LAW OF UKRAINE

On Electronic Identification and Electronic Trust Services

(Bulletin of the Verkhovna Rada (BVR), 2017, No. 45, Article 400)

{As amended by Laws

No. 440-IX of 14.01.2020, Bulletin of the Verkhovna Rada of Ukraine, 2020, No. 28, Article 188

No. 1089-IX of 16.12.2020

No. 1591-IX of 30.06.2021 — effective since 01.08.2022

No. 2801-IX of 01.12.2022}

{The amendments under Law No. 1909-IX of 18.11.2021, which are effective since 01.01.2024, have not been made}

{Additionally see the amendments to the Law effective since 31.12.2023 in the Law No. 2801-IX of 01.12.2022}

This Law defines the legal and organisational principles for electronic identification and provision of electronic trust services, the rights and obligations of the parties of the legal relations in the field of electronic identification and electronic trust services, the procedure of carrying out the state control over the compliance with the requirements of the legislation in the field of electronic identification and electronic trust services.

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

Title I

GENERAL PROVISIONS

Article 1. Terms and definitions

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

1) ‘authentication’ shall mean an electronic procedure that enables the electronic identification of a natural, legal person, information or information and communication system and/or the origin and integrity of electronic data in electronic form;

2) ‘multi-factor authentication’ shall mean authentication by means of two or more authentication factors that pertain to different groups of authentication factors;

3) ‘blocking of the certificate for a public key’ shall mean temporary suspension of the validity of the certificate for a public key;

4) ‘website’ shall mean 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;

5) ‘public key’ (data to verify the electronic signature or electronic seal) shall mean the data used to verify the electronic signature or electronic seal;

6) ‘separate point of registration’ shall mean a representative office (branch, business unit, territorial body) of the provider of electronic identification services, the provider of electronic trust services or the legal or natural person, including a notary, which, based on the order from the provider of electronic identification services, the provider of electronic trust services (its director) or based on the agreement concluded with it, carries out the registration of the electronic identification users or signatories in compliance with the requirements of the legislation in the field of electronic identification, electronic trust services and information protection;

7) ‘wallet with digital identification’ shall mean the identification means that enables a user to furnish information on identification data upon third parties’ request, carry out electronic identification and authentication to provide the service, and create qualified electronic signatures and/or seals, and that has to meet the requirements of Article 15^{1} hereof;

8) ‘Trusted List’ shall mean the list of qualified providers of electronic trust services and the information on such providers and the electronic trust services they provide;

9) ‘documented information’ shall mean the documents based on which the users of electronic trust services were provided the electronic trust services, including the ones based on which the qualified certificates for public keys were created, blocked, renewed, cancelled, all the created qualified certificates for public keys as well as registries of the valid qualified certificates for public keys;

10) ‘electronic trust service’ shall mean a service that is provided in order to ensure electronic interaction of two or more parties, which commit the provision of such service to the provider of electronic trust services;

11) ‘electronic identification’ shall mean the process of using person identification data in electronic form which uniquely represent either a natural or a legal person, or an authorised representative of a legal person;

12) ‘electronic seal’ shall mean the data in electronic form that are attached to or logically associated with other data in electronic form and are used to identify the origin of related data in electronic form, or to certify electronic signatures of users in electronic documents, or to certify true copies of the documents and to identify integrity breaches;

13) ‘electronic time stamp’ shall mean the data in electronic form which bind other data in electronic form to a particular time in order to confirm that data in electronic form existed at that time;

14) ‘electronic service’ shall mean any service of providing a certain tangible or intangible benefit for the benefit of another person which is provided via an information and communication system;

15) ‘electronic signature’ shall mean the data in electronic form that are attached to, or logically associated with, other data in electronic form and are used by the signatory to sign;

16) ‘data in electronic form’ shall mean any information in electronic form;

17) ‘confirmation of validity of the public key’ shall mean the procedure of creation of the certificate for a public key;

18) ‘electronic signature or seal device’ shall mean a hardware and software device or a hardware device or software used in order to create the electronic signature or seal;

19) ‘electronic identification’ means shall mean a tangible and/or intangible item containing identification data of a person and used for authentication of a person in the information and communication systems;

20) ‘qualified electronic signature or seal device’ shall mean an electronic signature or seal device that meets the requirements laid down in paragraphs 1 to 4 of Article 19 of this Law;

21) ‘person identification data’ shall mean a unique set of data enabling to identify a natural, legal person or a representative of a legal person;

22) ‘person identification’ shall 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 an authorised representative of a legal person as well as verification of pertinence of such data to the person;

23) ‘interoperability’ shall mean technological compatibility of technical solutions that are used when providing electronic services and their ability to interact together;

24) ‘qualified electronic trust service of registered electronic delivery’ shall mean the registered electronic delivery that meets the requirements laid down in paragraph 1 of Article 27 of this Law;

25) ‘qualified electronic seal’ shall mean an advanced electronic seal that is created using a qualified electronic seal creation device and is based on a qualified certificate for an electronic seal;

26) ‘qualified electronic time stamp’ shall mean the electronic time stamp that meets the requirements laid down in paragraph 2 of Article 26 of this Law;

27) ‘qualified electronic signature’ shall mean an advanced electronic signature that is created using a qualified electronic signature creation device and is based on a qualified certificate for an electronic signature;

28) ‘qualified provider of electronic trust services’ shall mean a legal person, regardless of the legal and organisational form and form of ownership, an individual entrepreneur

providing one or more qualified electronic trust services, with the information thereon added to the Trusted List;

29) ‘qualified certificate for website authentication’ shall mean a certificate for website authentication that is issued by a qualified provider of electronic trust services, a validation centre or the central validation authority and meets the requirements laid down in paragraph 2 of Article 23 of this Law;

30) ‘qualified certificate for an electronic signature’ shall mean a certificate for an electronic signature that is issued by a qualified provider of electronic trust services and meets the requirements laid down in paragraph 2 of Article 23 of this Law;

31) ‘qualified certificate for an electronic seal’ shall mean a certificate for an electronic seal that is issued by a qualified provider of electronic trust services and meets the requirements laid down in paragraph 2 of Article 23 of this Law;

32) ‘compromise of an electronic identification means’ shall mean any event that has caused or is capable of causing unauthorised access to an electronic identification means;

33) ‘compromise of a personal key’ shall mean any event that has caused or is capable of causing unauthorised access to a personal key;

34) ‘users of the electronic trust services’ shall mean signatories, creators of electronic seals, senders 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;

35) ‘users of the electronic identification services’ shall mean natural and legal persons or authorised representatives of a legal person that use the electronic identification means, wallets with digital identification or receive the electronic identification services from the providers of such services in accordance with the requirements of this Law;

