LAW
ON ELECTRONIC DOCUMENT, ELECTRONIC IDENTIFICATION AND TRUST SERVICES IN ELECTRONIC BUSINESS
(“Official Gazette of the RS”, No 94/2017 and 52/21)

I INTRODUCTORY PROVISIONS

Subject matter

Article 1.

This Law shall regulate electronic document, electronic identification and trust services in electronic business.

Definitions

Article 2.

For the purposes of this Law, the following definitions apply:

1) ”electronic business” means the use of data in electronic form, means of electronic communication and electronic data processing in conducting the business of natural and legal persons;

2) ”electronic form of data” means the digital recording of data suitable for electronic processing and transmission by means of electronic communication;

3) ”electronic transaction” means the business activity between two or more parties that is carried out electronically;

4) ”electronic document” means a set of data consisting of letters, numbers, symbols, graphic, audio and video materials, in electronic form;

5) ”product” means hardware, software, i.e. hardware with accompanying software, or the relevant components thereof, intended for electronic processing, electronic transmission and/or storage of data;

6) ”interoperability” means the ability of two or more systems, or of the components thereof, to exchange data and enable joint use of data and knowledge;

7) ”public sector body” means a state authority, an authority of the Autonomous Province, an authority of a local self-government unit, of a company, institution, organization, and individuals entrusted with the tasks within the competence of the Republic of Serbia, i.e. public powers;

8) ”natural person representing a legal person” means a natural person that has been registered to conduct a certain business activity in compliance with the law;

9) ”authentication” means the process of identity verification of a legal person, natural person or natural person representing a legal person, including verification of integrity and origin of data presumed to be created, or sent by such person;

10) ”person identification data” means a set of data based on which it shall be possible to uniquely establish the identity of a legal person, a natural person, or a natural person representing a legal person;

11) ”electronic identification” means the process of using person identification data in electronic form uniquely representing either a legal person, a natural person, or a natural person representing a legal person;

12) ”electronic identification means” means a material and/or immaterial unit containing person identification data and which is used to prove identity during authentication;

13) ”electronic identification scheme” means a system for issuing electronic identification means to a legal person, natural person or a natural person representing a legal person;

14) ”electronic identification service” means a service enabling the use of a certain electronic identification scheme in electronic transactions, where, within such service, guarantees are provided that identification data from the electronic identification means is matched to the person to which the means was issued;

14a) a node represents the connection point that is a part of the interoperability structure of electronic identification and makes cross-border face authentication, and has recognition and processing functions, i.e. sends

data transmissions to other nodes by ensuring that the electronic identification structure of one state connects with the electronic identification structure of another state;

15) ”trust service” means an electronic service facilitating the business activity between two or more parties, based on the service provider's guarantees of authenticity of individual pieces of data to the parties, which is as such determined by this Law;

16) ”trust service provider” means a legal person or a natural person representing a legal person who provides one or more trust services;

17) ”relying party” means a legal or natural person that relies upon an electronic identification and/or a trust service;

18) ”qualified trust service” means a trust service that meets the requirements laid down in this Law for the qualified trust service;

19) ”qualified trust service provider” means a legal person or a natural person representing a legal person who provides one or more qualified trust services in accordance with this law;

20) ”electronic signature” means a set of data in electronic form, which is attached to or logically associated with other (signed) data in electronic form so that the integrity of these data and the identity of the signatory are verified by the electronic signature;

21) ”electronic seal” means a set of data in electronic form, which is attached to or logically associated with other (sealed) data in electronic form so that the integrity of these data and the identity of the creator of the seal are verified by the electronic seal;

22) ”electronic signature and/or seal creation data” means unique data used by the signatory and/or creator of the seal to create an electronic signature and/or seal, which are logically associated with the relevant data for electronic signature and/or seal validation;

23) ”electronic signature and/or seal validation data” means data that is used to check whether an electronic signature and/or seal corresponds to signed and/or sealed data;

24) ”certificate for electronic signature and/or seal” means an electronic attestation verifying the link between the electronic signature and/or seal validation data and the identity of the signatory and/or creator of the seal;

25) ”signatory” means a natural person who creates an electronic signature, and whose identification data is specified in the certificate based on which such electronic signature is created, i.e. in the certificate attesting the link between the identity of such signatory and electronic signature validation data which corresponds to electronic signature creation data used by the signatory in creating such electronic signature;

26) the “creator of a seal” is a legal person, natural person in the role of a registered subject, a natural person that has been entrusted with the exercise of public authority, and who, in accordance with special regulations, has the right to use a stamp (for example, persons who have licenses to perform work or activities), in whose name an electronic stamp is created, and whose identification data is listed in the certificate, based on which the electronic seal is created, i.e. a certificate in which the connection between the identity of the creator of a seal, and the data required to validate the electronic seal, which correspond to the data required for the creation of an electronic seal, as authorized by the person using the seal, used when creating the electronic seal in question;

27) “electronic signature and/or seal creation device” means a technical device (software and/or hardware) used to create an electronic signature and/or seal with the use of electronic signature and/or seal creation data;

28) “validation” means the process of verifying and confirming that an electronic signature and/or an electronic seal is valid;

29) “advanced electronic signature” means an electronic signature which meets additional requirements for the provision of a higher level of reliability in verification of data integrity and signatory's identity, in compliance with this Law;

30) “qualified electronic signature” means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signature and which is issued by the provider of a qualified trust service in accordance with this law;

31) “qualified electronic signature creation device” means a device that meets the requirements laid down in this Law;

32) ”qualified certificate for electronic signature” means a certificate for electronic signature that is issued by a provider of qualified service and meets the requirements laid down in this Law;;

33) ”advanced electronic seal” means an electronic seal that meets the additional requirements for the provision of a higher level of reliability in verification of data integrity and identity of a creator of the seal, in compliance with this Law;

34) ”qualified electronic seal” means an advanced electronic seal that is created by a qualified electronic seal creation device, and which is based on a qualified certificate for electronic seal;

35) ”qualified electronic seal creation device” means a device that meets the requirements laid down in this Law;

36) ”qualified certificate for electronic seal” means a certificate for electronic seal that is issued by a provider of qualified service and meets the requirements laid down in this Law;

36a) the service of managing a qualified asset for the long-distance creation of an electronic stamp is a service of developing long-distance, qualified electronic stamps via assets for the creation of an electronic stamp which is managed, in the name of the signatory, by a provider of qualified trust service, who guaranteed that the data used for the development of an electronic stamp are used under the signatory’s exclusive control, in accordance with this law;

36б) the service of managing the qualified assets for long distance the creation of an electronic stamp is the service of the development of a qualified electronic stamp remotely, using the funds to create an electronic seal which is managed by a qualified, trust service provider in the name of the creator of a seal, and who guarantees that the data used for the development of the electronic seal are used under the exclusive control of the creator of a seal, in accordance with this law;

37) the website authentication certificate is a the web site authentication certificate is a confirmation using the website authentication and by which the website is connected with the identity of the legal or natural person;

38) ”qualified certificate for website authentication” means a certificate for website authentication, which is issued by a provider of qualified service and meets the requirements laid down in this Law;

39) ”electronic time stamp” means official time attached to data in electronic form establishing evidence that such data existed at that time;

40) ”qualified electronic time stamp” means an electronic time stamp which meets the requirements laid down in this Law for a qualified electronic time stamp, and is issued by the provider of a qualified trust service in accordance with this law;

41) ”electronic registered delivery service” means a data transfer service by electronic means within which the service provider provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, whereby transmitted data is protected against the risk of loss, theft, damage and/or any other unauthorized alterations;

42) ”conversion” means translation of a document from one form into another in such a manner as to preserve the document content;

43) ”digitalization” means the conversion of a document from a form that is not electronic into an electronic form;

44) ”digitalized document” means a document created by means of digitalization of the original document;

45) ”conformity assessment body” means a body authorized to carry out conformity assessment of a provider of qualified service and the qualified trust services it provides with the requirements for the provision of qualified trust services.

All terms used in this law in the male gender include the same terms in the female gender.

Application

Article 3.

A trust service provider shall provide trust services in accordance with this Law.

The provisions of this Law shall not apply to trust services provided within a exclusively closed system and/or a limited circle of participants that may be determined by agreement, internal act or regulation, and which have no effect on third parties, or do not bind third parties outside of that system.

