|  |
| --- |
| http://zakonst.rada.gov.ua/images/gerb.gif |
| ***Law of Ukraine*** |

**On electronic trust services**

**(Bulleting of the Verkhovna Rada of Ukraine (BVR), 2017, No. 45, p. 400)**

This Law defines the legal and organisational principles for the provision of electronic trust services, including cross-border, the rights and obligations of the parties of the legal relations in the field of electronic trust services, the procedure of carrying out the state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services, as well as the legal and organisational principles for the carrying out of electronic identification.

The purpose of this Law is to regulate the relations in the field of provision of the electronic trust services and electronic identification.

**Title I**  
**GENERAL PROVISIONS**

**Article 1.**Terms and definitions

1. In this Law, the terms shall be used in the following meanings:

1) authentication – an electronic procedure that enables the electronic identification of a natural, legal person, information or information and telecommunication system and/or the origin and integrity of data in electronic form to be confirmed;

2) blocking of the certificate for a public key – temporary suspension of the validity of the certificate for a public key;

3) website – a combination of software located at an IP address in the computer network, including the Internet, together with the information resources available to certain entities and ensuring the access of legal and natural persons to such information resources and other information services via computer network;

4) public key – the parameter of the algorithm of the asymmetric cryptographic transformation, which is used as data in electronic form in order to verify the electronic signature or seal, as well as for the purposes determined by the standards applicable to the qualified certificates for public keys;

5) separate point of registration – a representative office (branch, business unit, territorial body) of the provider of electronic trust services of the legal or natural person, which, based on the order from the provider of electronic trust services (its director) or based on the agreement concluded with it, carries out the registration of the signatories in compliance with the requirements of this Law and the legislation in the field of information protection;

6) Trusted List – the list of qualified providers of the electronic trust services and the information on the services they provide;

7) electronic trust service – a service, which is provided in order to ensure electronic interaction of two or more parties, which commit the provision of such services to the provider of electronic trust services;

8) electronic identification – the process of using person identification data in electronic form, which uniquely represents either a natural or a legal person, or a representative of a legal person

9) electronic seal – the data in electronic form, which is attached by the creator of the electronic seal to, or logically associated with, other data in electronic form and which is used to identify the origin and verify the integrity of the related data in electronic form.

10) electronic time stamp – the data in electronic form, which binds other data in electronic form to a particular time in order to confirm that that data in electronic form existed at that time;

11) electronic service – any service, which is provided via an information and telecommunication system;

12) electronic signature – the data in electronic form, which is attached by the signatory to, or logically associated with, other data in electronic form and which is used by the signatory to sign;

13) data in electronic form – any information in electronic form;

14) confirmation of validity of the public key – the procedure of creation of the certificate for a public key;

15) electronic signature or seal device – a hardware and software device or a hardware device or software used in order to create and/or verify the electronic signature or seal;

16) electronic identification means – an information carrier containing person identification data of a person and which is used for authentication of a person while providing and/or receiving electronic services;

17) qualified electronic signature or seal device – a hardware and software device or a hardware device or software implementing the cryptographic algorithms of key pairs generation and/or creation of the qualified electronic signature or seal, and/or verification of the qualified electronic signature or seal, and/or storage of the personal key of the qualified electronic signature or seal, which fulfils the requirements of this Law;

18) advanced electronic signature or seal device – a hardware and software device or a hardware device or software implementing the cryptographic algorithms of key pairs generation and/or creation of the advanced electronic signature or seal, and/or verification of the advanced electronic signature or seal, and/or storage of the personal key for advanced electronic signature or seal;

19) person identification data – a unique set of data enabling to expressly identify a natural, legal person or a representative of a legal person;

20) person identification – a procedure of using the person identification data from the documents created on material carriers and/or data in electronic form, the carrying out of which shall ensure the express identification of a natural, legal person or a representative of a legal person;

21) interoperability – technological compatibility of technical solutions that are used when providing electronic services and their ability to interact together;

22) qualified electronic seal – an advanced electronic seal, which is created using a qualified electronic seal creation device and is based on a qualified certificate for an electronic seal;

23) qualified electronic signature – an advanced electronic signature, which is created using a qualified electronic signature creation device and is based on a qualified certificate for a public key;

24) qualified provider of electronic trust services – a legal person, regardless of the legal and organisational form and form of ownership, an individual entrepreneur providing one or more electronic trust services, which activities fulfil the requirements of this Law and the information on which was added to the Trusted List;

25) qualified certificate for a public key – a certificate for a public key, which is issued by a qualified provider of electronic trust services, the validation centre or the central validation authority and complies with the requirements of this Law;

26) compromise of a personal key – any event, which has caused or is capable of causing unauthorized access to a personal key;

27) users of the electronic trust services – signatories, creators of electronic seals and recipients of data in electronic form, other natural and legal persons receiving electronic trust services from the providers of such services in accordance with the requirements of this Law;

28) provider of electronic trust service – a legal person, regardless of the legal and organisational form and form of ownership, an individual entrepreneur providing one or more electronic trust services;

29) personal key – a parameter of the algorithm of the asymmetric cryptographic transformation, which is used as unique data in electronic form for the creation of an electronic signature or seal, accessible only to the signatory or the creator of the electronic seal, as well as for the purposes determined in the standards for the qualified certificates for public keys;

30) key pair – the personal key and the public key corresponding to it, which are interconnected by the parameters of the algorithm of the asymmetric cryptographic transformation;

31) verification – the process of confirming the authenticity and confirming the validity of the electronic signature or seal;

32) signatory – a natural person who creates an electronic signature;

33) renewal of the certificate for a public key – the renewal of the validity of the previously blocked certificate for a public key;

34) software and hardware system used when providing electronic trust services (hereinafter, the ‘software and hardware system’) – hardware, hardware and software, and software ensuring the exercising of the functions relating to the provision of electronic trust services;

35) registry of the valid, blocked and cancelled certificates for public keys – an electronic data base containing the data on the certificates for public keys created by the providers of electronic trust services, the validation centre or the central validation authority, their status and the lists of revoked certificates for public keys;

36) electronic registered delivery – a service that makes it possible to transmit data in electronic form between third parties by electronic means, provide evidence of the handling of the transmitted data in electronic form, including proof of sending and receiving the data in electronic form, and that protects transmitted data in electronic form against loss, theft, damage or unauthorized alterations;

37) self-signed certificate for a public key – a certificate for a public key issued by the central validation authority or the validation centre using the personal key of the central validation authority or the validation centre;

38) certificate for a public key – an electronic document, which certifies that the public key belongs to the natural or legal person, confirms their identification data and/or makes it possible to carry out website authentication;

39) cancellation of the certificate for a public key – termination of the validity of the certificate for a public key;

40) creator of electronic seal – a legal person that creates an electronic seal;

41) electronic identification scheme – a system for electronic identification, under which electronic identification means are issued to natural, legal persons, or representatives of legal persons;

42) technological neutrality of the national technical solutions – non-interference of the authorities in charge of the state regulation in the field of electronic trust services into the process of development of hardware and software systems, electronic signature or seal devices and devices for cryptographic protection of information, which shall not prevent achieving interoperability between them;

43) advanced electronic seal – an electronic seal created as the result of cryptographic transformation of data in electronic form, to which this electronic seal is connected, using am advanced electronic seal device and a personal key expressly related to the electronic seal creator, and which makes it possible to complete electronic identification of the electronic seal creator and detect disturbance of the integrity of the data in electronic form, to which this electronic seal is connected;

44) advanced electronic signature – electronic signature created as the result of cryptographic transformation of data in electronic form, to which this electronic signature is connected, using an advanced electronic signature device and a personal key expressly related to the signatory, and which makes it possible to complete electronic identification of the signatory and detect disturbance of the integrity of the data in electronic form, to which this electronic signature is connected.

2. Other terms shall be used in the meanings referred to them in the [Civil Code of Ukraine](http://zakon.rada.gov.ua/laws/show/435-15" \t "_blank), the Laws of Ukraine [‘On electronic documents and electronic document exchange’](http://zakon.rada.gov.ua/laws/show/851-15" \t "_blank), [‘On the protection of information in the information and telecommunication systems’](http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80" \t "_blank), [‘On standardization’](http://zakon.rada.gov.ua/laws/show/1315-18" \t "_blank), [‘On Technical Regulations and conformity assessment’](http://zakon.rada.gov.ua/laws/show/124-19" \t "_blank), [‘On the scientific and scientific and technical expertise’](http://zakon.rada.gov.ua/laws/show/51/95-%D0%B2%D1%80" \t "_blank), [‘On the National Bank of Ukraine’](http://zakon.rada.gov.ua/laws/show/679-14" \t "_blank).

**Article 2.**Scope of the Law

1. This Law regulates the relations arising between legal and natural persons, authorities in the process of providing, receiving electronic trust services, the procedure of provision of those services, supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services, as well as the main organisational and legal principles of electronic identification.

2. The Laws of Ukraine may provide for special legal regulation of the provision of electronic trust services and electronic identification in specific areas of social relations.

**Article 3.**Legislation in the fields of electronic trust services and electronic identification

1. The relations relating to the provision of electronic trust services and electronic identification shall be regulated by the [Constitution of Ukraine](http://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80" \t "_blank), [the Civil Code of Ukraine](http://zakon.rada.gov.ua/laws/show/435-15" \t "_blank), the Laws of Ukraine[‘On Information’](http://zakon.rada.gov.ua/laws/show/2657-12" \t "_blank), [‘On the protection of information in the information and telecommunication systems’](http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80" \t "_blank), [‘On electronic documents and electronic document exchange’](http://zakon.rada.gov.ua/laws/show/851-15" \t "_blank), [‘On the protection of personal data’](http://zakon.rada.gov.ua/laws/show/2297-17" \t "_blank), this Law, as well as other legislative and regulatory acts.

