the holder of the identification means alone.

**Article 7**
**Requirements for initial identification**

1. Initial identification is done based on the physical appearance of the applicant of the electronic identification means. The qualified trust service provider shall check diligently the identity of the applicant through the electronic identification document.
2. If the qualified trust service provider is not able to verify the identity of the applicant, the competent body issuing this document shall verify the identity and electronic identification document.

**Article 8**
**Electronic certificate for electronic identification**

The electronic certificate necessary for the safe electronic identification shall contain at least:
a) information on the qualified trust service provider;
b) information on the certificate holder;
c) validity period of the certificate;
ç) certificate identification data;
d) possible restrictions to certificate use;
dh) public key of the certificate holder;
e) qualified electronic signature of the qualified trust service provider.

**Article 9**
**Provision with safe electronic identification means**

1. Provision with safe electronic identification means is based on a written agreement between the applicant for electronic identification means and trust service provider.
2. Validity period of identification means may be shorter than the validity period of the agreement.
3. Identification means are issued always to natural persons.
4. Every identification mean is linked solely to its holder.

**Article 10**
**Cooperation and interoperability**

Safe electronic identification service provider shall cooperate and interoperate with state and private institutions through the safe electronic identification schemes providing electronic services for the purpose of authentication of natural or legal persons.

**CHAPTER III**

## TRUST SERVICES AND RESPONSIBLE AUTHORITY

### Article 11
### Accessibility for persons with disabilities

Trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

### Article 12
### Responsible authority

The National Authority for Electronic Certification shall be in charge of enforcing this law.

### Article 13
### Registration of trust service providers

The Authority shall record the names of the qualified trust service providers and the names of those who have suspended their activity in accordance with article 31 of this law. This registry book shall be updated and published electronically.

### Article 14
### Termination of the activity of the trust service provider by the Authority

The authority shall terminate temporarily, completely or partially the activity of qualified trust service providers, as foreseen in law no. 9880 dated 25.2.2008 “On electronic signature”.

### Article 15
### Qualified certificates

Issuing, repeal, revocation of qualified certificates shall be done as foreseen in law no. 9880 dated 25.2.2008 “On electronic signature”.

### Article 16
### Inspection and cooperation

The authority inspecting the qualified trust service provider are bound to cooperate as foreseen in law no. 9880 dated 25.2.2008 “On electronic signature”.

## CHAPTER IV
## TRUST SERVICE PROVIDER

### Article 17
### Requirements for the exercise of the trust service activity

1. The trust service provider, within 30 days from the start of the service, shall submit to the Authority the request for registration of this service.

2. The trust service provider must prove possession of:
a) necessary credibility and specialized knowledge appropriate for the activity of the trust service provider;
b) sufficient financial resources for the possible risk of liability for damages, in accordance with article 30 of this law.
3. Trust service provider shall employ reliable staff and make use of trustworthy products.
4. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this law.
5. If the Authority concludes that the trust service provider and the trust services provided by it comply with the requirements of this law, the Authority shall grant it the qualified status.
6. Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been awarded as referred to in paragraph 5 of this article.
7. The Authority shall, by means of instruction, define the formats and procedures for the purpose of this law.
8. The requirements and criteria to be met by the qualified trust service provider shall be defined in subordinate legal acts of the Council of Ministers.

**Article 18**
**Data protection and documentation of security measures**

Data protection from forgery and security of confidentiality of codes, documentation of security measures and qualified certificates by the qualified trust service provider are done in accordance with the provisions of the law no. 9880, dated 25.2.2008, "On electronic signature".

**Article 19**
**Reporting of the circumstances of failure to meet the requirements**

The qualified trust service provider shall ensure fulfilment of the conditions foreseen in article 17 of this law, during the period of exercise of the activity. Any circumstance which makes this impossible, shall be immediately reported to the Authority.