Data processing and protection

Article 4.

A trust service and/or electronic identification service provider shall, when processing personal data, act in accordance with the law governing the protection of personal data.

Within the framework of an electronic transaction, the parties may use a pseudonym if it is not otherwise specified by regulation, contract, or in another binding manner.

Consent to identification and authentication

Article 5.

The electronic identification and authentication procedure may be initiated only at the request of a legal or natural person that is the subject of the identification, unless otherwise specified by law.

Accessibility and access for people with disabilities

Article 6.

Trust services, electronic identification services and products used to provide these services shall be equally accessible to persons with disabilities.

II ELECTRONIC DOCUMENT

Legal effects and probative force of electronic document

Article 7.

An electronic document shall not be denied legal effect, probative force, and written form solely on the grounds that it is in electronic form.

Creating an electronic document

Article 8.

An electronic document shall be created using one of the available and usable information and communication technologies, unless otherwise provided by law.

An electronic document representing archival material shall be produced in a form that meets the requirements prescribed by this Law for reliable preparation for electronic storage.

Electronic document display form

Article 9.

An electronic document shall contain an internal and external display form.

The internal display form shall consist of a technical and program form of recording the content of the electronic document.

The external display form shall consist of a visual or other understandable display of the content of the electronic document.

If the document contains an electronic signature or an electronic seal, this fact should be clearly stated in the external form of the electronic document.

If the electronic document contains an electronic signature or seal of a natural person or an authorized person of a legal entity, any other form of the signature or seal of the same natural person or authorized person of a legal entity is unnecessary.

Original and copy

Article 10.

An electronic document originally created in electronic form shall be considered to be an original.

An electronic document that has the same digital signature as an original electronic document shall be considered to be an original.

A paper copy of an electronic document shall be made by printing the external form of the electronic document.

An electronic document created by digitizing a source document whose form is not electronic shall be considered to be a copy of the source document.

Certification of a digitized act

Article 11.

A digitized act shall have the same probative force as the original act, if the following conditions are cumulatively fulfilled:

1) the digitization of the act was carried out in one of the following ways, and/or under the supervision of:

(1) a natural person or an authorized person of a natural person in the capacity of a registered entity, or an authorized person of a legal entity whose act this is, or

(2) a person authorized to verify signatures, manuscripts and transcripts in accordance with the law governing certification of signatures, manuscripts and transcripts, or

(3) a person authorized by a special law to verify a digitized act;

2) the identity of the digitized act with the original was confirmed with a qualified electronic seal or a qualified electronic signature of the person from the sub-item (1) - (3) of this paragraph, or the person to whom the competencies, under which the act was adopted, were transferred.

An authorized person of the public sector body may, in the procedures conducted in the exercise of public authority, digitize the act and certify it with the qualified electronic seal of the body or with their qualified electronic signature, which confirms the identity of the digitized act with the original document.

A digitized act certified by the body referred to in paragraph 2 of this Article shall have the same probative force as the original in the course of the implementation of that procedure.

Certification of a printed copy of an electronic document

Article 12.

A printed copy of an electronic document shall have the same probative force as the original act, if the following conditions are cumulatively fulfilled:

1) printing of an electronic document was carried out under the supervision of:

(1) a natural person, an authorized person of a natural person representing a legal person, and/or an authorized person of a legal entity whose act this is, or

(2) a person authorized to verify signatures, manuscripts and transcripts in accordance with the law governing certification of signatures, manuscripts and transcripts;

2) the identity of the electronic document printed copy with the original was confirmed, indicating that it is a printed copy of the electronic document by:

(1) personal signature of a natural person, or

(2) personal signature of an authorized person of a natural person representing a legal person, or an authorized person of a legal person, as well as by a seal of a natural person representing a registered entity or a legal person, if there is a legal obligation for the act to contain a seal;

(3) a person authorized to verify signatures, manuscripts and transcripts in accordance with the law governing certification of signatures, manuscripts and transcripts.

An authorized person of a public sector body may, in the procedures conducted in the exercise of public authority, print an electronic document on paper and certify the printed copy of the electronic document in the

manner referred to in paragraph 1, item 2), sub-item (2) of this Article, whereby the printed copy of an electronic document must contain a seal determined by the law regulating the seal of state and other bodies.

A printed copy of an electronic document, certified by the body referred to in paragraph 2 of this Article, shall have the same probative force as the original in the course of the implementation of that procedure.

Certificate of receipt of an electronic document

Article 13.

The certificate of receipt of an electronic document shall be a proof that the document was received by the recipient.

The certificate of receipt of an electronic document shall be issued by the recipient of an electronic document or the provider of the electronic registered delivery service.

The obligation to issue the certificate of receipt of an electronic document, and the elements of the content of the certificate shall be regulated by regulations or by the will of the parties, unless otherwise provided by law.

Duplication of electronic documents

Article 14.

Each received electronic document shall be considered a separate document, unless the identical document has been received multiple times and the recipient knew or had to know that it was an identical document.

Electronic communication and electronic delivery between public authorities and parties

Electronic communication and electronic delivery between public authorities and parties

Article 15.

Electronic communication and electronic delivery between public authorities and parties is performed in accordance with the law governing the general administrative procedure, the law governing the electronic administration and other regulation, as well as via the service of qualified electronic delivery.

Delivery of electronic documents between public sector bodies

Article 16.

The delivery of electronic documents between the public sector bodies shall be performed by e-mail, service bus of the body, qualified electronic registered delivery service, or other electronic means, in accordance with the regulation.

III ELECTRONIC IDENTIFICATION

1. Electronic identification schemes

Conditions that must be met by an electronic identification scheme

Article 17.

The electronic identification scheme must:

1) include data for identification of persons on the issued identification means, which uniquely identify a legal or natural person;

2) ensure that the electronic identification service provider means provides identification data within the electronic identification means that correspond to the person to whom the means was issued;

3) clearly define the technical and other conditions that enable a relying party to verify the identity;

4) conditions to be met by service provider of electronic identification;

Reliability levels of electronic identification schemes

Article 18.

Electronic identification schemes shall be classified according to the assurance level to:

1) the assurance level low schemes, which provide a limited degree of confidence in the identity that a person uses, and use the means and procedures the purpose of which is to reduce the risk of abuse or false impersonation;

2) the assurance level substantial schemes, which provide a substantial degree of confidence in the identity that a person uses, and use the means and procedures the purpose of which is to decrease substantially the risk of misuse or false impersonation;

3) the assurance level high schemes, which provide a higher degree of confidence in the identity that a person uses, and use the means and procedures the purpose of which is to prevent misuse or false impersonation;

At the proposal of the ministry responsible for information society (hereinafter: the Ministry), the Government shall regulate closer conditions that the electronic identification schemes must fulfill for certain levels of reliability, and in particular:

1) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;

2) the procedure for the issuance of the electronic identification means;

3) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to another party in an electronic transaction;

4) the conditions to be fulfilled by the service provider of the electronic identification means;

4a) conditions relating to the data used in the process of cross-border cooperation for natural and legal persons for the use of registered schemes of electronic identification which, out of personal data, include the name, date of birth, address, and sex, for the purpose of reliable identification check of the person in question.

5) the conditions to be fulfilled by any other body involved in the application for the issuance of the electronic identification means;

6) the technical and security specifications of the issued electronic identification means;

7) minimum technical and organizational conditions in order to ensure the interoperability of the electronic identification schemes in accordance with national and international standards in this field.

Entry in the Register of electronic identification service providers and electronic identification schemes

Article 19.

Register of electronic identification service providers and electronic identification schemes presents a set of data on electronic identification service providers and electronic identification schemes, headed by the ministry.

The electronic identification service provider submits a request and necessary documentation to the ministry for entry in the register of electronic identification service providers and electronic identification schemes.

The register referred to in paragraph 1 of this article on personal data contains data about responsible persons, as follows: name, surname, function and contact data such as official address, official telephone number, official electronic email address, for the purpose of the availability of data to service users, on the electronic identification service provider.

An integral part of the register referred to in paragraph 1 of this article are also electronic identification schemes from the list published by the european commission, in accordance with article 9 of the eidas regulation.