**Article 4.**Basic principles of the state regulation in the fields of electronic trust services and electronic identification

1. The state regulation and management in the fields of electronic trust services and electronic identification shall be carried out based on the following principles:

ensuring the principle of the rule of law in the process of provision of electronic trust services and electronic identification;

creating favourable and competitive conditions for the development and operation of electronic trust services and electronic identification;

free circulation of electronic trust services in Ukraine, as well as allowing for the free provision of electronic trust services by the providers of electronic trust services located in other states, the activities of which comply with the requirements of this Law;

ensuring the protection of the rights and lawful interests of the users of electronic trust services;

ensuring access to, and the possibility of using, the electronic trust services for persons with disabilities;

conformity of the requirements for the provision of electronic trust services and electronic identification with the European and international standards;

ensuring operational compatibility and technological neutrality of the national technical solutions, as well as non-discrimination thereof;

ensuring the protection of personal data handled during the provision of electronic trust services and electronic identification.

2. The purpose of exercising the state regulation and management in the fields of electronic trust services and electronic identification shall be the following:

implementing unified and effective public policy in the fields of electronic trust services and electronic identification;

creating favourable conditions for the development and operation of electronic trust services and electronic identification;

ensuring operational compatibility and technological neutrality of the national technical solutions, as well as non-discrimination thereof;

ensuring equal possibilities for the access to electronic trust services and the protection of the rights of the parties thereto;

preventing monopolization and creating conditions for the development of fair competition in the field of electronic trust services;

ensuring personal data protection in accordance with the legislation in the field of personal data protection;

carrying out the measures to promote electronic trust services and electronic identification among the population and legal entities;

exercising control over the transparency and openness in the fields of electronic trust services and electronic identification;

facilitating Ukraine’s integration into the global electronic information space.

3. The state regulation and management in the fields of electronic trust services and electronic identification shall be carried out by means of the following:

legislative and regulatory regulation in the fields of electronic trust services and electronic identification;

supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services;

international cooperation in the fields of electronic trust services and electronic identification;

carrying out other measures of state regulation in the fields of electronic trust services and electronic identification envisaged by the legislation.

**Title II**  
**PARTIES TO THE RELATIONS IN THE FIELD OF ELECTRONIC TRUST SERVICES AND AUTHORITIES IN CHARGE OF THE STATE REGULATION IN THE FIELDS OF ELECTRONIC TRUST SERVICES AND ELECTRONIC IDENTIFICATION**

**Article 5.**The system of authorities in charge of the state regulation in the fields of electronic trust services and electronic identification

1. The state regulation in the fields of electronic trust services and electronic identification shall be carried out by:

the Cabinet of Ministers of Ukraine;

the main authority in the system of central executive authorities ensuring the formation of and implementing the public policy in the field of electronic trust services;

the specially authorized central executive authority on the matters of arranging special communication and information protection;

the central executive authority implementing the public policy in the field of information technology, e-government, development and use of national electronic information resources, and development of information society;

the National Bank of Ukraine (within the banking system of Ukraine).

**Article 6.**The powers of the Cabinet of Ministers of Ukraine in the fields of electronic trust services and electronic identification

1. The powers of the Cabinet of Ministers of Ukraine in the fields of electronic trust services and electronic identification shall include ensuring the following:

exercising public policy in the fields of electronic trust services and electronic identification;

determining priority development directions in the fields of electronic trust services and electronic identification;

coordinating the activities of the authorities in charge of the state regulation in the fields of electronic trust services and electronic identification, other than the National Bank of Ukraine;

adopting, within its powers, the regulatory acts in the fields of electronic trust services and electronic identification;

state support of the development in the fields of electronic trust services and electronic identification;

organizing international cooperation in the fields of electronic trust services and electronic identification;

exercising other powers in the fields of electronic trust services and electronic identification, as determined by law.

2. The Cabinet of Ministers of Ukraine shall ensure state regulation in the fields of electronic trust services and electronic identification, taking account of the national requirements, and the international and European standards.

**Article 7.**The powers of the main authority in the system of central executive authorities the formation of and implementing the public policy in the field of electronic trust services

1. The main authority in the system of central executive authorities ensuring the formation of and implementing the public policy in the field of electronic trust services shall, as applicable to legal persons, and individual entrepreneurs intending to provide electronic trust services, perform the functions of the central validation authority by way of adding the data on them to the Trusted List in accordance with the requirements of this Law.

2. The powers of the main authority in the system of central executive authorities ensuring the formation of and implementing the public policy in the field of electronic trust services shall include ensuring the following:

the preparation of the regulatory acts in the field of electronic trust services;

the preparation of the norms, and standards in the field of electronic trust services;

the provision of an administrative service by way of adding the legal persons and individual entrepreneurs, intending to provide electronic trust services, to the Trusted List;

the operation of the software and hardware system of the central validation authority and the protection of the information handled therein, in accordance with the requirements of the legislation;

the operation of the website of the central validation authority;

the maintaining of the Trusted List;

the maintaining of the registry of the valid, blocked and cancelled certificates for public keys;

the generation of key pairs and creating self-signed qualified certificates for an electronic seal of the central validation authority;

the provision of the qualified electronic trust services using a self-signed certificate for an electronic seal of the central validation authority intended for the provision of such services;

the provision of the service of providing accurate time signals synchronized with the State standard of time and frequency;

the coordination of the procedures, prepared by the providers of electronic trust services, of synchronizing the time with Coordinated Universal Time (UTC);

the coordination of the plans of termination of the activities by the qualified providers of electronic trust services;

the obtaining and storage of the documented information, the created qualified certificates for public keys, the registry of the valid, blocked and cancelled qualified certificates for public keys, in the event of termination of the activities by the qualified provider of electronic trust services;

the consideration of proposals (comments) from the parties to the relations in the field of electronic trust services concerning the improvement of the state regulation in the field of electronic trust services;

the provision of consultations to the parties to the relations in the field of electronic trust services on the matters relating to the provision of electronic trust services;

the notification of the supervisory authority of the circumstances that interfere with the activities of the central validation authority;

the mutual recognition of Ukrainian and international certificates for public keys and electronic signatures used during the provision of legally valid electronic services;

the round-the-clock access to the registry of the valid, blocked and cancelled certificates for public keys and to the information on the status of the certificates for public keys via public telecommunication networks;

the cancellation, blocking and renewal of the qualified certificates for public keys in the cases prescribed by this Law;

the interoperability and technological neutrality of the national technical solutions, as well as non-discrimination thereof;

the evaluation of the development status of the field of electronic trust services based on the results of carrying out the analysis of the information on the activities of the providers of electronic trust services and the validation centre, provided under the procedure established by the main authority in the system of central executive authorities ensuring the formation of and implementing the public policy in the field of electronic trust services;

the state regulation on the matters of electronic identification using electronic trust services, within its competence in accordance with this Law;

exercising other powers in the fields of electronic trust services and electronic identification, as determined by law.

3. The technical and technological support of the functions of the central validation authority shall be ensured by the administrator of the information and telecommunication system of the central validation authority, being the state enterprise managed by the main authority in the system of central executive authorities ensuring the formation of and implementing the public policy in the field of electronic trust services.

**Article 8.**The powers of the specially authorized central executive authority on the matters of arranging special communication and information protection in the fields of electronic trust services and electronic identification

1. The specially authorized central executive authority on the matters of arranging special communication and information protection shall perform the functions of the supervisory authority in the field of electronic trust services.

2. The powers of the specially authorized central executive authority on the matters of arranging special communication and information protection in the fields of electronic trust services and electronic identification shall include ensuring the following:

state control over the compliance with the requirements of the legislation in the field of electronic trust services;

establishing the requirements for the information security and protection applicable to the qualified providers of electronic trust services and their separate points of registration;

approving the rules of procedure of the central validation authority, the validation centre and the legal persons, individual entrepreneurs intending to provide electronic trust services;

interaction with the central validation authority and the conformity assessment authorities on the matters of state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services;

cooperation with the bodies on the matters of personal data protection by way of notifying violations of the legislation in the field of personal data protection detected when carrying out inspections by the supervisory authority of the qualified providers of electronic trust services;

analysis of the documents on conformity based on the results of carrying out conformity assessment procedures of the qualified providers of electronic trust services;

issuing instructions concerning the removal of violations of the requirements of the legislation in the field of electronic trust services;

imposition of administrative fines for the violation of the requirements of the legislation in the field of electronic trust services;

state regulation of the matters of electronic identification using electronic trust services, within its competence in accordance with this Law;

determining the standards applicable during the provision of trust services in the field of special communication;

exercising other powers in the fields of electronic trust services and electronic identification, as determined by law.

**Article 9.**The powers of the National Bank of Ukraine in the fields of electronic trust services and electronic identification

1. The National Bank of Ukraine shall create a validation centre to ensure that the qualified providers of electronic trust services within the banking system of Ukraine and the qualified providers of electronic trust services providers making transfers of funds (of the parties to the payment systems) are added to the Trusted List in accordance with the requirements of this Law.

The validation centre shall provide a qualified electronic trust service on the creation, verification, and validation of the qualified certificate for an electronic signature or seal to the qualified providers of electronic trust services using a self-signed certificate for a public key of the validation centre.

2. The validation centre and the qualified providers of electronic trust services, in respect of which the validation centre has taken a decision to add the information thereon to the Trusted List, shall have the same mutual rights and obligations as the central validation authority and the qualified providers of electronic trust services, in respect of which the central validation authority has taken a decision to add the information thereon to the Trusted List.

3. The powers of the National Bank of Ukraine in the fields of electronic trust services and electronic identification shall include the following:

establishing the requirements to be fulfilled by the qualified providers of electronic trust services added to the Trusted List based on the application of the validation centre, including the requirements applicable to their software and hardware systems;

establishing the procedure of provision and use of electronic trust services within the banking system of Ukraine when making transfers of funds;

establishing the procedure of provision of the service of providing accurate time signals by the validation centre to the qualified providers of electronic trust services added to the Trusted List based on the application of the validation centre, and identifying the source of time synchronization;

state regulation of the matters of electronic identification within the banking system of Ukraine;

exercising other powers in the fields of electronic trust services and electronic identification, as determined by law.

4. The validation centre must, during the provision of electronic trust services, fulfil the requirements established for the qualified providers of electronic trust services added to the Trusted List based on the application of the validation centre.

5. The software and hardware system of the validation centre used by it for the provision of electronic trust services must fulfil the requirements established for the software and hardware system of the qualified providers of electronic trust services added to the Trusted List based on the application of the validation centre.

6. The organisational and methodological, the technical and technological conditions of the activities of the validation centre when providing the qualified electronic trust services, the procedure of interaction of the qualified providers of electronic trust services with the validation centre when providing the qualified electronic trust services shall be established by the rules of procedure of the validation centre.