**Article 20**
**Transfer of tasks to the trust services**

The qualified trust service provider, when unable to perform the activity, may transfer to third persons the tasks foreseen in this law and subordinate legal acts issued in implementing the law, if the persons meet the requirements foreseen in this law for the exercise of the activity. The transfer does not exclude the responsibility of the service provider for the obligations deriving from this law.

**Article 21**
**Reporting to Authority by the qualified trust service provider**

Every qualified trust service provider shall submit a detailed annual report of its activity, not later than 31 March of the next year. Moreover, the qualified trust service provider shall report to the Authority whenever information is requested by the latter.

## CHAPTER V
## ELECTRONIC SEALS

### Article 22
### Legal effects of electronic seals

1. A qualified electronic seal shall be considered admissible in legal proceedings, irrespective of it being in electronic form.
2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.
3. A qualified electronic seal based on a qualified certificate issued by a qualified trust service provider shall have the same legal validity as the embossing seal.

### Article 23
### Requirements for qualified electronic seals

An electronic seal shall meet the following requirements:
1. it is uniquely linked to the creator of the seal.
2. it is capable of identifying the creator of the seal.
3. it is created using electronic seal creation data that the creator of the seal can use.
4. it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
5. it is based on a qualified electronic certificate.

### Article 24
### Qualified certificates for electronic seals

Qualified certificates for electronic seals shall contain:
a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;
b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, for a legal person, the name and the unique identification number of the subject;
c) electronic seal validation data, which corresponds to the electronic seal creation data;
ç) details of the beginning and end of the certificate's period of validity;
d) the certificate identity code, which must be unique for the qualified trust service provider;
dh) the electronic signature or qualified electronic seal of the issuing qualified trust service provider;
e) the location where the certificate supporting the electronic signature or electronic seal referred to in letter "dh", of this article, is available free of charge;
ë) the location of the services that can be used to enquire as to the validity status of the qualified certificate; where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.

**Article 25**
**Qualified electronic seal creation devices**

Qualified electronic seal creation devices must meet the requirements and technical specification for qualified electronic signature creation devices as stipulated in law no. 9880 dated 25.2.2008 "On electronic signature".

## CHAPTER VI
## ELECTRONIC REGISTERED DELIVERY SERVICE

**Article 26**
**Legal effect of an electronic registered delivery service**

1. Data sent and received using an electronic registered delivery service shall be admitted in legal proceedings irrespective of their being in electronic form.
2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt.

**Article 27**
**Requirements for qualified electronic registered delivery services**

Qualified electronic registered delivery services shall meet the following requirements:
a) they are provided by one or more qualified trust service provider(s);
b) they ensure with a high level of confidence the identification of the sender;
c) they ensure the identification of the addressee before the delivery of the data;
ç) the sending and receiving of data is secured by a qualified electronic signature or a qualified electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;
d) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;
dh) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp. In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (dh) of this article shall apply to all the qualified trust service providers.

## CHAPTER VII
## WEBSITE AUTHENTICATION

**Article 28**
**Requirements for qualified certificates for website authentication**

Qualified certificates for website authentication shall contain:
a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;

b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least:

i) for a natural person: the name of the person to whom the certificate has been issued;

ii) for a legal person: the name and, where applicable, registration number as stated in the official records;

c) elements of the address, including the residence place, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;

ç) the domain name(s) operated by the natural or legal person to whom the certificate is issued;

d) details of the beginning and end of the certificate's period of validity;

dh) the certificate identity code, which must be unique for the qualified trust service provider;

e) the electronic signature or electronic seal of the issuing qualified trust service provider;

ë) the location where the certificate supporting the electronic signature or electronic seal referred to in letter (e) of this article is available free of charge;

f) the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.

## CHAPTER VIII
## LEGAL LIABILITY

### Article 29
### Indemnification

1. The qualified trust service provider shall indemnify third persons for any damage caused, in the following cases:

a) it violates the requirements of this law and subordinate legal acts issued in implementing the law;

b) its products for qualified trust services of technical safety do not function properly.