The ministry prescribes the content and manner of upkeeping the register referred to in paragraph 1 of this article, as well as the manner of submitting requests for entry in that register, in accordance with the law regulating the general administrative procedure, the needed documentation with a request, a request form, and the way the data from this register is to be published.

Use of electronic identification schemes in electronic business and in communication with the public sector body

Article 20.

The electronic identification schemes registered in the Register referred to in Article 19 of this Law, as well as electronic identification schemes that are not registered in the Register, can be used to establish identity in electronic business.

A statement of will can not be challenged only because electronic identification schemes from paragraph 1 of this Article were used instead of signature.

The electronic identification scheme registered in the Register referred to in Article 19 of this Law (hereinafter: registered electronic identification scheme) may be used to determine the identity of a party in communication with a public sector body.

In the party's communication with the public sector body, the identity of the party established on the basis of a registered electronic identification scheme of high reliability level shall replace the party's signature on the submission.

The regulation may stipulate that, in the case referred to in paragraph 4 of this Article, an electronic identification scheme of medium or basic reliability level may be used if the risk of abuse and possible damage from abuse are such that it is not necessary to use high reliability level scheme.

Liability in electronic identification

Article 21.

The entity issuing the electronic identification means shall be liable for the damage arising because the identification means was not issued in accordance with the electronic identification scheme that meets the requirements of Article 17 of this Law.

The damage caused by incorrectly conducted authentication procedure is the responsibility of the party conducting the procedure if the damage was caused intentionally or negligently.

Security conditions to be met by electronic identification service providers

Article 22.

Electronic identification service providers shall undertake the necessary technical, physical and organizational measures to manage risks that jeopardize the reliable and secure provision of these services.

The technical and organizational measures shall ensure that the level of security corresponds to the level of risk and the predicted level of reliability of the electronic identification scheme, taking into account the latest available technological solutions, and in particular, the measures shall be taken to prevent security incidents and to limit the harmful effects of possible incidents, as well as to inform stakeholders about unwanted effects of security incidents.

2. Cross-border cooperation in the field of electronic identification

Interoperability of technical systems

Article 23.

The Ministry shall cooperate with relevant international bodies on issues of cross-border interoperability of the electronic identification schemes, and shall take measures within its jurisdiction in order to establish the highest level of interoperability of the electronic identification on a national level.

Cross-border interoperability of registered schemes of electronic identification is achieved via the establishment of nodes, which provide cross-border identification of faces, thus insuring that the infrastructure of electronic identification of one country is connected to the identification infrastructure of another country.

The node is established and managed by the government service responsible for design, development, construction, maintenance and improvement of the computer network of the authorities of the republic.

In the node management process, the authority referred to in paragraph 3 of this article is obligated to:

1) provide connection with nodes of other states whose electronic identification schemes are an integral part of the register referred to in article 19 of this law, or which are recognized on the basis of an international agreement;

2) apply protective measures to prevent unauthorized access to data exchanged and ensure the integrity of data transmitted between nodes using appropriate technical solutions and practice;

3) ensure that personal data is not stored in the node;

4) uses technical solutions that provide integrity and authenticity of data, which are used when cross-border connecting nodes;

5) ensure that the node meets the prescribed conditions regarding the message format;

6) enable the submission of metadata on node management in a standard form suitable for automatic data processing, in a safe and reliable way;

7) provide automatic processing of security parameters;

8) keeps data which, in the event of an incident, would allow the determination of the place and type of incident within the legal deadline.

9) ensure the transmission of data providing reliable representation of a natural or legal entity, based on the use of a registered electronic identification scheme for cross-border compartments, in accordance with the law.

By the government's regulation from article 18, paragraph 2 of this law, the conditions from article 3, item 5), 8), and 9) of this article are more closely determined, referring to the node.

Reporting

Article 24.

The Ministry may report to the European Commission the registered electronic identity schemes that meet the requirements of the EU Regulation no. 910/2014 of the European Parliament and of the Council (hereinafter: the eIDAS Regulation).

IV TRUST SERVICES

1. General Provisions

Liability of trust service providers and burden of proof

Article 25.

Trust service provider shall be liable for damage resulting from failure to act in accordance with this Law if the damage was caused intentionally or negligently.

The burden of proving intention or negligence of a trust service provider shall lie with the natural or legal person claiming the damage referred to in paragraph 1 of this Article.

The burden of proving that the damage was not incurred as a result of intention or negligence of a qualified trust service provider referred to in paragraph 1 of this Article shall lie with that service provider.

A trust service provider shall not be liable for damages arising from the use of service exceeding the indicated limitation if the trust service user is duly informed in advance of such limitations.

Responsibility of trust service users for protection of means and data used for creation of an electronic signature or seal

Article 26.

The trust service user shall be obliged to protect the means and data used to create an electronic signature or seal from unauthorized access and use, and to use them in accordance with the provisions of this Law.

Security conditions to be met by trust service providers

Article 27.

Trust service providers, including qualified trust service providers, shall undertake the necessary technical and organizational measures to manage risks that jeopardize the reliable and secure provision of these trust services.

The technical and organizational measures shall ensure that the level of security corresponds to the level of risk, taking into account the latest available technological solutions, and in particular, the measures shall be taken to prevent security incidents and to limit the harmful effects of possible incidents, as well as to inform stakeholders about unwanted effects of security incidents.

Trust service providers, including qualified trust service providers, without delay, and no later than within 24 hours of becoming aware of it, shall notify the Ministry of any security breaches or loss of integrity of the service that have a significant impact on the provision of trust services.

If compromising the security or losing the integrity of a trust service could adversely affect the trust service users, the trust service provider shall inform, without delay, the trust service user about the breach of security or the loss of integrity of the service.

The Ministry shall inform the public or request the trust service provider to do so if it finds that disclosure of data on security breach or loss of integrity of the service is in the public interest.

The Ministry shall cooperate with relevant institutions in other countries regarding the exchange of information on security and integrity breaches, in accordance with the relevant ratified international agreements.

Responsibility of the Ministry

Article 28.

The Ministry shall perform the following tasks:

1) keep the Register of the qualified trust service providers;

2) consider the reports on the fulfillment of conditions for the provision of qualified trust services;

3) perform inspection supervision over the work of a trust service provider;

4) order an extraordinary check of the fulfillment of conditions for the provision of qualified trust services, in accordance with the law;

5) cooperate with the competent personal data protection authority and inform it without delay if it finds out that the qualified trust service providers do not comply with the regulations on personal data protection;

6) verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information, issued and received by a qualified trust service provider, is kept accessible;

7) cooperate with the supervisory bodies referred to in Article 17 of the eIDAS Regulation;

8) inform the public of the security breach or the loss of integrity of trust services that have a significant impact on the provided trust service or the personal data contained therein.

Competencies of the Ministry in the framework of cross-border cooperation in the field of trust services

Article 29.

The Ministry shall also carry out the following tasks:

1) inform the competent authorities in the foreign countries of the security breach or the loss of integrity that have a significant impact on the provided trust service or the personal data contained therein.

2) report to the European Commission on its activities in accordance with the eIDAS Regulation, starting from the date of entry of the Republic of Serbia into the European Union.

2. General Provisions on Qualified Trust Services

Establishing the relationship between the qualified trust service provider and user

Article 30.

A contract on qualified trust service provision between the qualified trust service provider and user shall be concluded at the request of the user.

The qualified trust service provider shall, before concluding the contract referred to in paragraph 1 of this Article, notify the person who submitted the request for qualified trust service provision about all important circumstances of the use of the service, in particular:

1) regulations and rules relating to the use of a qualified trust service;

2) any limitations on the use of a qualified trust service;

3) the measures to be implemented by users of a qualified trust service, and the necessary technology for safe use of qualified trust services.

The user of a qualified trust service may use the trust services of one or more trust service providers.

The conditions for the provision of qualified trust services

Article 31.

A qualified trust service provider must:

1) employ staff who possess the necessary expertise, experience, and qualifications to apply administrative and management procedures which correspond to national and international standards, and who have received appropriate training regarding information security and personal data protection;

2) be insured against liability for damages resulting in the performance of a qualified trust service;

3) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;

4) use trustworthy systems to store data provided to it, so that:

(1) they are publicly available only where the consent of the person to whom the data relates has been obtained,

(2)only authorized persons can make entries and changes to the stored data,

(3) the data can be checked for authenticity;

5) take appropriate measures against forgery and theft of data;

6) keep accessible for an appropriate period of time all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings. Such recording may be done electronically;

7) keep updated, accurate and protected by safe measures database of issued electronic certificates in the case when it provides the service of issuing qualified electronic certificates, as well as the database that was created or received by the providers of trust qualified services as a part of providing trust qualified services;

8) have an up-to-date termination plan to ensure continuity of qualified trust services;

9) ensure processing of personal data in accordance with the laws of the Republic of Serbia.