The rules of procedure of the validation centre shall be adopted and approved in accordance with the requirements of the legislation.

**Article 10.**The powers of the central executive authority implementing the public policy in the field of information technology, e-government, development and use of national electronic information resources, and development of information society

1. The powers of the central executive authority implementing the public policy in the field of information technology, e-government, development and use of national electronic information resources, and development of information society shall include the following:

participation in the preparation of the norms, and standards in the field of electronic identification;

establishing the requirement applicable to the electronic identification means, assurance levels for the electronic identification means in order to apply them in the field of e-government;

exercising other powers in the fields of electronic identification, as determined by law.

**Article 11.**Parties to the relations in the field of electronic trust services

1. The parties to the relations in the field of electronic trust services shall include the following:

the users of electronic trust services;

the providers of electronic trust services;

the conformity assessment authorities;

the validation centre;

the central validation authority;

the supervisory authority.

**Article 12.**The rights and obligations of the users of electronic trust services

1. The users of electronic trust services shall have the rights to the following:

receiving electronic trust services;

free choice of the provider of electronic trust services;

challenging in judicial proceedings the actions or inaction of the providers of electronic trust services and the authorities in charge of the state regulation in the field of electronic trust services;

compensation of the damage caused to them and the protection of their rights and lawful interests;

applying with an application to cancel, block or renew their certificate for a public key.

2. The users of electronic trust services shall have the following obligations:

to ensure confidentiality and non-access of other persons to the personal key;

to promptly notify the provider of electronic trust services of the suspicion or the fact of compromise of the personal key;

to provide reliable information required in order to receive electronic trust services;

to make timely payments for electronic trust services, where such payments are provided for by the agreement between the provider and the user of electronic trust services;

to timely provide to the provider of electronic trust services the information on the change of identification data contained in the certificate for a public key;

to not use the personal key in the event of its compromise, as well as in the event of cancellation or blocking of the certificate for a public key.

3. The protection of the rights of the users of electronic trust services, as well as the mechanism of exercising the protection of those rights, shall be regulated by this Law and [the Law of Ukraine](http://zakon.rada.gov.ua/laws/show/1023-12" \t "_blank) ‘On consumer rights protection’.

**Article 13.**The rights and obligations of the qualified providers of electronic trust services

1. The qualified providers of electronic trust services shall have the following rights:

to provide electronic trust services in compliance with the requirements of this Law;

to receive documents required in order to identify the person, whose identification data will be contained in the certificate for a public key;

to obtain consultations with the central validation authority or the validation centre on the matters relating to the provision of electronic trust services;

to apply to the conformity assessment authorities in order to obtain the documents on conformity;

to apply with an application to cancel, block or renew the qualified certificates for public keys created in the central validation authority or the validation centre;

to independently choose, from the list of standards determined by the Cabinet of Ministers of Ukraine, which specific standards will be applied by them when providing trust services, save for the field of special communication.

2. The providers of qualified electronic trust services shall be obliged to ensure the following:

the protection of the personal data of the users of electronic trust services, in accordance with the requirements of the legislation;

the operation of the software and hardware system used by them and the protection of the information handled within it, in accordance with the requirements of the legislation;

the creation and operation of their website;

the introduction, updating and publication, on their website, of the registry of the valid, blocked and cancelled certificates for public keys;

the possibility of round-the-clock access to the registry of the valid, blocked and cancelled certificates for public keys and to the information on the status of the certificates for public keys via public telecommunication networks;

round-the-clock acceptance and verification of the applications from the signatories and creators of electronic seals on the cancellation, blocking and renewal of their certificates for public keys;

the cancellation, blocking and renewal of their certificates for public keys, in accordance with the requirements of this Law;

establishing, during the creation of the certificate for a public key, that the public key and the personal key corresponding to it belong to the signatory or the creator of the electronic seal;

adding the signatory’s or the creator’s identification data to the relevant certificate for a public key;

notification of the supervisory authority on the disturbances of the confidentiality and/or integrity of the information that effect the provision of electronic trust services or relating to the personal data of the users of electronic trust services, no later than within 24 hours from the moment they become aware of such disturbances;

notification of the users of electronic trust services on the disturbances of the confidentiality and/or integrity of the information that effect the provision to such users of electronic trust services or relating to their personal data, no later than within two hours from the moment they become aware of such disturbances;

making it impossible to use the personal key in the event of its compromise;

permanent storage of all issued qualified certificates for public keys;

depositing funds to the current bank account with the special regime of use (the account with the authority in charge of the treasury servicing of the budgetary funds) or insuring the civil liability in order to ensure compensation of damage that can be caused to the users of such services or to third persons resulting from improper performance by the qualified providers of the electronic trust services of their obligations, in the amount specified by [the third part](http://zakon.rada.gov.ua/laws/show/2155-19" \l "n237) of Article 16 of this Law;

hiring employees who possess the required knowledge, experience and expertise, including in the fields of information technologies and information protection, in order to provide the qualified electronic trust services;

the use, during the provision of electronic trust services, exclusively of the qualified certificates confirmed with the central validation authority or the validation centre;

storage of the documents submitted by the users in order to receive electronic trust services;

notification of the supervisory authority and the central validation authority or the validation centre of any changes in the procedure of provision of electronic trust services within 48 hours from the moment such changes take effect;

the transfer to the central validation authority or the validation centre of the information in the event of termination of the activities on providing electronic trust services.

3. The mandatory requirements for the qualified providers of electronic trust services, as well as the procedure of supervision of compliance therewith, shall be established by the Cabinet of Ministers of Ukraine.

**Title III**  
**ELECTRONIC IDENTIFICATION**

**Article 14.**Electronic identification means

1. Electronic identification shall be carried out by means of electronic identification means falling under the electronic identification scheme adopted by the Cabinet of Ministers of Ukraine.

2. International agreements of Ukraine concerning the electronic trust services shall provide for the procedure of notification and recognition of electronic identification schemes (with an indication of the assurance level for the electronic identification means).

**Article 15.**Electronic identification schemes

1. The electronic identification scheme shall provide for the high, substantial or low assurance levels for electronic identification means used within them. The electronic identification scheme shall be determined by the Cabinet of Ministers of Ukraine.

2. The assurance levels low, substantial and high shall meet the following criteria:

the low assurance level of electronic identification means shall refer to electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identification data, and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or denial of the identity;

the substantial assurance level of electronic identification means shall refer to electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identification data, and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or denial of the identity;

the high assurance level of electronic identification means shall refer to electronic identification means in the context of an electronic identification scheme, which provides the highest degree of confidence in the claimed or asserted identification data, and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

3. The use of the qualified electronic signatures and seals ensures the high assurance level of electronic identification schemes.

The use of the advanced electronic signatures and seals ensures the substantial assurance level of electronic identification schemes.

**Title IV**  
**ELECTRONIC TRUST SERVICES**

**Article 16.**Requirements applicable to electronic trust services

1. The electronic trust services shall be provided, as a rule, on a contractual basis by the providers of electronic trust services.

2. The electronic trust services shall consist of the following:

the creation, verification, and validation of the advanced electronic signature or seal;

the creation, verification, and validation of the certificate for an electronic signature or seal;

the creation, verification and validation of the certificate for website authentication;

the creation, verification and validation of the electronic time stamp;

the registered electronic delivery;

the preservation of the advanced electronic signatures, seals, electronic time stamps and certificates related to those services.

Each service within the electronic trust services may be provided both separately, as well as in combination.

3. The activities of the qualified providers of electronic trust services shall be performed subject to depositing funds to the current bank account with the special regime of use (the account with the authority in charge of the treasury servicing of the budgetary funds) or insuring the civil liability in order to ensure compensation of damage that can be caused to the users of such services or to third persons. The amount of the funds in the current bank account with the special regime of use (the account with the authority in charge of the treasury servicing of the budgetary funds) or insurance coverage may not be less than 1,000 minimum salaries.

4. The distribution of damages that can be caused to the users of electronic trust services and to third persons by natural or legal persons that have not been added by the central validation authority to the Trusted List shall be determined by the parties to the legal relations on a contractual basis.

**Article 17.**The use of electronic trust services

1. The electronic interaction in electronic form of natural and legal persons that requires the sending, receiving, use and permanent storage, involving third persons, of data in electronic form, which equivalents in paper form are not required to contain a handwritten signature according to the legislation, as well as authentication in the information systems, in which such data in electronic form is handled, may be carried out using the electronic trust services or without obtaining such services, provided that there is a preliminary agreement between the interacting parties concerning the procedure of electronic identification of the parties to such relations.

2. The electronic interaction of natural and legal persons that requires the sending, receiving, use and permanent storage, involving third persons, of data in electronic form, which equivalents in paper form are not required to contain a handwritten signature according to the legislation, as well as authentication within the components of the information systems, in which such data in electronic form is handled and where the holders of such data in electronic form are the state authorities, local self-government bodies, enterprises, institutions and organisations of the public form of ownership, shall be carried out using the qualified electronic trust services.

The public authorities, local self-government bodies, enterprises, institutions and organisations of the public form of ownership, the state registrars, notaries and other entities authorized by the state in order to perform the functions of the state registrar for the purpose of confirming the validity of the public key shall use exclusively the qualified certificate for a public key, and for the purpose of exercising the powers aimed at the acquisition, change or termination of the rights and/or obligations of a natural or legal person according to law, shall apply exclusively the qualified electronic signature or seal devices, which are incorporated into the hardware and software devices that ensure the protection of the data recorded therein from unauthorized access, from direct exposure of the parameters values of the personal keys and the copying thereof.

3. [The Procedure of use of electronic trust services within the public authorities, local self-government bodies, enterprises, establishments and organisations of the public form of ownership](http://zakon.rada.gov.ua/laws/show/749-2018-%D0%BF" \l "n12" \t "_blank) shall be established by the Cabinet of Ministers of Ukraine.

4. The notarial actions using the qualified electronic signature or seal or other electronic identification means shall take place under the procedure determined by the main authority in the system of central executive bodies ensuring the formation of and implementing public policy in the field of notarial system.

5. The administration of justice using the qualified electronic signature or seal or other electronic identification means shall take place under the procedure determined by law.

6. The use of electronic trust services shall have no effect on the procedure of conclusion of agreements established by law.