36) ‘provider of electronic trust services’ shall mean a legal person, regardless of the legal and organisational form and form of ownership, an individual entrepreneur providing one or more electronic trust services as a qualified or non-qualified provider of electronic trust services;

37) ‘provider of electronic identification services’ shall mean a legal person, regardless of the legal and organisational form and form of ownership, an individual entrepreneur that provides the electronic identification service based on the scheme on the list of the electronic identification schemes and can also register users of electronic identification means;

38) ‘non-qualified provider of electronic trust services’ shall mean a provider of electronic trust services whose data are not on the Trusted List and that meets the requirements set by the Cabinet of Ministers of Ukraine for the non-qualified providers of electronic trust services;

39) ‘conformity assessment authority’ shall mean an undertaking, an institution, an organisation or their units that carry out the conformity assessment activity, are accredited in accordance with the legislation in the field of accreditation or designated in accordance with the legislation on technical regulations and conformity assessment, as well as a foreign conformity assessment authority duly accredited by the foreign accreditation authorities that are signatories to the International Accreditation Forum Multilateral Recognition Arrangement and/or the European Accreditation (EA MLA);

40) ‘personal key’ (data to create an electronic signature or seal) shall mean unique data used by the signatory or creator of the electronic seal to create the electronic signature or seal;

41) ‘key pair’ shall mean the personal key and the public key corresponding to it, which are interconnected by the parameters;

42) ‘verification of the electronic signature or seal’ shall mean the process of verifying and validating the electronic signature or seal;

43) ‘verification of electronic identification’ shall mean the process of verifying and validating pertinence of the identification data to a natural or legal person or an authorised representative of a legal person;

44) ‘signatory’ shall mean a natural person who creates an electronic signature;

45) ‘renewal of the certificate for a public key’ shall mean the renewal of the validity of the previously blocked certificate for a public key;

46) ‘electronic identification service’ shall mean the service provided to ensure and verify electronic identification;

47) ‘software and hardware system used when providing electronic trust services’ (hereinafter the ‘software and hardware system’) shall mean the hardware and software, and software ensuring the exercising of the functions related to the provision of electronic trust services;

48) ‘registry of the valid, blocked and cancelled certificates for public keys’ shall mean 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;

49) ‘registered electronic delivery’ shall mean a service that makes it possible to transmit data in electronic form between third parties by electronic means, provide evidence of the processing 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 unauthorised alterations;

50) ‘self-signed certificate for an electronic seal’ shall mean a qualified certificate for an electronic seal issued by the central validation authority or the validation centre using the personal key of the central validation authority or the validation centre;

51) ‘website authentication certificate’ shall mean an electronic certificate that enables website authentication and links the website to the natural or legal person to which the certificate has been issued;

52) ‘certificate for an electronic signature’ shall mean an electronic certificate which links the electronic signature public key to a natural person and verifies at least the first name, patronymic (if any) and last name or the pseudonym of that person;

53) ‘certificate for an electronic seal’ shall mean an electronic certificate which links the electronic seal public key to the legal person carrying out the business activity and verifies the name of that person;

54) ‘cancellation of the certificate for a public key’ shall mean termination of the validity of the certificate for a public key;

55) ‘creator of an electronic seal’ shall mean a legal person or an individual entrepreneur that creates an electronic seal;

56) ‘electronic identification scheme’ shall mean a system for electronic identification under which electronic identification means are issued to natural, legal persons, or authorised representatives of legal persons;

57) ‘technological neutrality of the technical solutions’ shall mean prevention of establishment of the mandatory requirements for the technical solutions used in the process of electronic identification and provision of electronic trust services that can be satisfied only with one technology;

58) ‘advanced electronic seal’ shall mean an electronic seal that meets the requirements laid down in paragraph 1 of Article 17^1 of this Law;

59) ‘advanced electronic signature based on the qualified certificate for an electronic signature’ shall mean an advanced electronic signature that is created by means of the qualified certificate for an electronic signature issued by the qualified provider of electronic trust services, and contains no data that the personal key is kept in the qualified electronic signature device;

60) ‘authentication factor’ shall mean one of the attributes based on the knowledge (information (data) available to the user only) or possession (use of the tangible item possessed by the user only) or inherence (verification of biometric data or other properties (features, characteristics) that are inherent only to the user and distinguish it from the other users).

2. The other terms shall be used in the meanings referred to them in the Civil Code of Ukraine, the Laws of Ukraine ‘On electronic documents and electronic document exchange’, ‘On the protection of information in the information and communication systems’, ‘On standardisation’, ‘On technical regulations and conformity assessment’, ‘On the scientific and scientific and technical expertise’, ‘On the National Bank of Ukraine’.

{Article 1(2) as amended by Law No. 1089-IX of 16.12.2020}

Article 2. Scope of the Law

1. This Law regulates the relations arising between legal and natural persons, authorities in the process of providing and receiving electronic identification services, wallets with digital identification and electronic trust services, the procedure of provision of those services, supervision and control over the compliance with the requirements of the legislation in the field of electronic identification and electronic trust services.

This Law shall not apply to electronic identification and provision of electronic trust services in the systems that process service information and classified information as well as in the systems that are only used by the designated group of participants on a contractual basis for internal needs of legal or natural persons.

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

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

1. The relations related to electronic identification and provision of electronic trust services shall be regulated by the Constitution of Ukraine, the Civil Code of Ukraine, the Laws of Ukraine 'On Information', 'On the protection of information in the information and communication systems', 'On electronic documents and electronic document exchange', 'On the protection of personal data', this Law, as well as other legislative and regulatory acts.

{Article 3(1) as amended by Law No. 1089-IX of 16.12.2020}

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

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

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

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

ensuring free circulation of electronic identification services and electronic trust services in Ukraine, as well as allowing for the free provision of electronic identification services and electronic trust services by the providers of electronic identification services and the providers of electronic trust services not being residents of Ukraine provided that their services are consistent with the requirements of this Law;

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

ensuring access to, and the possibility of using, the electronic identification services and electronic trust services for persons with disabilities at the same level as other natural persons;

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

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

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

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

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

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

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

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

preventing monopolisation and creating conditions for the development of fair competition in the fields of electronic identification and electronic trust services;

ensuring protection of the personal data processed during provision of electronic identification services and electronic trust services in accordance with the legislation in the field of personal data protection;

carrying out the measures to promote electronic identification and electronic trust services among the public and legal persons;

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

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

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

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

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

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

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

Article 4[1]. Usage of pseudonyms in the fields of electronic identification and electronic trust services

1. When they are provided electronic identification services and electronic trust services, the natural persons being users thereof shall have the right to use a pseudonym instead of their first name, patronymic (if any) and last name in the cases prescribed by the law, provided that such usage is specified in the electronic identification means and certificates for public keys as prescribed by the Cabinet of Ministers of Ukraine.