A qualified trust service provider shall be obliged to adopt acts determining:

1) the general conditions for the provision of service that are publicly available;

2) service policies and practical rules for the provision of services that the qualified trust service provider uses to ensure the provision of service in accordance with the regulations and general conditions referred to in item 1) of this paragraph.

On the proposal of the Ministry, the Government shall more closely regulate the conditions for the qualified trust service provision referred to in paragraph 1 of this Article, and the content of the acts referred to in paragraph 2 of this Article, including determining the international standards that apply.

3) information security.

Providers of trust services who issue qualified electronic certificates are obliged to submit to the ministry data on the number of certificates issued from the beginning of the service until December 31 of the calendar year, as well as the data on the number of valid certificates on December 31 of the calendar year.

Updated data referred to in paragraph 3 of this article will be submitted regularly, no later than January 15 for the previous year, as well as if necessary as an exception, at the request of the ministry.

Professional liability insurance

Article 32.

The Ministry shall prescribe the lowest amount of insurance against the risk of liability for damages arising from the performance of a qualified trust service;

Identity verification of a qualified trust service user

Article 33.

When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify the identity information of the natural or legal person, contained in the qualified certificate, in accordance with the law.

The information referred to in paragraph 1 of this Article shall be verified by the qualified trust service provider:

1) by the physical presence of the natural person or of an authorized representative of the legal person or

2) remotely, by the public document serving as identification means, in accordance with the law, or

3) by manner of remote identification, in accordance with the law.

Verification of data referred to in paragraph 2 of this article will be performed in the manner regulated by the regulation referred to in article 31 of this law, which regulates the conditions for providing a qualified trust service.

Assessment of the fulfillment of requirements for the provision of qualified trust services

Article 34.

Assessment of the fulfillment of requirements for the provision of qualified trust services (hereinafter: assessment of the fulfillment of requirements) shall be performed by the conformity assessment body which, in accordance with the law governing accreditation, shall be accredited to assess the conformity of the qualified trust service provider and the qualified trust services they provide.

After completing the assessment of the fulfillment of requirements, the conformity assessment body shall make a conformity assessment report.

Assessment of the fulfillment of requirements shall be made before the beginning of the provision of qualified trust services, and at least once in 24 months.

Upon completing the assessment of the fulfillment of requirements, the trust service provider shall submit to the Ministry the conformity assessment report, within three working days from the day it was received.

The Ministry may order an extraordinary assessment of the fulfillment of requirements if irregularities were identified in the provision of qualified trust services, or if an incident occurred that significantly jeopardized or violated information security.

The extraordinary assessment of the fulfillment of requirements shall be performed by the conformity assessment body that is not associated with the performance of a prior assessment.

The cost of the assessment of the fulfillment of requirements, including extraordinary assessments, shall be borne by the qualified trust service provider.

The Ministry shall determine the list of standards that must be fulfilled by the conformity assessment body, the mandatory content of the conformity assessment report, and the procedure for assessing the fulfillment of requirements and/or assessing the conformity of qualified trust services.

Entry in the register of providers of qualified trust services

Article 35.

The register of providers of trust qualified services is a set of data on the providers of trust qualified services, and trust qualified services themselves, which is managed by the ministry.

A qualified trust service provider shall submit a request to the Ministry for registration in the Register of qualified trust service providers.

A qualified trust service provider must be registered in the Register referred to in paragraph 1 of this Article before commencing the provision of qualified trust services.

The request referred to in paragraph 1 of this Article shall be accompanied by evidence of the facts stated in the request, including the conformity assessment report referred to in Article 34, paragraph 4 of this Law, stating that the applicant and the qualified trust services they intend to provide fulfill the requirements of this law.

The Ministry shall decide on the registration of the qualified trust service provider in the Register referred to in paragraph 1 of this Article, within 60 days from the date of submission of a proper request.

In the decision process referred to in paragraph 4 of this Article, the Ministry may request additional evidence, as well as additional verification of technical and safety components and operational work.

If the service provider ceases to fulfill the requirements prescribed by this Law, the Ministry shall issue a decision on its deletion from the Register referred to in paragraph 1 of this Article.

The register referred to in paragraph 1 of this article from personal data contains the following data about responsible persons: name, surname, function and contact information such as official address, official telephone number to official email address for the purpose of availability of information about the provider of the trust qualified service, with which the service contract is concluded.

The Ministry shall prescribe the content and method of keeping the Register referred to in paragraph 1 of this Article, the manner of applying for entry into the Register referred to in paragraph 1 of this Article, in accordance with the law regulating the general administrative procedure, the necessary documentation required with the application, the application form and the method of checking the fulfillment of requirements for provision of qualified trust service.

Termination of the service of issuing qualified electronic certificates

Article 36.

An issuer of qualified electronic certificates, who intends to cease its activities, shall be obliged to notify each qualified trust service user and the Ministry about the intention to terminate the contract, at least three months before the intended end of the performance of the activities.

The issuer of qualified electronic certificates, who intends to cease its activities, shall be obliged to provide continuation of the service with another trust service provider for the qualified trust service users who were issued the certificate, and if there is no possibility for that, it shall be obliged to revoke all issued certificates and immediately inform the Ministry of the measures taken.

The issuer of qualified electronic certificates shall be obliged to submit all documentation and necessary technical means connected with the performance of the trust services to another issuer to whom it shall transfer the obligations of performing one or more trust services.

If the issuer of qualified electronic certificates fails to comply with paragraph 3 of this Article, it shall be obliged to submit all documentation to the Ministry that will execute the revocation of all certificates, without delay, at the expense of the issuer of qualified electronic certificates.

In the case of a temporary prohibition of provision of services, the certificates issued as of the date of the occurrence of the cause the measure of prohibition was imposed, shall remain valid.

Use of qualified electronic certificates and qualified electronic time stamps in public authorities' software solutions

Article 36a

The government authority is obliged to, in providing services of electronic administration in accordance with the law regulating government software solutions, allow the use of qualified electronic certificates and qualified electronic time stamps issued by all providers of trust electronic services, entered into the register from article 35 of this law.

State body as a provider of qualified trust services

Article 37.

A state authority may provide trust qualified services if it meets the conditions for providing services specified in this law.

Assessment of the fulfillment of the conditions of the state authority for the provision of trust services is performed by the ministry, or inspector for electronic identification and trust services, after the submitted request.

Notwithstanding paragraph 2 of this article assessing whether the conditions shall be based on internal control of cooperation with relevant ministries only when the qualified trust service provider is the ministry, in charge of defense, with the obligation to submit a report on the completed internal control, to the relevant ministry.

After checking whether or not the conditions are fulfilled, the government decides by decree that the state authority may perform a qualified trust service which was subject to the assessment referred to in paragraph 2 of this article.

The ministry makes an entry of the state authority in the register referred to in article 35 of this law, on the basis of the regulation referred to in paragraph 4 of this article.

Public list of qualified trust services

Article 38.

The public list of trust qualified services provides a reliable piece of information automatically to reliable parties, regarding the status of the provider of trust qualified services and their qualified services in accordance with the data entered into the register from article 35 of this law.

Public list of qualified services trust contains information on relevant past events concerning the status of current and former providers and their services over time, including information on the beginning of the offering, the loss of integrity of trust services, the temporary ban, the termination of services deregistration, and other events recorded in the framework of register maintenance, inspection supervision or events reported by the provider, which affect the acceptability of a trust qualified service and the procedure of determining its status at a certain time.

In the public list of trust qualified services, data from paragraph 1 and 2 of this article as well as other information determined by the regulation of the ministry referred to in paragraph 6 of this article and the relevant standards.

The providers of trust qualified services are obliged to at the request of the ministry, within seven days, submit the information referred to in paragraph 3 of this article, as well as to notify the ministry without delay of any change in data referred to in paragraph 3 of this article.