The agreements subject to notarization and/or state registration in the cases prescribed by law shall be concluded in electronic form exclusively by means of the qualified electronic trust services and under the prescribed procedure.

7. The results of provision of the qualified electronic trust services shall be acknowledged by all state institutions and other users of those services.

**Article 18.** The qualified electronic trust service of the creation, verification, and validation of the qualified electronic signature or seal

1. The qualified electronic trust service of the creation, verification, and validation of the qualified electronic signature or seal shall be provided by the qualified provider of electronic trust services and shall include the following:

the provision, to the users of electronic trust services, of the qualified electronic signature or seal devices for the generation of key pairs and/or the creation of the qualified electronic signatures or seals, and/or the storage of the personal key of the qualified electronic signature or seal;

technical support and maintenance of the provided qualified electronic signature or seal devices.

2. The qualified electronic signature or seal shall be considered as having completed the verification and having been validated, provided that:

the verification of the qualified electronic signature or seal has been carried out using the qualified electronic signature or seal devices;

the verification has established that, in accordance with the requirements of this Law at the moment of creation of the qualified electronic signature or seal, the qualified certificate for an electronic signature or seal of the signatory or the creator of the seal was valid;

the identification of the signatory or the creator of the electronic seal has been completed by means of the qualified certificate for an electronic signature or seal;

it has been confirmed, in the course of the verification by means of the qualified certificate for the electronic signature or seal, that the personal key belonging to the signatory or the creator of the electronic seal, is stored within the qualified electronic signature or seal device;

in the course of the verification, the integrity of the electronic data in electronic form, to which this qualified electronic signature or seal is connected, has been confirmed.

3. The electronic signature or seal may not be held invalid and denied the possibility to be considered as evidence in the court proceedings solely based on the fact that they are in electronic from or fail to fulfil the requirements for the qualified electronic signature or seal.

4. The qualified electronic signature shall have the same legal effect as the handwritten signature and shall be presumed to be equivalent of the handwritten signature.

5. The qualified electronic seal shall be presumed to possess the integrity of the data in electronic form and the reliability of the origin of the data in electronic from, to which it is connected.

6. The mandatory requirements for the provision of the qualified electronic trust service of the creation, verification, and validation of the qualified certificate for electronic signatures or seals, as well as the procedure of verifying compliance therewith, shall be established by the Cabinet of Ministers of Ukraine.

7. The issuance and circulation of the electronic identification means with the functions of the qualified electronic signature as being the personal identity documents shall be regulated by the legislation.

The requirements for the qualified electronic trust services, which are provided using the electronic identification means with the functions of the qualified electronic signature as being the personal identity documents, shall be established by this Law and other legislative acts.

**Article 19.**The qualified electronic signature or seal devices

1. The qualified electronic signature or seal devices shall ensure the following:

the appropriate level of uniqueness of the key pair generated by them;

the confidentiality of the personal keys in the course of their generation, storage and the creation of the qualified electronic signature or seal;

the protection from the access to the personal keys by third persons.

The qualified electronic signature or seal devices may not modify the data in electronic form, to which that qualified electronic signature or seal is connected, or deny access to them by the signatory or the creator (the authorized representative of the creator) of the electronic seal.

2. The qualified electronic signature or seal devices shall, in the course of verification of the qualified electronic signature or seal, provide to the user of the electronic trust services the results of the verification process and detect all events relating to the breach of the protection of the information.

3. The requirements for the qualified electronic signature or seal devices shall be established by the Cabinet of Ministers of Ukraine.

The compliance of the qualified electronic signature or seal devices with the specified requirements shall be confirmed by the documents on conformity or the positive examination conclusions based on the results of their state examination in the field of cryptographic protection of information.

4. The establishing of the mandatory requirements for the qualified electronic signature or seal devices, as well as verifying compliance therewith, shall be carried out based on the requirements established by the Cabinet of Ministers of Ukraine.

**Article 20.**The qualified electronic trust service of the creation, verification, and validation of the qualified certificate for an electronic signature or seal

1. The qualified electronic trust service of the creation, verification, and validation of the qualified certificate for an electronic signature or seal shall include the following:

creating conditions for the generation of key pair personally by the user or the creator (authorized representative of the creator) of the electronic seal by means of the qualified electronic signature or seal device;

the creation of the qualified certificates for an electronic signature or seal in compliance with the requirements of this Law, and their issuance to the user of the electronic trust service;

the cancellation, blocking and renewal of the qualified certificates for an electronic signature or seal in the cases prescribed by this Law;

verification and validation of the qualified certificates for an electronic signature or seal by way of providing the information to third persons on their status and compliance with the requirements of this Law;

providing access to the created qualified certificates for electronic signatures or seals by way of making them available on the official website of the qualified provider of electronic trust services, subject to the consent of the signatory or the creator of the electronic seal to the publication of the qualified certificate for an electronic signature or seal.

2. The creation and issuance of the qualified certificates for an electronic signature or seal failing to comply with the requirements of this Law shall be prohibited.

3. The mandatory requirements for the qualified electronic trust service of the creation, verification, and validation of the qualified certificate for an electronic signature or seal, as well as the procedure of verifying compliance therewith, shall be established by the Cabinet of Ministers of Ukraine.

**Article 21.**The qualified electronic trust service of the creation, verification, and validation of the qualified certificate for website authentication

1. The qualified electronic trust service of the creation, verification, and validation of the qualified certificate for website authentication shall include the following:

the creation of the qualified certificate for website authentication in compliance with the requirements of this Law, and its transfer to the user of the electronic trust service;

creating conditions for the generation of key pair personally by the user of this electronic trust service by means of the qualified electronic signature or seal device;

the cancellation, blocking and renewal of the qualified certificate for website authentication in the cases prescribed by this Law;

verification and validation of the qualified certificate for website authentication by way of providing to third persons the information on its status and compliance with the requirements of this Law;

providing access to the qualified certificate for website authentication by way of making it available on the official website of the qualified provider of electronic trust services, subject to the consent of the person whose identification data will be contained in the qualified certificate for website authentication to the publication of the qualified certificate for website authentication.

2. The mandatory requirements for the qualified electronic trust service of the creation, verification, and validation of the qualified certificate for website authentication, as well as the procedure of verifying compliance therewith, shall be established by the Cabinet of Ministers of Ukraine.

**Article 22.**Person identification during the creation and issuance of the qualified certificate for a public key

1. The creation and issuance of the qualified certificate for a public key without the identification of the person whose identification data will be contained in the qualified certificate for a public key, shall not be permitted.

2. The identification of the natural person who applied to receive the service of the creation of the qualified certificate for a public key shall be carried out subject to its personal presence, based on the passport of the citizen of Ukraine or based on other documents, which exclude any doubts as to the identity, in accordance with the legislation on the Unified State Demographic Registry and the documents identifying the person, confirming the citizenship of Ukraine or the special status of the person.

3. The identification of the natural person by the qualified provider of electronic trust services based on the identification data contained in the qualified certificate for a public key previously created by it shall also be allowed, provided that that certificate is valid.

4. The identification of foreigners shall be carried out in accordance with the legislation.

5. During the verification of civil capacity of the legal person, the qualified provider of electronic trust services shall acknowledge the information on the legal person indicated in the Unified State Registry of Legal Persons, Individual Entrepreneurs and Civic Associations, and shall also make sure that the scope of its civil capacity is sufficient for the creation and issuance of the qualified certificate for a public key.

6. The qualified provider of electronic trust services shall, in the course of the creation and issuance of the qualified certificate for a public key, establish the identity of the representative of the legal person in accordance with the requirements of this Law, and shall also verify the scope of his or her powers based on the document or the information from the Unified State Registry of Legal Persons, Individual Entrepreneurs and Civic Associations specifying the powers of the representative.

Where a collegial body represents the legal person, a document shall be submitted to the qualified provider of electronic trust services specifying the powers of the relevant body and the distribution of the obligations among its members.

**Article 23.**Qualified certificates for public keys

1. When providing qualified electronic trust services, the qualified certificates for an electronic signature, the qualified certificates for an electronic seal and the qualified certificates for website authentication shall be used.

2. The qualified certificates for public keys must contain the following:

1) an indication that the certificate for a public key has been issued as a qualified certificate for a public key;

2) an indication that the certificate for a public key has been issued in Ukraine;

3) the identification data expressly identifying the qualified provider of electronic trust services, the validation centre or the central validation authority, which issued the qualified certificate for a public key (hereinafter, the ‘entities that issued the certificate’), including the following mandatory information:

as applicable to a legal person: the name and the code under the Unified State Registry of Enterprises and Organisations of Ukraine, under which its state registration was carried out;

as applicable to an individual entrepreneur: the surname, first name, patronymic (if any) and the unique number of the entry in the Unified State Demographic Registry or the registration number of the tax payer’s record card, or the passport series and number (as applicable to the individuals who refused, due to their religious beliefs, to accept the registration number of the tax payer’s record card and notified the relevant revenue and tax authority to that effect and have the respective mark in the passport indicating the right to make payments based on the passport series and number), based on which the person’s state registration was carried out;

4) the identification data expressly identifying the electronic trust services user, including the following mandatory information:

the surname, first name, patronymic (if any) of the signatory and the unique number of the entry in the Unified State Demographic Registry or the registration number of the tax payer’s record card, or the passport series and number (as applicable to the individuals who refused, due to their religious beliefs, to accept the registration number of the tax payer’s record card and notified the relevant revenue and tax authority to that effect and have the respective mark in the passport indicating the right to make payments based on the passport series and number), or;

the name or the surname, name, patronymic (if any) of the creator of the electronic seal and the code under the Unified State Registry of Enterprises and Organisations of Ukraine, based on which their state registration was carried out, or the unique number of the entry in the Unified State Demographic Registry or the registration number of the tax payer’s record card, or the passport series and number (as applicable to the individuals who refused, due to their religious beliefs, to accept the registration number of the tax payer’s record card and notified the relevant revenue and tax authority to that effect and have the respective mark in the passport indicating the right to make payments based on the passport series and number);

5) the location of the legal person, to which the qualified certificate for a public key was issued;

6) the value of the public key, which corresponds to the personal key;

7) the information about the start and expiration of the validity period of the qualified certificate for a public key;

8) the serial number of the qualified certificate for a public key, being unique for the entity that issued the certificate;

9) the qualified electronic signature or qualified electronic seal created by the entity that issued the certificate;

10) the information concerning the qualified certificates, for public keys of the entity that issued the certificate, being publicly accessible;

11) the information concerning the availability of the information required to obtain the qualified electronic trust service of the creation, verification, and validation of the qualified certificates for public keys;

12) the information that the personal key is stored in the qualified electronic signature or seal device (as applicable to the qualified certificate for an electronic signature or seal);

13) the information about restrictions in the use of the qualified electronic signature or seal (as applicable to the qualified certificate for an electronic signature or seal);

14) the name(s) of the domain belonging to the natural or legal person, to whom the certificate for a public key was issued (as applicable to the qualified certificate for website authentication).