2. The qualified trust service provider shall be exempt from the obligation to pay damages if it proves that it has acted in absence of fault or third persons have been aware of the existence of the grounds foreseen in paragraph 1 of this Article.

3. Where qualified trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, qualified trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

4. The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to above.

### Article 30
### Assets warranty

The qualified trust service provider shall be obliged to take the adequate financial measures to ensure fulfilment of the legal obligations according to the stipulations of the law no. 9880 dated 25.2.2008 "On electronic signature".

### Article 31
### Actions following termination of activity of the qualified trust service provider

1. The qualified trust service provider shall immediately report to the Authority for the termination of the exercise of activity.
2. In case of activity termination, the qualified trust service provider must immediately:
a) see to that the valid certificates are transferred under another trust service provider and support the substitute provider by making all the necessary data available to the latter;
b) if provisions of letter "a" of this paragraph are impossible to be applied, revoke all the valid electronic certificates;
c) inform the holder of electronic certificates of the termination of the activity and related consequences.

**Article 32**
**Data use and delivery**

Data use and delivery by the qualified trust service provider shall be done in accordance with the law no. 9880 dated 25.2.2008 "On electronic signature".

**Article 33**
**Conformity assessment body**

Conformity assessment body shall meet the requirements foreseen in law no. 9880 dated 25.2.2008 "On electronic signature".

**Article 34**
**Acceptance and use of foreign products**

Trust products created by qualified trust service provider outside the Republic of Albania shall be recognised only based on the respective agreement signed by the Republic of Albania with the other states.

**Article 35**
**Fees**

Council of Ministers, on the proposal of the competent minister shall approve the amount and types of fees to be paid by the qualified trust service provider to the Authority in implementing the obligations defined in this law. The fee amount may not be higher than the costs of the service provider by the Authority.

**CHAPTER IX**
**ADMINISTRATIVE MEASURES**

**Article 36**
**Administrative offences**

The following offences, unless they constitute criminal offences, shall be considered administrative offences and the following penalties shall apply:

1. 1 million ALL fine for the following offences:
a) failing to meet the requirements for the exercise of the activity, according to article 17 of this law;
b) failing to meet the requirements laid down in article 18 of this law;
c) failing to cooperate with the Authority, in implementing articles 16, 21 and 32 of this law.
2. 2 million ALL fine for the following offences:
a) failing to notify initiation of the activity, according to article 17 of this law;
b) failing to meet the requirements and conditions for the safe identification, according to article 6 and 7 of this law;
c) failing to take the measures required after termination of the trust service, according to article 31 of this law.
Income generated from the fines shall be disbursed to the State Budget.

**Article 37**
**Other measures**

Where the Authority, irrespective of the measures foreseen in article 36, and also the requirements laid down in article 14 of this law, reasonably deems that breaches are to the extent or of that kind to infringe integrity and reliability of the service providers, the Authority shall temporarily, completely or partially, terminate the activity of trust service providers.

**Article 38**
**Appeal and execution**

1. The decision imposing fines or activity termination measure may be appealed against with the responsible minister within 10 days from notification.
2. The minister shall take a decision within 30 days. The decision may be appealed against with the administrative court within 45 days from the date of promulgation or notification.
3. Review of administrative offences, appeal and execution of decisions shall be done in compliance with the law on "Administrative offences".

**CHAPTER X**
**FINAL PROVISIONS**

**Article 39**
**Subordinate legal acts**

The Council of Ministers is tasked, within 6 months from the entry into force of this law, with issuing subordinate legal acts in implementing article 5, 17 and 35 of this law.

**Article 40**
**Entry into force**

This law enters into force 15 days after publication in the Official Gazette.
Adopted on 1.10.2015

Promulgated by decree no.9279 dated 15.10.2015 of the President of the Republic of Albania Bujar Nishani.