Information on the certificate supporting the signature of the public list of trust qualified services, including sha-256 impression, is published in the "official gazette of the republic of serbia."

The ministry prescribes technical requirements, form, and manner of publication of the list of trust qualified public services, and the conditions which the ministry is authorized to publish, the public lists of qualified trust services must be provided while it is formed, signed, and published.

Form and manner of publishing the public list of qualified trust services referred to in paragraph 6 of this article should be compliant with the technical requirements for the trust lists referred to in article 22 of the eidas regulation.

Trust mark for the qualified trust services

Article 39.

Trust mark for the qualified trust services (hereinafter: Trust mark) is a sign that indicates in a simple, recognizable and clear manner the qualified trust services.

Registered qualified trust service providers have the right to use the Trust mark for the qualified trust services they provide.

The Trust mark referred to in paragraph 1 shall be used until the entry of the Republic of Serbia into the European Union. The Ministry shall prescribe the appearance, composition, size and design of the Trust mark for the qualified trust services.

Cross-border recognition of qualified trust services

Article 40.

A qualified trust service provided by a foreign trust service provider shall be in reciprocity with a domestic trust service in a country of a foreign service provider, which shall be governed by a validated international agreement.

V INDIVIDUAL TYPES OF TRUST SERVICES

Types of services

Article 41.

Trust services shall be provided in the following areas:

1) electronic signature and electronic seal;
2) electronic time stamp;
3) electronic registered delivery;
4) website authentication;
5) electronic document preservation.

Qualified trust services are:

1) issuing qualified electronic signature certificates;
2) qualified electronic signature creation device management service remotely;
3) qualified electronic signature validation service;
4) issuing qualified electronic seal certificates;
5) qualified electronic seal creation device management service remotely;
6) qualified electronic seal validation service;
7) issuing qualified electronic time stamps;
8) qualified electronic registered delivery service;
9) issuing qualified certificates for website authentication;
10) qualified electronic document preservation service.

A trust service provider or a qualified trust service provider may provide one or more services from paragraph 1 and 2 of this Article.

1. Electronic signature and electronic seal

Advanced electronic signature and advanced electronic seal

Article 42.

Advanced electronic signature and/or advanced electronic seal must meet the following requirements:

1) it is uniquely linked to the signatory and/or the creator of the seal;
2) it is capable of identifying the signatory and/or the creator of the seal;
3) it is created using electronic signature/seal creation data that the signatory/creator of the seal can, with a high level of confidence, use under its sole control;
4) it is linked to electronically signed/sealed data in such a way that any subsequent change in the data is detectable.

Content of a qualified electronic certificate

Article 43.

Qualified electronic certificate shall contain:

1) an indication, in a form suitable for automated processing, that the electronic certificate has been used as a qualified certificate for electronic signature/seal;

2) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic certificates including at least the country of origin of the provider and the name of the provider;

3) a set of data unambiguously representing the signatory/creator of the seal, including at least:

(1) for the signatory:

- name and surname or pseudonym, and if the pseudonym is used, it must be clearly marked within the qualified electronic certificate;
- Personal identity number, if, in the application for the issue of the certificate, the signatory has requested the certificate to contain the personal identity number;

(2) for the creator of the seal: name, state and registration number, or unique identification mark in accordance with the legal regulations of the state, if any;

4) electronic signature/seal validation data, which corresponds to the electronic signature/seal creation data;

5) details of the beginning and end of the qualified electronic certificate"s period of validity;

6) the qualified electronic certificate serial number, which must be unique within the issuer of the qualified electronic certificate;

7) the advanced electronic signature or advanced electronic seal of the issuer of the qualified electronic certificate;

8) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point 7) of this Article is available free of charge;

9) the location of the service that can be used to enquire as to the validity status of the qualified electronic certificate;

10) an appropriate indication that the electronic signature/seal creation data related to the electronic signature/seal validation data from the qualified electronic certificate, is located in a qualified electronic signature/seal creation device, if this requirement is fulfilled.

The qualified electronic certificates, in addition to the indication referred to in paragraph 1 of this Article, may include additional attributes. The Ministry shall prescribe more precisely the requirements that must be met by the qualified electronic certificates referred to in paragraph 1 of this Article.

Revocation and suspension of a qualified electronic certificate

Article 44.

The issuer of the qualified certificates shall be obligated to revoke the issued certificates when:

1) the certificate revocation is requested by the owner of the certificate or their proxy;

2) the owner of the certificate loses its legal capacity, or has ceased to exist, or the circumstances that significantly affect the validity of the certificate have changed;

3) it finds that the data in the certificate is incorrect;

4) it determines that the data for the qualified electronic signature/seal validation, or the system of the qualified trust service providers are endangered in a manner that affects the security and reliability of the certificate;

5) it determines that the data for electronic signing/sealing, or the system of the certificate owner are endangered in a manner that affects the reliability and security of the electronic signature;

6) it has stopped working or its work has been prohibited.

The issuer of the qualified certificates shall be obliged to inform the qualified trust service user about the revocation of the certificate within 24 hours of the received notification, or of the occurrence of the circumstances for which the certificate is revoked.

A qualified trust service user shall be obliged to immediately request the revocation of their qualified electronic certificate in case of loss or damage to the certificate creation devices or data.

In the case of revocation, the qualified electronic certificate shall cease to be valid from the moment of revocation.

In the case of suspension, the qualified electronic certificate shall lose its validity during the suspension period.

The data on suspension and on duration of the suspension of a qualified electronic certificate shall be entered in the database of issued certificates maintained by the issuer of the qualified electronic certificates, and they must be visible during the suspension within the services providing information on the status of the certificate.

Preservation of documentation on issued and revoked qualified certificates

Article 45.

The issuer of qualified electronic certificates shall be obliged to preserve complete documentation on issued and revoked qualified electronic certificates as a means of proofing and verification in administrative, judicial and other proceedings, at least ten years after the expiration of the certificate validity.

The data referred to in paragraph 1 of this Article may be preserved in electronic form.

Qualified electronic signature/seal creation devices

Article 46.

A qualified electronic signature or seal creation device must, by means of appropriate technical solutions and procedures, provide:

1) confidentiality of electronic signature and/or seal creation data;

2) that the electronic signature and/or seal creation data appear only once;

3) that the electronic signature and/or seal creation data can not be obtained outside the electronic signature or seal creation devices using the available technology in a reasonable time;

4) that the electronic signature and/or seal is reliably protected against forgery using the available technology;

5) the possibility of reliable protection of electronic signature and/or seal creation data against unauthorized use.

The qualified electronic signature or seal creation devices, when creating an electronic signature or seal, must not change the signed or sealed data, or disable the signatory or the creator of the seal to access the data before the process of the qualified electronic signature or seal creation.

The qualified electronic signature or seal creation device may be used by the qualified trust service user through a qualified electronic signature or seal creation device management service, remote (hereinafter: remote qualified asset management service), which also constitutes a qualified trust service.

Notwithstanding paragraph 1 of this Article, an eligible trust service provider referred to in paragraph 3 of this Article may create a copy of data for the electronic signature or seal creation, for the purpose of protecting against loss of data if:

1) the creation and preservation of the copies of the qualified electronic signature or seal creation data do not reduce the prescribed level of protection of such data;

2) the number of created copies for the electronic signature or seal creation is no greater than necessary to ensure the continuity of the service provision.

The Ministry shall prescribe more precisely the requirements that must be fulfilled by the qualified electronic signature or seal creation device.

Certification of qualified means for creating an electronic signature or stamps and entry in the register of qualified means for creating electronic signatures and electronic stamps

Article 47.

In accordance with the law regulating the technical requirements for products and the assessment of conformity, the ministry appoints a body for the assessment of the conformity with the means for the creation of a qualified electronic signature i.e. stamp (hereinafter: designated body), which performs the assessment of conformity in accordance to the regulation from article 46 of this law.

The regulation referred to in article 46 of this law regulates in details of the conditions which must be fulfilled by the designated body.

The register of qualified means for creating electronic signatures and electronic stamps is a set of data on qualified means for creating electronic signatures and electronic stamps.

The request for entry in the register referred to in paragraph 3 of this law shall be submitted to the ministry, on the basis of the report received from the designated bodies.