3. The qualified certificates for public keys may contain other identification data of natural and legal persons, non-mandatory additional special attributes determined in the standards for the qualified certificates for public keys. These attributes shall not influence the interoperability and recognition of the qualified electronic signatures.

4. The mandatory requirements applicable to the qualified certificates for public keys, as well as the procedure of verifying compliance therewith shall be established by the Cabinet of Ministers of Ukraine.

5. An agreement completed in electronic form may be held by the court invalid if, during its completion, a qualified electronic signature or seal was used, which qualified certificate failed to contain the information prescribed by the second part of this Article, or contains unreliable information.

**Article 24.**Validity of the qualified certificates for public keys

1. The qualified certificate for a public key shall be considered valid subject to the following, at the moment of validity verification:

the duration period indicated in the qualified certificate for a public key has not expired;

the status of the qualified certificate for a public key has not been modified to being cancelled or blocked based on the grounds determined by this Law by the entity that issued the certificate;

based on the previous two conditions, the qualified certificate for a public key of the entity that issued the certificate was valid.

2. The entities that issue certificates for public keys may not issue qualified certificates for public keys with the duration period exceeding the duration period of their own qualified certificates for public keys.

3. The information on the status of the qualified certificates for public keys shall be provided by the entities that issued them, via their information and telecommunication system, on a round-the-clock basis.

4. The access to the qualified certificates for public keys shall be granted to the entities that issued the certificates, taking account of the legislative requirements in the field of personal data protection.

**Article 25.**Cancellation, blocking and renewal of the qualified certificates for public keys

1. The qualified certificate for a public key shall be cancelled no later than within two hours by the entity that issued the certificate in the event of the following:

1) submission by the user of electronic trust services of the application requesting to cancel the qualified certificates for public keys issued to it, submitted in any way that ensures the identification of the user;

2) the receiving, by the entity that issued the certificate, of the document confirming:

the death of the individual entrepreneur;

the termination of the activities of the creator of the electronic seal;

the change of the identification data of the user of electronic trust services;

the fact of the state registration of the termination of commercial activities of the individual entrepreneur or termination of the activities, under the procedure prescribed by the legislation, of the legal person;

the provision by the user of electronic trust services of unreliable identification data in the course of creation of its qualified certificate for a public key;

the fact of compromise of the personal key of the user of electronic trust services, revealed independently by the user or by the supervisory authority in the course of carrying out measures on the state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services;

entering into full force by the court decision on the cancellation of the qualified certificate for a public key, declaring the signatory dead, missing, legally incapable, limiting his or her civil capacity, declaring the user of electronic trust services bankrupt.

2. The self-signed certificate for an electronic seal of the central validation authority shall, no later than within 24 hours, be cancelled by the central validation authority in the event of the following:

confirmation of the fact of compromise of the personal key of the central validation authority, revealed by it independently or revealed by the supervisory authority in the course of carrying out measures on the state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services;

entering into full force by the court decision on the cancellation of the self-signed certificate for an electronic seal of the central validation authority.

3. In the event of submission of the notification on the adoption by the qualified provider of electronic trust services of the decision on terminating the activities of providing qualified electronic trust services, the central validation authority of the validation centre shall, based on the relevant decision, cancel the qualified certificate for a public key issued to such applicant in accordance with the requirements of this Law.

4. The qualified certificate for a public key shall be considered cancelled from the moment the entity that issued the certificate amends the status of the qualified certificate for a public key to being cancelled.

5. The cancelled qualified certificate for a public key may not be renewed.

6. The qualified certificate for a public key shall, no later than within two hours, be blocked by the entity that issued the certificate in the event of the following:

submission by the user of electronic trust services of the application requesting to block the qualified certificates for public keys issued to it, submitted in any way that ensures the identification of the user;

notification by the user of the electronic trust services or the supervisory authority of the suspicion of compromise of the personal key of the user of electronic trust services;

entering into full force by the court decision on the blocking of the qualified certificate for a public key;

breach by the user of the electronic trust services of the essential terms of the agreement on the provision of the qualified electronic trust services.

7. The qualified certificate for a public key issued by the central validation authority shall also be blocked in the event the supervisory authority adopts the decision on the blocking of the qualified certificates for public keys of the qualified provider of electronic trust services based on the results of carrying out the state supervision (control) in accordance with the requirements of this Law.

8. The qualified certificate for a public key shall be considered blocked from the moment the entity that issued the certificate amends the status of the qualified certificate for a public key to being blocked.

9. The qualified certificate for a public key, which status has been changed to being blocked, shall not be used during the period of being blocked.

10. The blocked qualified certificate for a public key shall, no later than within two hours, be renewed by the entity that issued the certificate in the event of the following:

the submission by the user of electronic trust services of the application requesting to renew its blocked qualified certificate for a public key (where the blocking took place based on the application requesting the blocking of the qualified certificate for a public key);

the notification of establishing unreliability of the information concerning fact of compromise of the personal key by the user of the electronic trust services or the supervisory authority that has previously notified of such a suspicion;

the receiving by the entity that issued the certificate of the notification that the court decision has been granted on the renewal of the qualified certificate for a public key and has entered into full force.

11. The blocked qualified certificate for a public key issued by the central validation authority shall also be renewed in accordance with the requirements of this Law in the event of the following:

renewal of the status of the qualified provider of electronic trusts services;

entering into full force by the court decision in favour of the provider of electronic trust services.

12. The qualified certificate for a public key, which has been blocked, shall resume its validity from the moment of its renewal.

13. The qualified certificate for a public key shall be considered renewed from the moment the entity that issued the certificate amends the status of the qualified certificate for a public key to being renewed.

14. The entity that issued the qualified certificate for a public key shall ensure access to the information on the date and time of change of the status of the qualified certificate for a public key.

**Article 26.**The qualified electronic trust service of the creation, verification and validation of the qualified electronic time stamp

1. The qualified electronic trust service of the creation, verification and validation of the qualified electronic time stamp shall include the following:

the creation of the qualified electronic time stamp;

the transfer of the qualified electronic time stamp to the user of the electronic trust service.

The qualified electronic time stamp shall be presumed to possess the accuracy of the date and time that it indicates, and the integrity of the data in electronic form, to which those date and time are connected.

2. The qualified electronic time stamp shall ensure the following:

the connection of the date and time with the data in electronic form in such a way that completely excludes the possibility of unnoticed modification of the data in electronic form;

the accuracy of the time in the software and hardware system of the qualified provider of electronic trust services, which is synchronized with Coordinated Universal Time (UTC) with accuracy to the second.

3. The advanced electronic signature or advanced electronic seal created for the qualified electronic time stamp shall be attached to the latter.

4. The use of the qualified electronic time stamp for the permanent storage of data in electronic form shall be mandatory.

5. The mandatory requirements to the procedures of providing the qualified electronic trust service of providing the qualified electronic time stamp, as well as the procedure of verifying compliance therewith, shall be established by the Cabinet of Ministers of Ukraine.

**Article 27.**The qualified electronic trust service of the registered electronic delivery

1. The qualified electronic trust service of the registered electronic delivery shall fulfil the following requirements:

shall be provided by one or more qualified providers of electronic trust services;

the electronic identification of the sender shall be ensured;

the electronic identification of the recipient, prior to the delivery of the data in electronic form, shall be ensured;

the advanced electronic signature or advanced electronic seal of the qualified provider of electronic trust services, created for the data in electronic form being sent, shall be attached to that data;

the sender and the recipient of the data in electronic form shall be notified of any modification of the data in electronic form that is required in order to send or receive that data;

the date and time of sending, receiving and making any modification of the data in electronic form shall be recorded using the qualified electronic time stamp;

in the event of sending the data in electronic form between two or more qualified providers of the electronic trust services, the requirements specified above shall apply to all qualified providers of the electronic trust services.

2. The mandatory requirements to the qualified providers of the electronic trust service of the registered electronic delivery, as well as the procedure of verifying compliance therewith, shall be established by the Cabinet of Ministers of Ukraine.

3. The data in electronic form sent or received using the qualified electronic trust service of the registered electronic delivery may not be held legally invalid and denied the possibility to be considered as evidence in the court proceedings solely based on the fact that they are in electronic from, provided that such data fulfils the requirements to the qualified electronic trust service of the registered electronic delivery.

4. The data in electronic form sent or received using the qualified electronic trust service of the registered electronic delivery shall be presumed to possess integrity of data in electronic form, their guaranteed transfer by the identified sender and the guaranteed receiving by the identified recipient, as well as the accuracy of the date and time of sending and receiving of the data in electronic form, which are indicated during the provision of this service.

**Article 28.**The qualified electronic trust service of storage of the qualified electronic signatures, seals and the certificates connected with such services

1. The qualified electronic trust service of storage of the qualified electronic signatures, seals and the certificates connected with such services shall ensure the storage of the previously created qualified electronic signatures or seals and the created certificates connected with such services, for the time period determined by the legislation in the field of archive-keeping as applicable to documents in paper form.

2. The mandatory requirements to the qualified electronic trust service of storage of the qualified electronic signatures, seals, electronic time stamps and the certificates connected with such services, as well as the procedure of verifying compliance therewith, shall be established by the Cabinet of Ministers of Ukraine.

**Article 29.**Special provisions on the provision of qualified electronic trust services by the central validation authority

1. The central validation authority shall provide the electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal to the qualified providers of electronic trust services using the self-signed certificate for a public key of the central validation authority.

The qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal shall be provided by the central validation authority based on the application requesting to provide such service and the concluded agreement on the provision of the qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal, which form shall be established by the main authority in the system of central executive authorities ensuring the formation of and implementing public policy in the field of electronic trust services.