2. Usage of a pseudonym shall not release the provider of electronic identification services, the provider of electronic trust services from the obligation to identify the natural person who intends to use the pseudonym, in accordance with the legislation in the fields of electronic identification and electronic identification services.

Title II

PARTIES TO THE RELATIONS IN THE FIELDS OF ELECTRONIC IDENTIFICATION AND ELECTRONIC TRUST SERVICES, AND AUTHORITIES IN CHARGE OF THE STATE REGULATION IN THE FIELDS OF ELECTRONIC IDENTIFICATION AND ELECTRONIC TRUST SERVICES

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

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

the Cabinet of Ministers of Ukraine;

the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services;

the designated central executive authority in charge of arranging special communication and information protection;

the National Bank of Ukraine.

Article 6. Powers of the Cabinet of Ministers of Ukraine in the fields of electronic identification and electronic trust services

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

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

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

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

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

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

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

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

2. The National Bank of Ukraine shall participate in drafting of the acts of the Cabinet of Ministers of Ukraine in the fields of electronic identification and electronic trust services.

Article 7. Powers of the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services

1. The powers of the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services shall include the following:

providing the administrative services of inclusion of the electronic identification scheme into the list of the electronic identification schemes, and introducing amendments to such list;

coordinating the plans for terminating the activity of qualified providers of electronic trust services;

carrying out state regulation in the field of electronic identification within its competence in accordance with this Law;

notifying the supervisory authority of the circumstances that interfere with the activity;

ensuring mutual recognition of the Ukrainian and foreign certificates for public keys and electronic signatures used to provide legally valid electronic services;

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

drafting laws and regulations in the fields of electronic identification and electronic trust services;

participating in drafting of the regulations and standards in the fields of electronic identification and electronic trust services, including to ensure the interoperability and technological neutrality of the technical solutions, as well as non-discrimination thereof;

drafting resolutions of the Cabinet of Ministers of Ukraine on the implementation and introduction of the initiatives to test the innovation schemes, means and technologies of electronic identification and electronic trust services as well as evaluation of the outcome of such initiatives;

considering proposals from the parties to the relations in the fields of electronic identification and electronic trust services concerning the improvement of the state regulation in the fields;

studying the progress and development prospects in the fields of electronic identification and electronic trust services, analysing information on activities of the qualified providers of electronic identification services, their separate points of registration and the validation centre, providers of electronic identification services, which is furnished in accordance with the prescribed procedure;

approving the operational regulations of the qualified providers of electronic trust services and legal persons, individual entrepreneurs that intend to provide electronic trust services, and sending copies of the documents to the supervisory authority;

analysing the documents on conformity of the providers of electronic trust services based on the conformity assessment procedures, following which the decision is taken to enter data thereon into the Trusted List;

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

2. The central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services shall perform the functions of the central validation authority by providing free administrative services of entering data on legal persons and individual entrepreneurs who intend to provide qualified electronic trust services into the Trusted List, and of amending the Trusted List.

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

Article 7[1]. Rights and obligations of the administrator of the information and communication system of the central validation authority and the integrated electronic identification system

1. The administrator of the information and communication system of the central validation authority and the integrated electronic identification system shall be in charge of technical and technological support of the following functions:

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

operation of the official websites of the central validation authority and the integrated electronic identification system;

operation of the electronic service to create, verify and validate the electronic signature and the electronic seal on the official websites of the central validation authority and the integrated electronic identification system, and consistency thereof with the requirements of Articles 18 and 19 of this Law;

maintenance of the Trusted List;

maintenance of the registry of the valid, blocked and cancelled certificates for public keys created by the central validation authority in accordance with the procedure established by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services;

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

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

use of the information and communication system of the central validation authority in order to validate and verify the Ukrainian and foreign certificates for public keys and electronic signatures used to provide legally valid electronic services, and the integrated electronic identification system for mutual recognition of the electronic identification schemes;

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

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

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 electronic communication networks;

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

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

processing and publication of findings of the analysis of the progress and development prospects in the fields of electronic identification and electronic trust services in accordance with the procedure established by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services;

creation, update and publication of the list of the electronic identification schemes on the website of the integrated electronic identification system;

conclusion of agreements on connection of the information and information and communication systems to the integrated electronic identification system;

exercise of other powers in the fields of electronic identification and electronic trust services as envisaged by the law.

2. Financial support of the administrator of the information and communication system of the central validation authority and the integrated electronic identification system for the purposes of technical and technological performance of the functions specified in paragraph 1 of this Article shall be carried out from the state budget.

Article 8. Powers of the designated central executive authority in charge of arranging special communication and information protection in the fields of electronic identification and electronic trust services

1. The designated central executive authority in charge of arranging special communication and information protection shall perform the functions of the supervisory authority in the fields of electronic identification and electronic trust services.

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

state control over the compliance with the requirements of the legislation in the fields of electronic identification and electronic trust services;

interaction with the central validation authority, the validation centre and the conformity assessment authorities on the matters of state control over the compliance with the requirements of the legislation;

cooperation with the personal data protection authorities by notifying without a delay of violations of the legislation in the field of personal data protection detected when carrying out inspections by the supervisory authority of the qualified provider of electronic identification services that implement the identification schemes as well as providers of electronic trust services;

notification of the public in case the providers of electronic identification services that implement the electronic identification schemes and the providers of electronic trust services provide information on a breach of confidentiality and/or integrity of information that influences provision of electronic identification services or electronic trust services or is associated with personal data of users of the electronic identification services or users of the electronic trust services, or in case such information is received during the inspection of such providers;

issue of instructions to remedy breaches of the requirements of the legislation in the fields of electronic identification and electronic trust services;

imposition of administrative fines for breaching the requirements of the legislation in the fields of electronic identification and 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 within the state supervision (control) desk activities.

Article 9. Powers of the National Bank of Ukraine in the fields of electronic identification and electronic trust services

1. The National Bank of Ukraine shall create a validation centre to ensure that data on the banks, other entities operating on the financial services markets subject to state regulation and supervision by the National Bank of Ukraine, on the payment system operators and/or

payment system participants, technical payment service providers that intend to provide qualified electronic trust services in accordance with this Law are added to the Trusted List.