The designated body, without delay, and no later than seven days from the change, shall notify the ministry of issued and withdrawn certificates of the conformity of assets for the creation of electronic signatures, i.e. stamps.

An integral part of the register referred to in paragraph 3 of this article are also qualified means for creating an electronic signature and electronic stamp from the list which, in accordance with article 31 of the eIDAS regulation, is published by the European Commission

For qualified means for creating electronic signatures and electronic stamps referred to in paragraph 6 of this article, no request for entry into the register of qualified means for creating electronic signatures shall be submitted.

The ministry prescribes the content and manner of keeping the register referred to in paragraph 3 of this article, the manner of submitting requests for entry into the register in accordance with the regulations governing the general administrative procedure, the needed documentation, along with a request and a request form.

Qualified electronic signature and qualified electronic seal validation process

Article 48.

The process for the validation shall confirm the validity of a qualified electronic signature provided that:

1) it has been determined that the certificate that supports the electronic signature was, at the time of signing, a qualified certificate for electronic signature;

2) it has been determined that the qualified electronic certificate was issued by a provider of qualified certificate for electronic signature and was valid at the time of signing;

3) it has been determined that the electronic signature validation data from the qualified electronic certificate corresponds to the combination of electronic signature and data signed with the electronic signature;

4) the unique set of data representing the signatory in the qualified electronic certificate is correctly provided to the relying party;

5) the data signed using electronic signature is accurately displayed to the relying party;

6) the use of pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

7) it has been determined that the electronic signature was created by a qualified electronic signature creation device;

8) it has been determined that the integrity of the signed data has not been compromised;

9) it has been determined that the electronic signature meets the requirements for the advanced electronic signature under this Law.

The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

The provisions of paragraphs 1 and 2 of this Article shall be applied accordingly to the electronic seal.

The Ministry shall prescribe more precisely the requirements for the qualified electronic signature and qualified electronic seal validation process.

Qualified validation service for qualified electronic signatures and qualified electronic seals

Article 49.

A provider of a qualified validation service for qualified electronic signatures and qualified electronic seals shall provide:

1) validation of a qualified electronic signature/seal in accordance with Article 48 of this Law;

2) that the relying party using the service receives the result of the validation process electronically, in an automated manner, which is reliable and efficient;

3) that the result of the validation process from item 2) of this paragraph bears the advanced electronic seal or advanced electronic signature of the provider of the service.

The Ministry shall prescribe more precisely the requirements for providing the service of qualified validation of qualified electronic signatures and qualified electronic seals.

Legal effect of electronic signature

Article 50.

An electronic signature shall not be denied legal effect and probative force solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

A qualified electronic signature may replace the authentication of a handwritten signature, if prescribed by a special law.

The provisions of paragraphs 1 and 2 of this Article shall not apply to legal affairs for which a special law provides that they shall not be undertaken in electronic form.

Contracts and other legal affairs which are specifically envisaged by the special law to be drafted in the form of authentication of signatures, publicly certified (notarized) documents, or in the form of a public notary record shall not be made in accordance with paragraphs 1 and 2 of this Article, but in accordance with the regulations governing the authentication of signatures, validation and drafting of documents on legal affairs.

Legal effect of electronic seal

Article 51.

An electronic seal shall not be denied legal effect and probative force solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seal.

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.

A public body act adopted in the exercise of its public authorities in the form of an electronic document shall contain the qualified electronic seal of that body instead of the seal, or the signature and seal of the official or a qualified electronic signature of an authorized person of the public authority.

A qualified electronic seal on a submission in the procedure that public bodies perform in exercising their public authority in the form of an electronic document, shall have the same legal effect as a handwritten signature, or seal.

The provisions of paragraphs 1-4 of this Article shall not apply to legal affairs for which a special law provides that they shall not be undertaken in electronic form.

Contracts and other legal affairs which are specifically envisaged by the special law to be drafted in the form of authentication of signatures, publicly certified (notarized) documents, or in the form of a public notary record shall not be made in accordance with paragraphs 1-4 of this Article, but in accordance with the regulations governing the authentication of signatures, validation and drafting of documents on legal affairs.

2. Electronic Time Stamp

Requirements for qualified electronic time stamps

Article 52.

A qualified electronic time stamp shall meet the following requirements:

1) it is linked to Coordinated Universal Time (UTC) in such a manner as to preclude any possibility of the data being changed undetectably;

2) it is based on an accurate time source;

3) it is issued by the provider issuing the qualified time stamp;

4) it is signed/sealed by the provider issuing the qualified time stamp using an advanced electronic signature or an advanced electronic seal.

The Ministry shall prescribe detailed requirements for qualified electronic time stamps.

Legal effect of electronic time stamp

Article 53.

An electronic time stamp shall not be denied legal effect and probative force solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic time stamp.

A qualified electronic time stamp and the data to which that time stamp is linked shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

3. Electronic registered delivery

Requirements for qualified electronic registered delivery services

Article 54.

Qualified electronic registered delivery services shall meet the following requirements:

1) they are provided by one or more qualified trust service provider(s);

2) they ensure with a high level of confidence the identification of the sender;

3) they ensure the identification of the addressee when delivering the data;

4) in the process of sending and receiving the electronic message, it uses an advanced electronic signature or an advanced electronic seal of a qualified electronic registered delivery service provider in such a manner as to preclude the possibility of the data being changed undetectably;

5) to ensure that 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;

6) to ensure that the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp;

7) in the event of the data being transferred between two or more qualified electronic registered delivery service providers, to ensure that the requirements in this paragraph apply to all of them.

Certificate of electronic delivery

Article 55.

The service provider is obliged to issue two confirmations to the sender when providing the qualified electronic delivery service, as follows:

1) confirmation that he received the sender's electronic message and forwarded to the recipient;

2) confirmation that the recipient has accepted the delivered electronic message.

The certificates referred to in paragraph 1 of this Article shall be delivered automatically by the service provider in an electronic form, signed with an advanced electronic seal, and may be issued in electronic or paper form on request.

The certificate referred to in paragraph 1 items 1) and 2) of this Article shall contain:

1) an identification code of the electronic message provided by the service provider;

2) the information on the sender and the recipient, which may contain personal data referred to in Article 43, paragraph 1, item 3) of this Law, as well as the address for electronic delivery;

3) the data linking the certificate with the contents of the electronic message;

4) date and time of reception and forwarding of the electronic message by the service provider, i.e. date and time of the reception of the delivered electronic message by the recipient.

The certificate referred to in paragraph 1, item 2) of this Article shall be considered as a delivery note in electronic form in terms of the law governing the administrative procedure, where the date and time of the download, referred to in paragraph 3, item 4) of this Article shall be considered as the date and time of delivery.

The date and time of receipt of a submission filed by the party in the administrative procedure to the authority through qualified electronic delivery shall be considered as the date and time of the download referred to in paragraph 3, item 4) of this Article.

If technical problems occur in the electronic delivery or reception of data, the provider of qualified electronic delivery service shall be obliged to inform the sender and the recipient thereof.

The Ministry shall prescribe detailed requirements for qualified electronic delivery services referred to in Article 54 of this Law, and the contents of the certificates referred to in paragraph 3 of this Article.

Exchange of electronic messages between providers of qualified electronic registered delivery services

Article 56.

The qualified electronic delivery service providers are obligated to enable the reception and sending of messages during providing the service of qualified electronic delivery, including the time when the message sender or recipient is the user of another qualified electronic delivery service provider.

The exchange of electronic messages referred to in paragraph 1 of this article will be carried out in the manner regulated by the regulation referred to in article 55 of this law, which regulates the conditions for qualified electronic delivery services.

Legal effect of electronic registered delivery service

Article 57.

Data sent or received using a electronic delivery service shall not be denied legal effect and admissibility as evidence in legal transactions solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic delivery services.

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.

4. Website authentication

Qualified certificates for website authentication

Article 58.

Website authentication shall be used to verify the identity of the website by a qualified trust service users, which guarantees its reliability.

A qualified certificate issued by a qualified trust service provider shall be used for website authentication. The qualified certificate for website authentication must meet the requirements from Article 59 of this Law.

Content of qualified certificates for website authentication

Article 59.