2. The agreement on the provision by the central validation authority of the qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal shall include the terms concerning the following:

the procedure of providing services in compliance with the requirements of this Law and the legislative and regulatory acts adopted towards its implementation, and the rules of procedure of the central validation authority;

its duration period;

the grounds for making amendments to or terminating the agreement on the provision by the central validation authority of the qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal.

The grounds for terminating the agreement on the provision by the central validation authority of the qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal shall include the following:

exclusion of the qualified provider of electronic trust services from the Trusted List;

non-fulfilment of its essential terms.

The central validation authority shall provide the qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal to the public authorities, local self-government bodies, other legal persons of public law free of charge.

The central validation authority, in the course of providing the qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal, shall have the right to terminate the provision of electronic trust services to the qualified providers of electronic trust services in the event of their violation of the legislation in the field of electronic trust services and the terms of the agreement on the provision of electronic trust services.

3. The central validation authority, in the course of providing the qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal, shall carry out identification of legal and natural persons and shall verify their civil capacity based on the submitted documents. The identification data from the submitted documents shall be added by the central validation authority to the qualified certificate for the public key of the natural or legal person.

4. The central validation authority, in the course of providing the qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal, shall fulfil the requirements established for the qualified providers of electronic trust services.

5. The software and hardware system of the central validation authority, which it uses in order to provide the qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal, shall fulfil the requirements established for the software and hardware system of the qualified providers of electronic trust services.

6. The organisational and methodological, the technical and technological conditions of the activities of the central validation authority, in the course of its provision of the qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal, the procedure of interaction of the providers of electronic trust services with the central validation authority, in the course of its provision of the qualified electronic trust service of the creation, verification and validation of the qualified certificate for an electronic signature or seal, shall be established by the rules of procedure of the central validation authority.

The rules of procedure of the central validation authority shall be adopted and approved according to the legislative requirements.

**Article 30.**Obtaining the status of the qualified provider of electronic trust services

1. The status of the qualified provider of electronic trust services shall be obtained by the legal persons, individual entrepreneurs from the day the information on them is added to the Trusted List based on the decision of the central validation authority or the validation centre (in the event of providing electronic trust services within the banking system of Ukraine and when making transfers of funds).

2. The legal persons, individual entrepreneurs, in order for the information on them to be added to the Trusted List, shall provide to the central validation authority or the validation centre the following:

1) an application to be added to the Trusted List;

2) a document allowing to expressly identify the individual entrepreneur or the representative of the legal person;

3) a copy, duly certified under the procedure established by the legislation, of the certificate of compliance of the integrated information protection system with the requirements of the regulatory documents in the field of information protection, together with a copy, duly certified under the procedure established by the legislation, of the affirmative examination report based on the results of the state examination in the field of cryptographic protection of information or a copy, duly certified under the procedure established by the legislation, of the document on conformity issued based on the results of carrying out the conformity assessment procedure in the field of electronic trust services;

4) copies, duly certified under the procedure established by the legislation, of the documents confirming the title to, or the right to use, the non-residential premises, which will be used for the placing of components of the software and hardware system that will ensure the provision of qualified electronic trust services;

5) the list and the positions of the employees whose obligations will be directly related to the provision of the qualified electronic trust services;

6) copies, duly certified under the procedure established by the legislation, of the documents confirming the level of expertise and the three year of occupational experience of the employees whose obligations will be directly related to the provision of the qualified electronic trust services;

7) copies, duly certified under the procedure established by the legislation, of the documents confirming the title to, or the right to use, the qualified electronic signature or seal devices that will be used to provide qualified electronic trust services;

8) a copy, duly certified under the procedure established by the legislation, of the agreement on insurance of civil liability or copies, duly certified under the procedure established by the legislation, of the documents confirming the depositing of funds to the current bank account with the special regime of use (the account with the authority in charge of the treasury servicing of the budgetary funds) in order to ensure compensation of damage that can be caused by the qualified provider of electronic trust services to the users of electronic trust services resulting from improper fulfilment by the former of its obligations;

9) a copy, duly certified under the procedure established by the legislation, of the rules of procedure of the qualified provider of electronic trust services, as approved by the regulatory authority (or the validation centre - as applicable to the providers of electronic trust services that are added to the Trusted List based on the application from the validation centre), which comply with the requirements for the rules of procedure of the qualified provider of electronic trust services;

10) copies of the documents specified by points 1-9 of this part, in electronic form.

In the event of provision of electronic trust services within the banking system of Ukraine and when making transfers of funds, the information to the Trusted List shall be added based on the application from the validation centre.

3. In the event a legal person, an individual entrepreneur intend to provide qualified electronic trust services via separate points of registration, the information on the separate points of registration and their employees whose obligations will be directly related to the provision of the qualified electronic trust services shall be submitted to the central validation authority or the validation centre together with the documents specified in the second part of this Article.

4. The central validation authority or the validation centre shall, based on consideration of the submitted documents, within 15 working days from the day of registration of the application requesting to be added to the Trusted List, adopt a decision on adding the qualified provider of electronic trust services, or send a substantiated refusal of adding the information, to the Trusted List.

5. The qualified provider of electronic trust services shall, based on the decision adopted by the central validation authority or the validation centre on adding the information thereon to the Trusted List, confirm its public key with the central validation authority or the validation centre in accordance with the requirements of the rules of procedure of the central validation authority or the validation centre.

6. The central validation authority or the validation centre shall take a decision on the refusal of adding information to the Trusted List in the event of the following:

submission of incomplete documents specified by the second part of this Article;

revealing in the application, requesting to be added to the Trusted List, and the documents attached thereto, unreliable information, faults not allowing to clearly interpret the contents, corrections or additions.

7. Change of the information on the qualified provider of electronic trust services indicated in the Trusted List shall serve as the basis for making amendments to the Trusted List.

Where the grounds arise to make amendments to the Trusted List, the qualified provider of electronic trust services must, within five working days from the day such grounds arise, submit to the authority that adopted the decision on adding information thereon to the Trusted List, an application requesting to make amendments to the Trusted List together with the documents supporting the relevant changes.

The central validation authority shall, within five calendar days from the day of registration of the application requesting to make amendments to the Trusted List, make the relevant amendments to the Trusted List or provide substantiated refusal of making the amendments to the Trusted List.

The central validation authority of the validation centre shall provide a substantiated refusal of making the amendments to the Trusted List in the event of the following:

the failure to submit the documents being the ground for making the relevant amendments to the Trusted List;

revealing in the application, requesting to make amendments to the Trusted List, and the documents attached thereto, unreliable information, faults not allowing to clearly interpret the contents, corrections or additions.

8. The validation centre shall, within three working days from the day the decision on adding the information on the qualified provider of electronic trust services to the Trusted List is adopted, or from the day of receiving from such applicant an application requesting to make amendments to the Trusted List, notify the central validation authority, which shall, within two working days from the day of registration of the notification from the validation centre, make the relevant amendments to the Trusted List.

9. The central validation authority shall adopt a decision on the exclusion of the qualified provider of electronic trust services from the Trusted List in the event of receiving:

an application from the qualified provider of electronic trust services requesting to remove the information thereon from the Trusted List;

an application from the validation centre requesting the exclusion of the qualified provider of electronic trust services from the Trusted List;

an application from the supervisory authority requesting the exclusion of the qualified provider of electronic trust services from the Trusted List based on the results of the inspection of compliance with the legislative requirements in the field of electronic trust services;

information on the termination of the activities of the qualified provider of electronic trust services (the state registration of the termination of commercial activities of the individual entrepreneur or termination of the activities, under the procedure prescribed by the legislation, of the legal person);

information of the death of the qualified provider of electronic trust services (the individual entrepreneur);

information on the entering into full force by the court decision on the exclusion of the qualified provider of electronic trust services from the Trusted list, declaring the qualified provider of electronic trust services dead, declaring him or her missing, legally incapable, limiting his or her civil capacity, declaring the qualified provider of electronic trust services bankrupt.

**Article 31.**Termination of the activities of the provision of qualified electronic trust services by the qualified provider of electronic trust services

1. The qualified provider of electronic trust services shall terminate its activities of providing qualified electronic trust services in the event of:

adoption by the central validation authority of the decision on its exclusion from the Trusted List;

its adoption of the decision on the termination of providing qualified electronic trust services indicated in the Trusted List;

termination of the activities of the qualified provider of electronic trust services (the state registration of the termination of commercial activities of the individual entrepreneur or termination of the activities, under the procedure prescribed by the legislation, of the legal person);

entering into full force by the court decision on its exclusion from the Trusted list, declaring him or her dead, missing, legally incapable, limiting his or her civil capacity, declaring it bankrupt.

2. The qualified provider of electronic trust services shall inform the users of electronic trust services, the central validation authority or the validation centre and the supervisory authority of the adoption of the decision on terminating the provision of qualified electronic trust services no later than within five working days from the day such decision is adopted.

3. The central validation authority and/or the validation centre must make publicly available the information on the decision of the central validation authority or the validation centre accordingly on the termination, by the qualified provider of electronic trust services, of providing qualified electronic trust services or exclusion of the qualified provider of electronic trust services by the central validation authority from the Trusted List, no later than in the course of the working day following the adoption of such decision by means of:

placing the information on that decision on its official website;

sending to the qualified provider of electronic trust services a notification of that decision indicating the grounds for the cancellation.

4. The central validation authority and/or the validation centre must publish on their official website a notification of the termination of provision of qualified electronic trust services by the qualified provider of electronic trust services no later than in the course of the day following the day of receiving the notification of the grounds specified in the third to fifth indents of the first part of this Article.

The notification of the central validation authority or the validation centre on the termination of providing qualified electronic trust services by the qualified provider of electronic trust services shall indicate the publication date.

5. The qualified provider of electronic trust services shall terminate its activities of providing electronic trust services within three months from the day of publication by the central validation authority or the validation centre accordingly on its official website of the notification on the termination of provision of qualified electronic trust services by the qualified provider of electronic trust services.

6. From the moment of publication by the central validation authority or the validation centre accordingly on its official website of the notification on the termination of provision of qualified electronic trust services by the qualified provider of electronic trust services and until the day of termination of provision of qualified electronic trust services, the qualified provider of electronic trust services shall provide electronic trust services, other than the creation of new qualified certificates for public keys.