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 data on which are on the Trusted List, based on the decision of the validation centre using a self-signed certificate for an electronic seal 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 identification and electronic trust services shall include the following:

establishing the requirements for providing and using electronic trust services in the banking system of Ukraine and on the markets of non-bank financial services subject to state regulation and supervision by the National Bank of Ukraine as well as for providing payment services;

establishing the requirements for time synchronisation in the software and hardware systems of the qualified providers of electronic trust services specified in the first indent of paragraph 1 of this Article;

approving the operational regulations and amendments thereto of the entities specified in the first indent of paragraph 1 of this Article, and sending copies of such documents to the supervisory authority;

notifying the supervisory authority of the circumstances that interfere with the activity of the validation authority;

approving the plans for termination of activities of the qualified providers of electronic trust services specified in the first indent of paragraph 1 of this Article;

adopting legislative and regulatory acts on operation of the regulatory platform to test services, technologies and instruments at the financial services markets based on the innovative technologies, with the electronic identification schemes, means and technologies and electronic trust services;

carrying out state regulation in the field of electronic identification in the banking system of Ukraine and on the markets of non-bank financial services subject to state regulation and supervision by the National Bank of Ukraine as well as when providing payment services;

exercising other powers prescribed by the law in the fields of electronic identification and electronic trust services in the banking system of Ukraine and on the markets of non-

bank financial services subject to state regulation and supervision by the National Bank of Ukraine as well as when providing payment services.

4. While providing electronic trust services, the validation centre shall meet the requirements established for the qualified providers of electronic trust services added to the Trusted List based on the decision of the validation centre.

5. The software and hardware system of the validation centre used by it to provide electronic trust services shall meet the requirements established for the software and hardware systems of the qualified providers of electronic trust services added to the Trusted List based on the decision of the validation centre.

6. The organisational and methodological, technical and technological conditions of the activities of the validation centre in provision of the qualified electronic trust services, the procedure of interaction of the qualified providers of electronic trust services with the validation centre in provision of 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 approved by the National Bank of Ukraine.

7. The National Bank of Ukraine shall keep accounts of the banks being qualified providers of electronic trust services, the validation centre, the qualified provider of electronic trust services established by the National Bank of Ukraine, in order to keep funds for indemnification for the damages that might result from a default by the bank being a qualified provider of electronic trust services, a validation centre.

Article 10. *(Deleted)*

Article 11. Parties to the relations in the fields of electronic identification and electronic trust services

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

the users of electronic identification services;

the providers of electronic identification services;

the owners (holders) of the information and information and communication systems;

the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services;

the supervisory authority;

the National Bank of Ukraine.

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

the users of the electronic trust services;

the providers of electronic trust services;

the owners (holders) of the information and information and communication systems;

the holders of public electronic registers;

the conformity assessment authorities;

the validation centre;

the central validation authority;

the supervisory authority.

Article 11[1]. Rights and obligations of the users of electronic identification services

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

receive electronic identification services;

be free to choose the provider of electronic identification services with the respective assurance level to receive electronic services;

exercise sole control over use of the wallet with digital identification and their data;

be free to use the deliverables of electronic identification services with account of the restrictions set by the legislation and providers of electronic identification services;

challenge in judicial proceedings the actions or omission of the providers of electronic identification services and the authorities in charge of the state regulation in the field of electronic identification;

obtain compensation for the damages inflicted and the protection of their rights and lawful interests.

2. The users of electronic identification services shall:

ensure confidentiality and no unauthorised access of other persons to the electronic identification means;

promptly notify the provider of electronic identification services of the suspected or confirmed compromise of the electronic identification means;

provide reliable information necessary to receive electronic identification services;

timely furnish the provider of electronic identification services with the information on the change of the identification data contained in the electronic identification means;

not use the electronic identification means that has been compromised.

3. The protection of the rights of users of electronic identification services, as well as the mechanism of exercising the protection of those rights shall be regulated by this Law and the Law of Ukraine ‘On consumer rights protection’.

Article 11[2]. Rights and obligations of the providers of electronic identification services

1. The providers of electronic identification services shall have the right to:

provide electronic identification services in accordance with the requirements of the legislation in the field of electronic identification;

receive the documents and/or data in electronic form necessary to identify the person whose identification data will be contained in the electronic identification means;

submit inquiries to the competent public authorities in order to verify and validate the person identification data contained in the electronic identification means;

while issuing electronic identification means, verify information on the persons to which such means are issued, based on data from the information resources of the unified information system of the Ministry of Internal Affairs of Ukraine (data in the Unified State Demographic Register, and data on the documents stolen (lost), upon citizens' requests), the State Register of Individual Tax Payers, the State Register of Vital Records, the Unified State Register of Legal Entities, Individual Entrepreneurs and Public Organisations as well as information from other public electronic registers in accordance with the Law of Ukraine 'On public electronic registers' obtained during the electronic interaction by means of the integrated electronic identification system, as prescribed by the Cabinet of Ministers of Ukraine;

obtain consultations with the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services, on the matters relating to the provision of electronic identification services, the designated central executive authority in charge of arranging special communication and information protection in the fields of electronic identification and electronic trust services, the National Bank of Ukraine;

apply to the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services for inclusion of the electronic identification schemes being implemented by them into the list of the electronic identification schemes.

2. If provision of a certain electronic identification service pertains to the obligations of the provider of electronic identification services prescribed by the legislation, it may not refuse to provide such service on the grounds that are not laid down in the law.

3. The providers of electronic identification services shall ensure the following:

conformity of the electronic identification means to the prescribed assurance levels;

protection of personal data of the users of electronic identification services in accordance with the requirements of the Law of Ukraine 'On personal data protection';

creation and operation of their website; protection of information in the information and communication system used to provide the electronic identification services, in accordance with the legislation on information protection;

identification of natural and legal persons or authorised representatives of legal persons in provision of the electronic identification services; introduction of the identification data of the user of the electronic identification services to the respective electronic identification means;

appropriate organisational and technical risk management activities in connection with security of the electronic identification services;

notification of the supervisory authority and, where necessary, the authority in charge of personal data protection, on a breach of the confidentiality and/or integrity of the information that influences the provision of electronic identification services or is associated with personal data of the users of electronic identification services, without an undue delay, within 24 hours from the moment they become aware of such breach;

notification of the users of the electronic identification services on a breach of the confidentiality and/or integrity of the information that influences the provision of electronic identification services to them or is associated with their personal data, without an undue delay, within two hours from the moment they become aware of such breach;

making it impossible to use the electronic identification means issued by the provider of electronic identification services if it has found out that the respective electronic identification means has been compromised;

permanent storage of documents and data in electronic form received during registration of electronic identification means.

4. In addition to the obligations specified in paragraph 3 of this Article, the providers of electronic identification services with the high or medium assurance level shall also ensure clear and exhaustive notification of any person that has requested an electronic identification service on the terms and conditions for using the service, including any restrictions in use thereof, before the agreement on the provision of the electronic identification services is concluded.

5. The requirements for the providers of electronic identification services, their separate points of registration, including the requirements for information security and protection, as well as the procedure for inspecting how they are met, the procedure for notifying the supervisory authority and users of the electronic identification services shall be established by the Cabinet of Ministers of Ukraine.