Qualified certificates for website authentication shall contain:

1) an indication, in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;

2) a set of data unambiguously representing the service provider issuing the qualified certificates for website authentication, including at least the headquarters country, business name and registration number of that service provider;

3) for natural persons, the name and surname or a pseudonym of the person to whom the certificate has been issued, or for legal persons, the name and registration number of the person to whom the certificate has been issued;

4) the address, or headquarters of the natural or legal person to whom the certificate is issued;

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

6) details of the beginning and end of the certificate"s period of validity;

7) the certificate identity code, which must be unique for the service provider issuing the qualified certificates for website authentication;

8) the advanced electronic signature or advanced electronic seal of the service provider issuing the qualified certificates for website authentication;

9) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point 8) of this Article is available free of charge;

10) the location of the service that can be used to enquire as to the validity status of the qualified electronic certificate;

5. Electronic preservation of documents

Preparation of documents for electronic preservation

Article 60.

Preparation of documents for electronic preservation refers to:

1) documents originally created in an electronic form suitable for preservation;

2) conversion of a document in a different electronic form suitable for preservation;

3) digitization of a document originally created in a form that is not electronic into a form suitable for preservation.

A document prepared for electronic preservation may include additional information describing the document or derived from the document.

Preparation of documents for trustworthy electronic preservation

Article 61.

Preparation of documents for trustworthy electronic preservation must:

1) ensure that all essential elements of the content of the original document are faithfully transferred to a document prepared for electronic preservation, taking into account the nature and purpose of the document, i.e. the integrity of the content of the document is preserved;

2) ensure that the usability of the content of the original document is preserved;

3) ensure that all elements of the content of the original document, of relevance to authenticity, are included;

4) provide a verification of the authenticity of the original document and the accuracy of the additionally included data by a qualified electronic seal or signature with the associated time stamp;

5) ensure that the control of the accuracy and quality of the conversion is carried out, as well as the elimination of errors arising in the conversion process;

6) ensure that the content updates, entered notes, and data about precautions taken are kept separate from the original documents;

7) ensure that records are kept about undertaken actions in the preparation process for electronic preservation.

If the prescribed deadline for document preservation is longer than five years, the document prepared for preservation should be in a format that is suitable for long-term preservation.

On the proposal of the Ministry, the Government shall regulate the detailed requirements that must be met by a trustworthy preparation of a document for electronic preservation, and the document formats that are suitable for long-term preservation.

Trustworthy electronic preservation of a document

Article 62.

Trustworthy electronic preservation of documents, which originally contain a qualified electronic signature or seal as a confirmation of the integrity and origin of such documents, shall be performed so that during the preservation, the procedures and technological solutions are used which ensure the possibility of proving the validity of the qualified electronic signature or seal during the entire preservation period.

Trustworthy electronic preservation of documents prepared in accordance with Article 61 of this Law, whose authenticity and accuracy of the additionally included data have been verified by a qualified electronic signature or seal referred to in Article 61, paragraph 1, item 4), shall be performed so that the procedures and technological solutions ensuring the ability to prove the validity of a qualified electronic signature or seal are used throughout the entire preservation period.

The Ministry shall prescribe detailed requirements for the procedures and technological solutions referred to in paragraphs 1 and 2 of this Article.

The Ministry responsible for cultural affairs shall regulate the detailed requirements, tasks, activities, standards and processes of digitization of cultural heritage and contemporary art related to the procedures and technological solutions referred to in Art. 61 and 62 of this Law.

Qualified electronic document preservation service

Article 63.

A qualified electronic document preservation service is a qualified trust service through which a trustworthy electronic document preservation shall be provided in accordance with Art. 60-62 of this Law.

A qualified electronic document preservation service provider may opt to limit the qualified electronic document preservation service only to preservation of documents that contain a qualified electronic signature or seal in their original form.

A document preserved within a qualified electronic document preservation service shall enjoy the presumption of a verified authenticity of the original document, a certificate of which shall be issued by the provider of the qualified electronic document preservation service.

If the document is preserved within the qualified electronic document preservation service so that the preservation period provided for by that service includes the specified period of preservation of the document, the original document may be destroyed, unless otherwise specified.

VI INSPECTION SUPERVISION

Inspection activities for electronic identification and trust services in electronic business

Article 64.

The inspection for electronic identification and trust services in electronic business shall perform the inspection supervision over the implementation of this law and the work of electronic identification service providers and trust service providers (hereinafter: service providers), through inspectors for electronic identification and trust services (hereinafter: the inspector).

Within the inspection supervision of the service providers, the inspector shall determine whether the requirements prescribed by this Law and the regulations adopted for the implementation of this Law have been fulfilled.

Authorities of the inspector

Article 65.

The inspector shall be authorized to carry out the following during the inspection supervision procedure:

1) order the removal of established irregularities and give a deadline for it;

2) prohibit the use of inadequate procedures and infrastructure, and give a deadline to the service provider in which it is obliged to provide adequate procedures and infrastructure;

3) temporarily prohibit the performance of the service provider's services until the inadequacy of procedures and infrastructure is eliminated;

4) order a temporary revocation of some or all of the certificates issued by the service provider, if there is a reasonable suspicion of inadequate procedure or forgery.

VII PENAL, TRANSITIONAL AND FINAL PROVISIONS

Article 66.

A penalty of 50,000 to 2,000,000 dinars shall be imposed for infringement to the provider of qualified trust service - legal person if:

1) they fail to undertake the necessary technical and organizational measures to manage the risks that jeopardize the reliable and secure provision of these trust services (Article 27, paragraph 1);

2) they fail to inform, without delay, and no later than within 24 hours of becoming aware of it, the Ministry of any security breaches or loss of integrity of the service that have a significant impact on the provision of trust services (Article 27, paragraph 3);

3) they fail to inform, without delay, the trust service user about the security breach or the loss of the integrity of a trust service, if the security breach or the loss of integrity of the trust service could adversely affect the trust service users (Article 27, paragraph 4);

4) they fail to inform, before concluding the contract referred to in Article 30, the person who submitted the request for qualified trust service provision about all important circumstances of the use of the service referred to in Article 30, paragraph 2, item 1)-3) of this Law (Article 30, paragraph 2);

5) they fail to fulfill the requirements from Article 31 (Article 31);

6) when issuing a qualified certificate for a trust service, they fail to verify the identity information of the natural or legal person, contained in the qualified certificate, in accordance with Article 33, paragraph 2 of the Law (Article 33, paragraphs 1 and 2);.

7) they fail to conduct an assessment of the fulfillment of requirements before the beginning of the provision of qualified trust services, i.e. at least once in 24 months (Article 34, paragraph 3);

8) they fail to execute the order for an extraordinary assessment of the fulfillment of requirements (Article 34, paragraph 5);

9) they are not registered in the Register of qualified trust service providers before commencing the provision of qualified trust services (Article 35, paragraph 2);

10) an issuer of qualified electronic certificates, who intends to cease its activities, fails to notify each qualified trust service user and the Ministry about the intention to terminate the contract, at least three months before the intended end of the performance of the activities (Article 36, paragraph 1);

11) in case of the end of performance of the activities, it fails to provide continuation of the service with another trust service provider for the users who were issued the certificate, or it fails to revoke all issued certificates and immediately inform the Ministry of the measures taken (Article 36, paragraph 2);

12) it fails to submit all documentation regarding the performance of trust services to another issuer to whom it transfers the obligations of performing one or more trust services, or to the Ministry (Article 36, paragraph 3 and 4);

13) a qualified electronic certificate does not contain all the data referred to in Article 43 paragraph 1 of this Law (Article 43, paragraph 1);

14) an issuer of qualified certificates fails to revoke the issued certificates, in the cases referred to in Article 44, paragraph 1 (Article 44, paragraph 1);

15) the issuer of the qualified certificates fails to inform the qualified trust service user about the revocation of the certificate within 24 hours of the received notification, or of the occurrence of the circumstances for which the certificate is revoked (Article 44, paragraph 2);

16) an issuer of qualified electronic certificates fails to preserve complete documentation on issued and revoked qualified electronic certificates as a means of proofing and verification in administrative, judicial and other proceedings, at least ten years after the expiration of the certificate validity (Article 45);

17) does not ensure the reception and sending of messages including the time when the sender or recipient of the message is a user of another provider of qualified electronic delivery (article 56, paragraph 1);

18) a trustworthy electronic preservation of documents prepared in accordance with Article 61 of this Law, whose authenticity and accuracy of the additionally included data have been verified by a qualified electronic signature or seal referred to in Article 61, paragraph 1, item 4), is not performed so that the procedures and technological solutions ensuring the ability to prove the validity of a qualified electronic signature or seal are used throughout the entire preservation period (Article 62, paragraph 2).