7. The qualified provider of electronic trust services shall send to the central validation authority or the validation centre a plan of terminating the activities of providing qualified electronic trust services within 15 working days from the day of publication on the official website of the central validation authority or the validation centre of the notification on the termination of providing qualified electronic trust services by such provider.

The plan of terminating the activities of providing qualified electronic trust services shall be considered and approved by the central validation authority or the validation centre (in the event of providing electronic trust services within the banking system of Ukraine and when making transfers of funds) within 15 working days from the day of its registration.

In the event the plan of terminating the activities of providing qualified electronic trust services is not approved by the central validation authority or the validation centre, the qualified provider of electronic trust services shall be issued a substantiated refusal.

In the event of refusal, the qualified provider of electronic trust services shall re-send a revised plan of terminating the activities of providing qualified electronic trust services within 15 working days from the day of receiving such refusal from the central validation authority or the validation centre.

8. The qualified provider of electronic trust services terminating the provision of qualified electronic trust services shall ensure the protection of the users’ rights by way of returning the funds for the services that cannot be provided further on, where such services have been paid for in advance.

9. All qualified certificates for public keys, which have been created by the qualified provider of electronic trust services for the signatories or creators of an electronic seal, shall be cancelled according to the requirements of this law on the day determined according to the fifth part of this Article as the date of terminating the provision of qualified electronic trust services, or on the day the relevant court decision enters into force.

10. The central validation authority, on the day determined according to the fifth part of this Article as the date of terminating the provision of qualified electronic trust services, shall make the relevant amendments to the Trusted List.

11. In the event of terminating the provision of qualified electronic trust services, the qualified provider of electronic trust services shall transfer to the central validation authority or the validation centre the documented information (the documents, based on which the qualified electronic trust services have been provided to the users and the qualified certificates for public keys have been created, blocked, cancelled, all of the created qualified certificates for public keys, as well as the registries of the created qualified certificates for public keys), which shall ensure the long-term continuation of legal validity of the qualified electronic signatures and seals created for the data in electronic form, attached thereto, of the users of electronic trust services by way of ensuring the possibility of their verification.

12. The procedure of storing the documented information and its transfer to the central validation authority in the event of termination of the activities of the qualified provider of electronic trust services shall be established by the Cabinet of Ministers of Ukraine.

13. The procedure of transferring the documented information to the validation centre in the event of termination of the activities of the qualified provider of electronic trust services shall be established by the National Bank of Ukraine.

**Title V**  
**SUPERVISION (CONTROL) IN THE FIELD OF ELECTRONIC TRUST SERVICES**

**Article 32.**Conformity assessment in the field of electronic trust services

1. In order to prove conformity with the requirements applicable to the qualified providers of electronic trust services and to the services they provide, the legal persons, individual entrepreneurs intending to provide electronic trust services may, at their own expense, undergo the conformity assessment procedure in the field of electronic trust services.

2. The conformity assessment procedure in the field of electronic trust services shall be carried out by the conformity assessment authorities accredited according to the legislation in the field of accreditation.

3. The conformity assessment with the requirements applicable to the qualified providers of electronic trust services and to the services they provide shall be carried out taking account of the legislative requirements concerning the procedure of provision and use of the qualified electronic trust services, including within the banking system of Ukraine and when making transfers of funds, as well as taking account of the legislative requirements in the field information protection.

4. The qualified providers of electronic trust services, which have completed the conformity assessment procedure in the field of electronic trust services and the information on which has been added to the Trusted List, must, every 24 months, at their own expense, undergo the conformity assessment procedure in order to prove that they, and the electronic trust services they provide, comply with the requirements applicable to the qualified providers of electronic trust services and to the services they provide.

5. The results of conformity assessment in the field of electronic trust services must be notified by the qualified providers of electronic trust services to the supervisory authority by way of submitting a copy of the document on conformity compliance with the requirements applicable to the qualified providers of electronic trust services and to the services they provide, no later than within three working days from the days it was received.

6. The carrying out of the procedure of conformity assessment in the field of electronic trust services shall take place under the procedure approved by the Cabinet of Ministers of Ukraine.

**Article 33.**State supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services

1. The state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services shall be carried out by the supervisory authority.

2. The measures of the state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services shall be carried out in accordance with the [Law of Ukraine](http://zakon.rada.gov.ua/laws/show/877-16" \t "_blank) ‘On the main principles of state supervision (control) in the field of commercial activities’, taking account of the special provisions envisaged by this Law.

3. The regulatory authority shall perform the following scheduled measures of state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services:

1) inspection of the qualified providers of electronic services (their separate points of registration) or submitting an inquiry to the conformity assessment authority concerning the carrying out the procedure of conformity assessment of the qualified providers of electronic trust services, at their own expense, in order to confirm that those providers and the electronic trust services they provide comply with the requirements applicable to the qualified providers of electronic trust services and to the services they provide;

2) inspection of the validation centre;

3) inspection of the central validation authority.

4. The supervisory authority shall perform the following unscheduled measures of state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services:

1) inspection of the qualified providers of electronic trust services based on their applications;

2) inspection of the qualified providers of electronic trust services in the event unreliable information in the documents submitted by them is revealed and confirmed;

3) verification of the fulfilment by the qualified providers of electronic trust services of the instructions, concerning the removal of the violations of the legislative requirements, issued based on the results of the completed scheduled measures of state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services;

4) inspection of the qualified providers of electronic trust services following the receipt of information on, or notification of, the violations of the requirements of the legislation in the field of electronic trust services from the validation centre, the central validation authority, the court, the users of electronic trust services and third persons.

5. The supervisory authority shall, based on the results of the carrying out of inspections of the qualified providers of electronic trust services (their separate points of registration), the validation centre, the central validation authority, apply the following response measures:

1) demand that the qualified providers of electronic trust services, the validation centre, of the central validation authority remove the violations of the legislative requirements in the field of electronic trust services, within the time period established by the instruction;

2) adopt a decision on the blocking of the qualified certificates for public keys of the qualified provider of electronic trust services, the self-signed certificate for an electronic seal of the validation centre, the self-signed certificate for an electronic seal of the central validation authority, where the facts of compromise of the personal key have been revealed in the course of the inspection.

The decision on the blocking of the qualified certificates for public keys of the qualified provider of electronic trust services, the self-signed certificate for an electronic seal of the central validation authority shall be sent by the supervisory authority to the central validation authority on the day of its adoption.

The decision on the blocking of the self-signed certificate for an electronic seal of the validation centre shall be sent by the supervisory authority to the validation centre and the central validation authority on the day of its adoption;

3) send to the central validation authority an application requesting that the qualified provider of electronic trust services be excluded from the Trusted List in the event of the following:

the provision of qualified electronic trust services where the qualified provider of electronic services has no valid documents, as determined by the legislation, confirming the conformity compliance by the information protection system of the information and telecommunication system of the qualified provider of electronic services and the information protection means within that system with the requirements of the legislative and regulatory acts in the field of technical and cryptographic protection of information, or has no documents on conformity based on the results of the completed compliance assessment procedure in the field of electronic trust services;

the failure to complete an additional state examination of the integrated information protection system or the conformity assessment procedure of the information and telecommunication system of the qualified provider of electronic trust services in the event of modernization of the hardware, hardware and software or software within the software and hardware system, that is not required by the design and maintenance documentation to the integrated information protection system of the information and telecommunication system of the qualified provider of electronic trust services;

the provision of qualified electronic trust services where the qualified provider of electronic services has no current bank account with the special regime of use (the account with the authority in charge of the treasury servicing of the budgetary funds) with the required amount of funds or has no valid agreement on the insurance of civil liability with the required coverage, as established by [the third part](http://zakon.rada.gov.ua/laws/show/2155-19" \l "n237)of Article 16 of this Law, in order to ensure compensation of damages that can be caused to the users of electronic trust services or to third persons resulting from improper performance by the qualified providers of the electronic trust services of their obligations;

violation of the requirements for the conditions of operation of the integrated information protection system within the information and telecommunication system of the qualified provider of electronic trust services;

the failure to remove the violations revealed in the course of the inspection within the time period established by the instruction;

provision of the qualified electronic trust services by the qualified provider of electronic trust services without valid documents, as determined by the legislation, confirming the title to, or the right to use, the qualified electronic signature or seal devices, which are used for the provision of the qualified electronic trust services;

establishing the fact of providing unreliable information indicated in the documents submitted by the qualified provider of electronic trust services for the purpose of the information thereon being added to the Trusted List.

6. The supervisory authority shall, within a month from the day of generation by the central validation authority of the key pairs and the creation of the relevant self-signed certificates for electronic seals of the central validation authority, carry out an unscheduled inspection of the central validation authority in terms of protection of information in the software and hardware system of the central validation authority.

In the event of revealing violations of the requirements established by the legislation for the central validation authority, the supervisory authority shall notify the Cabinet of Ministers of Ukraine of the revealed violations and shall propose to the central validation authority solutions thereto.

The supervisory authority shall, on an annual basis, by 1 April, prepare and submit to the Cabinet of Ministers of Ukraine a report on the evaluation of the activities of the parties to the relations in the field of electronic trust services in terms of compliance with the legislative requirements.

**Article 34.**The powers of the officials of the supervisory authority when carrying out the measures of state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services

1. The officials of the supervisory authority when carrying out the measures of state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services shall have the following rights:

to carry out on-site and remote measures of state supervision (control) over the compliance with the requirements of the legislation in the field of electronic trust services;

in the event of revealing violations of the requirements of the legislation in the field of electronic trust services, to issue instructions, binding to the qualified providers of electronic trust services, on the removal of the violations and to appoint the time period for the removal of the revealed violations;

to impose on the guilty persons administrative sanctions for the violations of the requirements of this Law and other legislative and regulatory acts adopted in accordance with this Law;

to apply to the court regarding the application of response measures;

to exercise other powers as determined by law.

**Article 35.**The Trusted List

1. The central validation authority shall introduce, update and publish on its official website the Trusted List containing the information on the qualified providers of electronic trust services together with the information on the qualified electronic trust services they provide.

The Trusted List shall be introduced, updated and published in the secure mode with the mandatory attachment of the electronic seal of the central validation authority in the form suitable for automatic processing.