Article 12. Rights and obligations of the users of electronic trust services

1. Users of the electronic trust services shall have the right to:

receive electronic trust services;

be free to choose a provider of electronic trust services;

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

obtain compensation for the damages inflicted and the protection of their rights and lawful interests;

apply for cancelling, blocking or renewing their certificate for a public key;

be free to use the deliverables of electronic trust services with account of the restrictions set by the legislation and providers of electronic trust services.

2. The users of the electronic trust services shall:

ensure confidentiality and no unauthorised access of other persons to the personal key;

promptly notify the provider of electronic trust services of the suspected or confirmed compromise of the personal key;

provide reliable information necessary to receive electronic trust services;

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;

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

not use the personal key if it has been compromised, or the certificate for a public key has been cancelled or blocked.

3. The protection of the rights of 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 ‘On consumer rights protection’.

Article 13. Rights and obligations of the providers of electronic trust services

1. The providers of electronic trust services shall have the right to:

provide electronic trust services in accordance with the requirements of the legislation in the field of electronic trust services;

receive the documents and/or data in electronic form necessary to identify the person whose identification data will be contained in the certificate for a public key;

while creating and issuing qualified certificates for public keys, verify information on the persons to which such certificates are issued, based on data from the information resources of the unified information system of the Ministry of Internal Affairs of Ukraine (data in the Unified State Demographic Register, and data on the documents stolen (lost), upon citizens’ requests), the State Register of Individual Tax Payers, the State Register of Vital Records, the unified information system of the Ministry of Internal Affairs of Ukraine (data on the documents stolen (lost), upon citizens’ requests), the Unified State Register of Legal Entities, Individual Entrepreneurs and Public Organisations as well as information from other public electronic registers in accordance with the Law of Ukraine ‘On public electronic registers’ obtained during the electronic interaction by means of the integrated electronic identification system, as prescribed by the Cabinet of Ministers of Ukraine;

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

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

submit an application to create, cancel, block or renew the qualified certificates for public keys to the central validation authority or the validation centre.

2. In addition to the rights laid down in paragraph 1 of this Article, the qualified providers of electronic trust services shall also be free to choose within each service, from the list of standards determined by the Cabinet of Ministers of Ukraine, which specific standards will be applied by them when providing the qualified electronic trust services.

3. If provision of a certain electronic trust service pertains to the obligations of the provider of electronic trust services prescribed by the legislation, it may not refuse to provide such service on the grounds that are not laid down in the law.

4. The providers of electronic trust services shall ensure the following:

protection of personal data of the users of electronic trust services in accordance with the requirements of the Law of Ukraine ‘On personal data protection’;

operation of the information and communication system and the software and hardware system used by them to provide electronic trust services, and the protection of the information processed within it, in accordance with the requirements of the legislation on electronic trust services;

creation and operation of their website;

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

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 communication networks;

round-the-clock acceptance and verification of electronic applications from the signatories and creators of electronic seals for cancellation, blocking and renewal of their certificates for public keys; acceptance and verification of applications in hard copy from the signatories and creators of electronic seals for cancellation, blocking and renewal of their certificates for public keys within one business day upon receipt of the application, in accordance with the working hours of the provider of electronic trust services;

cancellation, blocking and renewal of the 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;

inclusion of the identification data of the signatory or creator of the electronic seal to the relevant certificate for a public key;

organisational and technical risk management activities in connection with security of the electronic trust services;

notification of the supervisory authority and, where necessary, the authority in charge of personal data protection, on a breach of the confidentiality and/or integrity of the information that influences the provision of electronic trust services or is associated with personal data of the users of electronic trust services, without an undue delay, within 24 hours from the moment they become aware of such breach, in accordance with the procedure established by the Cabinet of Ministers of Ukraine;

notification of the users of the electronic trust services on a breach of the confidentiality and/or integrity of the information that influences the provision of electronic trust services or is associated with personal data of the users of electronic trust services, without an undue delay, within two hours from the moment they become aware of such breach, in accordance with the procedure established by the Cabinet of Ministers of Ukraine;

prevention of use of the personal key of the signatory or creator of the electronic seal if it has been found out that the personal key has been compromised, or if the personal key of the signatory or creator of the electronic seal is kept by the provider of electronic trust services within the service of creation, verification and validation of the electronic signature or electronic seal;

permanent storage of all issued qualified certificates for public keys;

permanent storage of all issued qualified certificates for public keys;

permanent storage of documents and data in electronic form received in connection with provision of electronic trust services. The list of such documents shall be established by the Cabinet of Ministers of Ukraine.

5. In addition to the obligations laid down in paragraph 4 of this Article, the qualified providers of electronic trust services shall also ensure the following:

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 the account with the National Bank of Ukraine — for the banks being qualified providers of electronic trust services, the qualified provider of electronic trust services established by the National Bank of Ukraine) in order to ensure compensation for damages that can be caused to the users of electronic trust services or to third persons as a result of default by the qualified provider of the electronic trust services, or insuring civil legal liability in order to ensure compensation for such damages in the amount specified by the paragraph 16 of Article 16 of this Law;

replenishing the amount deposited 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 the account with the National Bank of Ukraine — for the banks being qualified providers of electronic trust services, the qualified provider of electronic trust services established by

the National Bank of Ukraine, or the coverage set by paragraph 5 of Article 16 of this Law, within three months in case the minimum wage is changed, or in case of compensation for the losses inflicted upon the users of the electronic trust services or third parties as a result of the default;

using, during the provision of the qualified electronic trust services, exclusively the qualified certificates for public keys created by the central validation authority or the validation centre;

hiring employees and, where necessary, subcontractors that possess the knowledge, experience and expertise necessary to provide the electronic trust services, and applying the administrative and management procedures consistent with the national and international standards;

ensuring clear and exhaustive notification of any person that has requested an electronic trust service on the terms and conditions for using the service, including any restrictions in use thereof, before the agreement on the provision of the electronic trust services is concluded;

notifying the supervisory authority and the central validation authority or the validation centre of the intention to terminate the activity and of any changes in the provision of qualified electronic trust services within 48 hours from the moment such changes take effect;

transferring the central validation authority, the validation centre or the other qualified provider of electronic trust services the documented information in the event of termination of the activity of providing qualified electronic trust services;

joining the programme interface of the information and communication system of the central validation authority in order to ensure the interoperability, study the progress and development prospects in the field of electronic trust services, and performing other powers laid down in Articles 7 and 7^1 of this Law, in case such provider of electronic trust services acquires the status of a qualified one based on the decision of the central validation authority.