For the infringement referred to in paragraph 1 of this Article, the responsible person of a trust service provider shall also be punished with a fine ranging from 5,000 to 100,000 dinars.

For the infringement referred to in paragraph 1 of this Article, a trust service provider - a natural person representing a legal person shall be punished with a fine ranging from 10,000 to 500,000 dinars.

Article 67.

A penalty of 50,000 to 200,000 dinars shall be imposed for infringement to the qualified trust service user - legal person if:

1) in case of change of the data referred to in paragraph 1 of Article 33 of this Law, it fails to notify, without delay, the qualified trust service provider (Article 33, paragraph 3);

For the infringement referred to in paragraph 1 of this Article, the responsible person of a legal person shall also be punished with a fine ranging from 5,000 to 50,000 dinars.

For the infringement referred to in paragraph 1 of this Article, a trust service user - a natural person representing a legal person shall be punished with a fine ranging from 10,000 to 100,000 dinars.

For the infringement referred to in paragraph 1 of this Article, a trust service user - a natural person shall be punished with a fine ranging from 5,000 to 50,000 dinars.

Article 68.

A penalty of 50,000 to 2,000,000 dinars shall be imposed for infringement to the registered provider of the electronic identification service - legal person if:

the electronic identification scheme does not meet the requirements of Article 17 (Article 17);

they fail to undertake the necessary technical and organizational measures to manage the risks that jeopardize the reliable and secure provision of the services from Article 22, paragraph 2 of this Law (Article 22, paragraphs 1 and 2);

For the infringement referred to in paragraph 1 of this Article, the responsible person of an electronic identification service provider shall also be punished with a fine ranging from 5,000 to 100,000 dinars.

For the infringement referred to in paragraph 1 of this Article, an electronic identification service provider - a natural person representing a legal person shall be punished with a fine ranging from 10,000 to 500,000 dinars.

Article 69.

A penalty of 50,000 to 2,000,000 dinars shall be imposed for infringement to the service provider referred to in Article 64 of this Law if they fail to act on the order of the inspector within the deadline specified in Article 65, paragraph 1 of this Law.

For the infringement referred to in paragraph 1 of this Article, the responsible person of a service provider shall also be punished with a fine ranging from 5,000 to 100,000 dinars.

For the infringement referred to in paragraph 1 of this Article, a service provider - a natural person representing a legal person shall be punished with a fine ranging from 10,000 to 500,000 dinars.

Article 70.

A penalty of 5,000 to 100,000 dinars shall be imposed for infringement to the responsible person in a state body, as well as a body of the Autonomous Province or local self-government unit, if, in the procedure it implements in the exercise of its public authority, it fails to recognize the validity, or denies the probative force of an electronic document created in accordance with this Law, or a digitized act certified in accordance with Article 11 of this Law, only because it was submitted in such format (Article 7).

A penalty of 20,000 to 150,000 dinars shall be imposed for infringement to the responsible person in a state body, as well as a body of the Autonomous Province or local self-government unit, if, in the procedure it implements in the exercise of its public authority, it fails to recognize the validity of an electronic document, including acts of public authorities, signed with a qualified electronic signature or a qualified electronic seal, if the obligation of handwritten signature or stamping is prescribed for the validity of that document (Articles 50 and 51).

Article 71.

A penalty of 50,000 to 2,000,000 dinars shall be imposed for infringement to the legal person that is a state body in terms of this Law, except for the bodies referred to in Article 70 of this Law, if, in the procedure it implements in the exercise of its public authority, it fails to recognize the validity, or denies the probative force of an electronic document created in accordance with this Law, or a digitized act certified in accordance with Article 11 of this Law, only because it was submitted in such format (Article 7).

For the infringement referred to in paragraph 1 of this Article, the responsible person of a legal person referred to in paragraph 1 of this Article shall also be punished with a fine ranging from 5,000 to 100,000 dinars.

For the infringement referred to in paragraph 1 of this Article, a public body if it is a natural person shall be punished with a fine ranging from 5,000 to 100,000 dinars.

A penalty of 100,000 to 2,000,000 dinars shall be imposed for infringement to the legal person that is a state body in terms of this Law, except for the bodies referred to in Article 70 of this Law, if, in the procedure it implements in the exercise of its public authority, it fails to recognize the validity of an electronic document, including acts of public authorities, signed with a qualified electronic signature or a qualified electronic seal, if the obligation of handwritten signature or stamping is prescribed for the validity of that document (Articles 50 and 51).

For the infringement referred to in paragraph 4 of this Article, the responsible person of a legal person referred to in paragraph 4 of this Article shall also be punished with a fine ranging from 20,000 to 150,000 dinars.

For the infringement referred to in paragraph 4 of this Article, a public body if it is a natural person shall be punished with a fine ranging from 20,000 to 150,000 dinars.

2. Transitional and final provisions

Implementation of the Law

Article 72.

The secondary legislation referred to in Article 18, paragraph 2, Article 19, paragraph 3, Article 31, paragraph 3, Article 35, paragraph 8, Article 46, paragraph 5 and Article 47, paragraph 7 of this Law shall be adopted within six months from the day of entry into force of this Law.

The secondary legislation referred to in Article 34, paragraph 8, Article 38, paragraph 4, Article 39, paragraph 4, Article 43, paragraph 3, Article 48, paragraph 4, Article 49, paragraph 2 and Article 52, paragraph 2 of this Law shall be adopted within 12 months from the date of entry into force of this Law.

The secondary legislation referred to in Article 55, paragraph 7, Article 61, paragraph 3 and Article 62, paragraphs 3 and 4 of this Law shall be adopted within 18 months from the date of entry into force of this Law.

Repeal of former regulations, continuation of implementation of secondary legislation and continuation of work on the basis of previous registration

Article 73.

On the day of the entry into force of this Law, the Law on Electronic Signature ("Official Gazette of the RS", No 135/04) and the Law on Electronic Document ("Official Gazette of the RS", No 51/09) shall be repealed.

The secondary legislation adopted pursuant to the law referred to in paragraph 1 of this Article shall apply after the said laws are repealed, until the adoption of appropriate regulations in accordance with this Law, unless they are contrary to the provisions of this Law.

On the day of the entry into force of this Law, the certification bodies issuing qualified electronic certificates, registered on the basis of the Law on Electronic Signature, shall continue to operate as qualified service providers issuing qualified certificates for electronic signature.

On the day of the entry into force of this Law, the time stamp providers, registered on the basis of the Law on Electronic Document, shall continue to operate as qualified service providers issuing qualified electronic time stamps.

The certification bodies referred to in paragraph 3 of this Article, and the time stamp providers referred to in paragraph 4 of this Article shall be obliged to harmonize their operations with the provisions of this Law within 12 months from the date of entry into force of this Law, and submit to the Ministry a report on the conformity assessment referred to in Article 34 of this Law.

The Ministry shall conduct the conformity assessment referred to in Article 34 of this Law until the accreditation of the first conformity assessment body in accordance with the regulations.

The manner of assessing the conformity with the means for creating a qualified electronic seal i.e. remote stamp, until the body for the assessment of conformity has been appointed

Article 73a

When performing the conformity assessment of the remote qualification management service, the conformity assessment of the means for creating an electronic signature, i.e. a stamp with prescribed conditions.

The assessment of the conformity of the assets referred to in paragraph 1 of this article shall be performed by the ministry, i.e. the body for conformity assessment referred to in article 34 of this law, until the appointment of body referred to in article 47 of this law.

The means referred to in paragraph 1 of this article are considered qualified only within the assessment of the evaluated management service of a qualified means for creating an electronic signature, or a remote stamp, provided by the trust qualified services provider.

The means referred to in paragraph 1 of this article will be entered in the register of qualified means for creating electronic signatures and electronic stamps, noting that the means are considered qualified only when they are used within the assessed service.

Entry into force

Article 74.

This Law shall enter into force on the eight day following that of its publication in the "Official Gazette of the Republic of Serbia".