The information contained in the Trusted List shall be publicly available.

2. [The mandatory requirements applicable to the Trusted List](http://zakon.rada.gov.ua/laws/show/775-2018-%D0%BF" \l "n10" \t "_blank) shall be established by the Cabinet of Ministers of Ukraine.

3. The procedure of maintaining the Trusted List shall be adopted by the main authority in the system of central executive authorities ensuring the formation of and implementing the public policy in the field of electronic trust services.

**Article 36.**Responsibility in the field of electronic trust services

1. The damage caused to the user of electronic trust services by the provider of electronic trust services, the validation centre, the central validation authority or the supervisory authority shall be compensated in full under the procedure established by law.

2. The persons guilty of the violation of the requirements of this Law or the legislative and regulatory acts regulating the activities in the field of electronic trust services, shall bear criminal, administrative and civil responsibility according to law.

3. The disputes arising in the field of electronic trust services shall be resolved under the procedure established by law.

**Title VI**  
**INTERNATIONAL COOPERATION**

**Article 37.**Parties to the international cooperation in the fields of electronic trust services and electronic identification

1. Ukraine participates in the international cooperation in the fields of electronic trust services and electronic identification, in particular, based on international treaties of Ukraine.

2. Ukraine’s participation in the international cooperation in the fields of electronic trust services and electronic identification shall take place under the procedure established by law.

3. Where an international treaty of Ukraine provides for the rules other than those provided for in this Law, the rules of the international treaties of Ukraine shall prevail.

**Article 38.**Recognition of foreign electronic trust services

1. The electronic trust services provided in accordance with the requirements of the legislative and regulatory acts regulating legal relations in the field of electronic trust services in the foreign states, shall be recognized in Ukraine as being electronic trust services of the same type, provided that at least one of the following conditions is met:

the qualified provider of electronic trust services of the foreign state meets the requirements of this Law, which is confirmed by the central validation authority (or the validation centre in the event of provision of electronic trust services within the banking system of Ukraine and when making transfers of funds);

the qualified provider of electronic trust services has been added to the Trusted List of the state, with which Ukraine has concluded the relevant bilateral or multilateral international treaty.

2. The electronic trust services may not be deemed invalid solely based on the fact that they have been provided in accordance with the requirements of the legislative and regulatory acts regulating the relations in the field of electronic trust services in the foreign states.

3. The procedure of using the information and telecommunication system of the central validation authority in order to ensure the recognition in Ukraine of the electronic trust services, the foreign certificates for public keys, that are used during the provision of legally valid electronic services in the process of interaction between the entities of various states, shall be established by the Cabinet of Ministers of Ukraine.

**Title VII**  
**FINAL AND TRANSITIONAL PROVISIONS**

1. This Law shall enter into force within a year from the date of its official publication, save for [Article 10](http://zakon.rada.gov.ua/laws/show/2155-19" \l "n157), which shall enter into force on the day of the publication of this Law.

2. [The Law of Ukraine ‘On electronic digital signature’](http://zakon.rada.gov.ua/laws/show/852-15" \t "_blank)(Bulletin of the Verkhovna Rada of Ukraine, 2003, No. 36, p. 276; 2009, No. 24, p. 296; 2013, No. 37, p. 488; 2015, No. 23, p. 158; 2016, No. 47, p. 800) shall cease to have effect.

3. The following Laws of Ukraine shall be amended:

1) in [Article 7](http://zakon.rada.gov.ua/laws/show/679-14" \l "n109" \t "_blank) of the Law of Ukraine ‘On the National Bank of Ukraine’ (Bulletin of the Verkhovna Rada of Ukraine, 1999, No. 29, p. 238, as amended):

[Point 26](http://zakon.rada.gov.ua/laws/show/679-14" \l "n151" \t "_blank) shall be replaced by the following:

‘26) create a validation centre in order to ensure the adding of the information on legal persons, individual entrepreneurs, intending to provide electronic trust services within the banking system of Ukraine, to the Trusted List according to the Law of Ukraine “On electronic trust services”’;

Point 26**-1** shall be supplemented by the following:

‘26**-1**) perform the state regulation of the matters of electronic identification within the banking system of Ukraine, establishing for this purpose the following:

the requirements to be met by the qualified providers of electronic trust services providing qualified electronic trust services within the banking system of Ukraine and when making transfers of funds, including the requirements to their software and hardware systems;

the procedure of provision and use of the electronic trust services within the banking system of Ukraine and when making transfers of funds;

the procedure of provision of the service of providing accurate time signals by the validation centre to the qualified providers of electronic trust services within the banking system of Ukraine and when making transfers of funds’;

2) in [the Law of Ukraine ‘On electronic documents and electronic document exchange’](http://zakon.rada.gov.ua/laws/show/851-15" \t "_blank) (Bulletin of the Verkhovna Rada of Ukraine, 2003, No. 36, p. 275; 2014, No. 24, p. 885; 2015, No. 45, p. 410):

а) the third part of Article 6 shall be replaced by the following:

‘The relations concerning the use of the advanced and qualified electronic signatures shall be regulated by the Law of Ukraine “On electronic trust services”’;

б) the first part of Article 7 shall be replaced by the following:

‘The original of the electronic document shall be considered the electronic copy of the document with the mandatory requisites, including the electronic signature of the author or the signature being the equivalent of a handwritten signature according to the Law of Ukraine “On electronic trust services”’;

в) in Article 12, the wording ‘may be carried out’ shall be replaced by the wording ‘shall be carried out’;

3) in [the Law of Ukraine ‘On the State Service for Special Communications and Information Protection of Ukraine’](http://zakon.rada.gov.ua/laws/show/3475-15" \t "_blank)(Bulletin of the Verkhovna Rada of Ukraine, 2014, No. 25, p. 890, No. 29, p. 946):

а) [the third indent](http://zakon.rada.gov.ua/laws/show/3475-15#n36) of Article 3 shall be replaced by the following:

‘participation in the formation and implementation of the public policy in the fields of electronic document exchange (in the context of protection of information of public authorities and local self-government bodies), electronic identification (using electronic trust services), electronic trust services (in the context of establishing the requirements for the information security and protection during the provision and use of electronic trust services, control over the compliance with the requirements of the legislation in the field of electronic trust services)’;

б) in the [first part](http://zakon.rada.gov.ua/laws/show/3475-15#n126) of Article 14:

[Point 2](http://zakon.rada.gov.ua/laws/show/3475-15" \l "n128" \t "_blank) shall be replaced by the following:

‘2) participation in the formation and implementation of the public policy in the fields of electronic document exchange (in the context of protection of information of public authorities and local self-government bodies), electronic identification (using electronic trust services), electronic trust services (in the context of establishing the requirements for the information security and protection during the provision and use of electronic trust services, control over the compliance with the requirements of the legislation in the field of electronic trust services)’;

[the third indent](http://zakon.rada.gov.ua/laws/show/3475-15" \l "n160" \t "_blank) of Point 29 shall be replaced by the following:

‘compliance with the requirements of the legislation in the field of electronic trust services’;

[Points 37](http://zakon.rada.gov.ua/laws/show/3475-15" \l "n170" \t "_blank) and [43](http://zakon.rada.gov.ua/laws/show/3475-15#n176) shall be replaced by the following:

‘37) establishing the requirements for the information security and protection applicable to the qualified providers of electronic trust services and their separate points of registration’;

‘43) coordinating the projects (objectives) of creation and development of information and telecommunication systems, special connection systems, electronic document exchange systems (in the context of information protection), within which the state information resources and the information, which protection is required by law, will be handled, the software and hardware systems of the providers of electronic trust services, the validation centre and the central validation authority (in the context of information protection), organizing the carrying out of expert assessment thereof’;

в) in the [first part](http://zakon.rada.gov.ua/laws/show/3475-15#n236) of Article 15:

[the fourth indent](http://zakon.rada.gov.ua/laws/show/3475-15" \l "n244" \t "_blank) of Point 5 shall be replaced by the following:

‘the qualified providers of electronic trust services, their separate points of registration, the validation centre, the central validation authority in respect of compliance with the requirements of the legislation in the field of electronic trust services’;

[Point 19](http://zakon.rada.gov.ua/laws/show/3475-15" \l "n265" \t "_blank) shall be replaced by the following:

‘19) apply to court where disputes arise on the matters of organizing special communication and information protection, cryptographic and technical protection of the state information resources and the information, which protection is required by law, disputes in the field of electronic trust services, as well as where other disputes arise, under the procedure established by law’.

4. The accredited centres for keys certification established under the [Law of Ukraine](http://zakon.rada.gov.ua/laws/show/852-15" \t "_blank) ‘On electronic digital signature’ and intending to provide qualified electronic trust services, shall automatically be added by the central validation authority to the Trusted List as the qualified providers of electronic trust services within a year from the date this Law enters into force.

5. The electronic digital signature and the advanced certificate for a public key confirming the former, which have been issued in accordance with the requirements of [the Law of Ukraine](http://zakon.rada.gov.ua/laws/show/852-15" \t "_blank) ‘On electronic digital signature’ prior to this Law entering into force, shall be used by the users of electronic trust services, the qualified providers of electronic trust services continuing to provide services to them, as being the qualified electronic signature and the qualified certificate for the electronic signature accordingly until the expiration of the validity period of the advanced certificate for the public key, but not later than within two years from the day this Law enters into force.

6. The data in electronic form with the electronic digital signature, applied thereto, which was confirmed by way of applying the advanced certificate for a public key, shall be considered, after the Law of Ukraine ‘On electronic trust services’ enters into force, but no later than within two years from the date this Law enters into force, to be the data in electronic form with the created qualified electronic signature.

7. Until the legislation is brought into compliance with this Law, the Laws of Ukraine and other legislative and regulatory acts shall apply to the extent not contradicting this Law.

8. The Cabinet of Ministers of Ukraine shall, within a year from the date this Law enters into force, do the following:

bring its own regulatory acts in compliance with this Law;

adopt the regulatory acts envisaged by this Law;

ensure that the regulatory acts of the Ministries and other central executive authorities shall be brought into compliance with this Law.

|  |  |
| --- | --- |
| **The President of Ukraine** | **P.POROSHENKO** |
| **City of Kyiv**  **5 October 2017**  **No. 2155-VIII** |  |