6. The requirements for the providers of electronic trust services, including the requirements for information security and protection and employees of the provider of electronic trust services, and their separate points of registration and the procedure for inspection thereof shall be established by the Cabinet of Ministers of Ukraine.

The requirements for the providers of electronic trust services and their separate points of registration, including the requirements for information security and protection and employees of the provider of electronic trust services, that provide qualified electronic trust services in the banking system of Ukraine and on the markets of non-bank financial services subject to state regulation and supervision by the National Bank of Ukraine as well as in provision of payment services shall be established by the National Bank of Ukraine.

The providers of electronic trust services that provide qualified electronic trust services in the banking system of Ukraine and on the markets of non-bank financial services subject to state regulation and supervision by the National Bank of Ukraine as well as in provision of

payment services shall meet the requirements established by the Cabinet of Ministers of Ukraine and the National Bank of Ukraine.

7. The list of the changes in provision of qualified electronic trust services whereof the qualified providers have to inform the supervisory authority and the central validation authority or the validation centre shall be established by the Cabinet of Ministers of Ukraine.

Title III

ELECTRONIC IDENTIFICATION

Article 14. Electronic identification

1. Electronic identification shall be carried out via the electronic identification means and the authentication procedure falling under the electronic identification schemes.

2. The conformity of the electronic identification means (except for the ones specified in the first indent of paragraph 3 of Article 15 of this Law) to the low, medium or high assurance level shall be established based on the findings of the conformity assessment procedures with account of paragraph 4 of Article 15 of this Law as well as the requirements of the Law of Ukraine 'On technical regulations and conformity assessment'.

3. The owners (holders) of the information and information and communication systems that are used to provide electronic trust services, to send and receive data in electronic form, with information therein owned by the public authorities, authorities of the Autonomous Republic of Crimea, local self-government bodies, other public entities, shall use electronic identification means with the medium or high assurance level for the purposes of authentication in the systems following the assessment of risks and effects of unlawful use or spoofing of the identity of the users of the electronic identification services. The owners (holders) of the information and information and communication systems that are used to provide electronic trust services, to send and receive data in electronic form, with information therein owned by the public authorities, authorities of the Autonomous Republic of Crimea, local self-government bodies, other public entities, shall assess risks and effects of unlawful use or spoofing of the identity of the users of the electronic identification services in accordance with the procedure prescribed by the Cabinet of Ministers of Ukraine while selecting the electronic identification means with the medium or high assurance level.

4. The owners (holders) of the information and information and communication systems that are used to provide electronic services, to send and receive data in electronic form, with information therein owned by the public authorities, authorities of the Autonomous Republic of Crimea, local self-government bodies, other public entities that ensure authentication in the systems shall:

ensure protection of information in the information or information and communication system in accordance with the legislation;

take actions to assess risks in accordance with the legislation;

inform the supervisory authority of providing electronic services with the electronic identification means in accordance with the procedure established by the Cabinet of Ministers of Ukraine;

inform the supervisory authority of establishing the fact of unauthorised access to information during provision of electronic services with the electronic identification means without an unreasonable delay, within 24 hours after they found out of such violation.

Article 15. Assurance levels of the electronic identification means and schemes

1. The electronic identification schemes shall maintain the low, medium and/or high assurance level of the electronic identification means issued within the framework of the corresponding electronic identification means.

2. The low, medium and/or high assurance level of the electronic identification means shall meet the following criteria:

the low assurance level of electronic identification means shall refer to the 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 characterised with reference to the technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of unlawful use or spoofing the identity;

the medium assurance level of electronic identification means shall refer to the 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 characterised with reference to the technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to substantially decrease the risk of unlawful use or spoofing the identity;

the high assurance level of electronic identification means shall refer to the electronic identification means in the context of an electronic identification scheme, which provides the higher degree of confidence in the claimed or asserted identification data than the electronic identification means with the medium assurance level, and is characterised with reference to the technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent unlawful use or spoofing the identity.

3. The use of the qualified electronic signatures and seals ensures the high assurance level of electronic identification means that are used to create such electronic signatures and seals, as well as of electronic identification schemes within which the corresponding electronic identification means are issued.

The use of the qualified electronic signatures and seals based on the qualified certificates for public keys ensures the medium assurance level of electronic identification means that are used to create such electronic signatures and seals, as well as of electronic identification schemes within which the corresponding electronic identification means are issued.

4. The technical regulation on the requirements for electronic identification means in the context of the electronic identification scheme and the procedures applied to establish the assurance level of electronic identification means shall be approved by the Cabinet of Ministers of Ukraine.

Article 15[1]. Wallets with digital identification

1. Wallets with digital identification shall be issued in accordance with the electronic identification scheme pursuant to the requirements prescribed by the Cabinet of Ministers of Ukraine.

2. Conformity of wallets with digital identification to the valid requirements shall be established by the conformity assessment authority accredited in accordance with the accreditation legislation, as prescribed by the Cabinet of Ministers of Ukraine.

3. The central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services shall provide administrative services of inclusion of wallets with digital identification into the list of electronic identification schemes, wallets with digital identification, and amendments thereto.

4. The results of receiving and using wallets with digital identification shall be recognised by all the users of such services, other natural and legal persons.

5. If a wallet with digital identification is used to create the qualified electronic signature or seal, it shall meet the requirements for qualified electronic signature or seal devices.

Article 15[2]. List of electronic identification schemes

1. The central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services shall provide free administrative services of inclusion of the electronic identification scheme into the list of electronic identification schemes, wallets with digital identification, and amendments thereto.

The procedure for keeping the list of electronic identification schemes, wallets with digital identification shall be approved by the Cabinet of Ministers of Ukraine.

In order to obtain the administrative services of inclusion of the electronic identification scheme into the list of electronic identification schemes, amendments thereto, the applicants shall submit documents in hard or soft copy, including via the integrated electronic identification system.

2. The providers of electronic identification services shall submit the following documents to the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services for inclusion of the electronic identification schemes being implemented by them into the list of the electronic identification schemes:

1) application for including the electronic identification scheme into the list of electronic identification schemes in the format prescribed by the central executive authority ensuring the

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

2) identification document of the individual entrepreneur or representative of the legal person that provides electronic identification services (if documents are submitted in hard copy);

3) description of the electronic identification scheme in the format prescribed by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services;

4) conformity assessment document on conformity of the electronic identification means issued within the framework of the corresponding electronic identification scheme to the low, medium or high assurance level;

5) data on separate points of registration (if electronic identification services under the corresponding electronic identification scheme are to be provided via separate points of registration).

The document specified in point 4 of this paragraph is not submitted by the qualified providers of electronic trust services. The documents specified in point 5 of this paragraph are not submitted by the qualified providers of electronic trust services in case information in such documents does not differ from the information submitted to include data on such qualified providers of electronic trust services into the Trusted List.

3. After the documents are considered, the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services shall, within fifteen (15) business days upon registration of the application for including the electronic identification scheme into the list of electronic identification schemes, resolve to include the electronic identification scheme into the list of electronic identification schemes or send the applicant a justified refusal.

4. The central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust decision shall resolve to refuse to include the electronic identification scheme into the list of electronic identification schemes in the field of electronic governance in case:

the documents laid down in paragraph 2 of this Article are not submitted in full, or the requirements for the documents submitted are violated;

unreliable data, damage that hinders unambiguous interpretation of the content, corrections or additions are detected in the documents being submitted to include the electronic identification scheme into the list of electronic identification schemes.

5. In case the data submitted by the provider of electronic identification services for inclusion of the electronic identification scheme that is implemented by such provider and is on the list of electronic identification schemes into the list of electronic identification schemes change, the provider of electronic identification services shall, within five business days following such change, submit an application for amending the list of electronic

identification schemes and the documents certifying the corresponding changes to the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

In case the deadlines for submission of the documents to amend the list of electronic identification schemes are missed, the provider of electronic identification services may not provide the electronic identification services under the electronic identification scheme(s) included into the list of electronic identification schemes until the applicable amendments are made to the list. The central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services shall, within five business days following the registration of the application for amending the list of electronic identification schemes, introduce corresponding amendments into such list or furnish a justified refusal. The central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services furnishes justified refusal to amend the list of electronic identification schemes in case:

the documents being a basis for corresponding amendments to the list of electronic identification schemes are not submitted, or the requirements for the documents submitted are violated;

unreliable data, damage that hinders unambiguous interpretation of the content, corrections or additions are detected in the application and/or documents being submitted to amend the list of electronic identification schemes.

6. The central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust decision shall add information on termination of the operation of the electronic identification scheme into the list of electronic identification schemes in case:

a statement of termination of the operation of the electronic identification scheme being implemented is received from the provider of electronic identification services;

the recommendation of the supervisory authority to terminate the operation of the electronic identification scheme based on the inspection of compliance with the legislation in the field of electronic identification is received;

the information or document that certifies the following is received: state registration of termination of the entrepreneurial activity of the individual entrepreneur or winding-up of the legal person that providers electronic identification services; death of the individual entrepreneur that provides electronic identification services;

entry into force of the court judgement terminating the operation of the electronic identification scheme, declaring the individual entrepreneur that provides electronic identification services deceased, missing, legally incapable, limiting his/her civil capacity, or declaring the provider of electronic identification services bankrupt.

A decision to termination the operation of the electronic identification scheme shall be taken within five business days upon registration of the corresponding application, submission or confirmation document.

7. The central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust decision shall publish information on termination of the operation of the electronic identification scheme at latest on the next business day after it is taken by:

posting the relevant information on its official website;

sending the provider of electronic identification services a notice of the decision taken, with the grounds specified.

Article 15[3]. Integrated electronic identification system

1. The integrated electronic identification system is the information and communication system designated for technological support of the convenient, accessible and safe electronic identification and authentication of its users, compatibility and integration of the electronic identification schemes, interaction thereof with the information and information and communication systems of the public authorities, local self-government bodies, natural persons, individual entrepreneurs and persons performing their independent occupational activity, protection of information and personal data by means of the uniform requirements, formats, protocols and classifiers as well as satisfaction of other legislative needs.

2. The integrated electronic identification system is owned by the State.

The integrated electronic identification system is held by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

The technical administrator of the integrated electronic identification system is the state-owned enterprise subordinated to the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

3. The Regulation on the integrated electronic identification system shall be approved by the Cabinet of Ministers of Ukraine.

4. Connection of the information and information and communication systems to the integrated electronic identification system shall be based on the agreement made with the technical administrator of the system.

The fee shall be paid for connection of the information and information and communication systems (except for the ones used to provide the electronic identification services and qualified electronic trust services) to the integrated electronic identification system and use of resources of the integrated electronic identification system by the services providers (except for the electronic identification services and qualified electronic trust services) in the amounts set by the central executive authority ensuring the formation of and

implementing the public policy in the fields of electronic identification and electronic trust services.

The fee for connection to the integrated electronic identification system and use of its resources shall not be paid by the public authorities, the National Bank of Ukraine, the Security Service of Ukraine, the National Council of Television and Radio Broadcasting of Ukraine, the Central Election Commission of Ukraine and other public authorities, authorities of the Autonomous Republic of Crimea, local self-government bodies as well as the Office of the President of Ukraine, the National Council of Television and Radio Broadcasting of Ukraine, the Secretariat of the Verkhovna Rada of Ukraine, the Secretariat of the Cabinet of Ministers of Ukraine, the Secretariat of the Ukrainian Parliament Commissioner for Human Rights, the Prosecutor General's Office, the General Staff of the Armed Forces of Ukraine, the main military administrative authority of the National Guard of Ukraine, the State Employment Centre, the Social Insurance Fund, state institutions and facilities.

5. Personal data shall be processed by the integrated electronic identification system in accordance with the requirements of the Law of Ukraine 'On personal data protection'.

6. Authentication in the information and information and communication systems that are used to provide electronic services, to send and receive data in electronic form, with information therein owned by the public authorities, other governmental authorities, authorities of the Autonomous Republic of Crimea, local self-government bodies shall be carried out by means of the integrated electronic identification system.

This requirement shall not apply to the information and information and communication systems that use the electronic identification schemes compatibility or integration of which is not supported with the integrated electronic identification system in order to provide electronic services, send and receive data in electronic form.

Article 15[4]. Initiatives to test the innovation schemes, means and technologies of electronic identification

1. The Cabinet of Ministers of Ukraine may take a decision to implement the initiatives to test the innovation schemes, means and technologies of electronic identification.

2. Implementation of the initiatives to test the innovation schemes, means and technologies of electronic identification can provide for resolutions of the Cabinet of Ministers of Ukraine on the matters associated with electronic identification.

Resolutions of the Cabinet of Ministers of Ukraine on implementation of the initiative to test the innovation schemes, means and technologies of electronic identification shall specify the time frames for the experiment, its participants, the executive authority responsible for controlling the experiment, description of the controlled environment where tests are run, and experimental rules of the legislation in the field of electronic identification to be applied to govern the relations associated with implementation of the corresponding initiatives.

3. The period of implementation of the initiatives to test the innovation schemes, means and technologies of electronic identification may not exceed two years. By the decision of the

Cabinet of Ministers of Ukraine, implementation of the initiative may be extended by the period necessary to make the rules limited by the area and term of implementation of the corresponding initiative general and permanent, but in any case for no more than two years.

4. The central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services together with the interested executive authorities, other public authorities shall draft resolutions of the Cabinet of Ministers of Ukraine on implementation of the initiatives to test the innovation schemes, means and technologies of electronic identification and submit proposals on improvement of the legislation in the field of following the assessment of the outcome of such initiatives in accordance with the established procedure.

Title IV

ELECTRONIC TRUST SERVICES

Article 16. Requirements applicable to electronic trust services

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

2. The electronic trust services shall consist of the following: creation, verification and validation of the advanced electronic signature or seal; creation, verification and validation of the certificate for an electronic signature or seal; creation, verification and validation of the certificate for website authentication; creation, verification and validation of the electronic time stamp; registered electronic delivery; storage 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 either separately or in combination.

3. The qualified electronic trust services shall consist of the following: creation, verification and validation of the qualified electronic signature or seal; creation, verification and validation of the qualified certificate for an electronic signature or seal; creation, verification and validation of the qualified certificate for website authentication; creation, verification and validation of the qualified electronic time stamp; electronic trust service of registered electronic delivery; storage of the advanced electronic signatures, seals, electronic time stamps and certificates related to those services. Each service pertaining to the list of the qualified electronic trust services may be provided either separately or in combination only by the qualified provider of electronic trust services, the validation centre and the central validation authority.

4. In case it is technically possible, electronic trust services and hardware and software devices and software used to provide electronic trust services and designated for end users of such services shall be made accessible for persons with disabilities.

5. The activities of the qualified providers of electronic trust services shall be performed provided that funds are deposited 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 the account with the National Bank of Ukraine — for the banks being qualified providers of

electronic trust services, the qualified provider of electronic trust services established by the National Bank of Ukraine) in order to ensure compensation for damages that can be caused to the users of electronic trust services or to third persons as a result of default by the qualified provider of the electronic trust services, or insuring civil legal liability in order to ensure compensation for such damages. The amount of deposit on 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 the coverage shall be at least one thousand salaries.

6. The distribution of risks of losses 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 to the Trusted List by the central validation authority shall be determined by the parties to the legal relations on a contractual basis.

Article 17. Use of electronic trust services

1. The electronic interaction of natural and legal persons that requires the sending, receiving, use and permanent storage of data in electronic form and involves third persons can be performed with or without electronic trust services.

2. The public authorities, authorities of the Autonomous Republic of Crimea, local self-government bodies, other public entities and officials thereof shall use the qualified electronic signatures and seals as well as electronic signatures and seals based on the qualified certificates for public keys.

The President of Ukraine, the Members of Parliament of Ukraine, the members of the Cabinet of Ministers of Ukraine, heads, deputy heads, officials of the public authorities, other public entities as well as state registrars, notaries and other entities authorised by the state to perform the functions of the state registrar for the purpose of registration and other actions shall use only the qualified electronic signatures provided that such persons use the electronic signature to exercise their powers associated with acquiring, altering or terminating rights and/or obligations of natural and legal persons in accordance with the law.

The law may prescribe binding use of the qualified electronic trust services in other areas of public relations.

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 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 central executive authority ensuring the formation of and implementing the public policy in the field of the 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 deeds subject to notarisation 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.

7. The legal force and admissibility of the electronic signature or seal as evidence may not be denied only on the ground that it is in electronic form or is inconsistent with the requirements for the qualified electronic signatures or seals.

The legal force and admissibility of the electronic time stamp as evidence may not be denied only on the ground that it is in electronic form or is inconsistent with the requirements for the qualified electronic signatures or seals.

The legal force and admissibility of the data in electronic form sent and received by means of the electronic trust service of registered electronic delivery as evidence may not be denied only on the ground that they are in electronic form or are inconsistent with the requirements for the qualified electronic trust service of registered electronic delivery.

8. The results of providing the qualified electronic trust services consistent with the requirements of this Law shall be acknowledged by all users of those services and other natural and legal persons.

Public authorities, local self-government bodies, state-owned enterprises, establishments and organisations shall ensure use of results of providing the qualified electronic trust services from all the qualified providers of electronic trust services.

Article 17[1]. Requirements for advanced electronic signatures and seals

1. An advanced electronic signature or seal shall meet the following requirements:

it has to be uniquely linked to the signatory or creator of the electronic seal;

it has to be capable of identifying the signatory or creator of the electronic seal;

it has to be created with the public key that can be used by the signatory or creator of the electronic seal with the high assurance level under its sole control;

it has to be linked to the data in electronic form signed or sealed with the advanced electronic signature or seal so that any subsequent change in such data can be detected.

2. The Cabinet of Ministers of Ukraine lays down the requirements for formats of the advanced electronic signatures and seals used to provide electronic public services.

3. The Cabinet of Ministers of Ukraine lays down the requirements for creating and verifying the advanced electronic signatures based on the qualified certificates for public keys.

4. The National Bank of Ukraine shall have the right to lay down the requirements for formats of the advanced electronic signatures and seals used in the banking system of Ukraine and on the markets of non-bank financial services subject to state regulation and supervision by the National Bank of Ukraine as well as in provision of payment services.

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

1. The qualified electronic trust service of 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:

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

provision, to the signatories and/or creators of the electronic seal, of the right to use qualified electronic signature or seal devices hosted with the qualified provider of electronic trust services that generates and/or manages the key pair on behalf of the signatory or creator of the electronic signature;

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:

use of the qualified certificate for an electronic signature or seal to create the qualified electronic signature or seal in accordance with the requirements laid down in paragraph 2 of Article 23 of this Law;

issue of the qualified certificate for an electronic signature or seal by the qualified provider of electronic trust services and validity thereof as of the date of creation of the qualified electronic signature or seal; conformity of the value of the public key to its value specified in the qualified certificate for an electronic signature or seal;

proper entry of the unique data set that identifies the signatory or the creator of electronic seal into the qualified certificate of the electronic signature or seal;

reference to use of the pseudonym in the qualified certificate for an electronic signature (in case it is used by the person when the qualified electronic signature is created);

confirmation that the personal key used to create the qualified electronic signature or seal is stored within the qualified electronic signature or seal device;

no breach of integrity of the data in electronic form to which this qualified electronic signature or seal is linked;

adherence to the requirements laid down in paragraph 1 of Article 17^{1} of this Law as of the date of creation of the qualified electronic signature or seal.

When the qualified electronic trust service of creation, verification and validation of qualified electronic signature or seal is provided, the Trusted List is used to verify the status of the qualified electronic trust service provided by such qualified provider of electronic trust services.

3. The information and information and communication system used to validate the qualified electronic signature or seal shall give the user the adequate result of the validation process and enable the user to detect any security-related issues.

4. The qualified electronic trust service of creation, verification and validation of the qualified electronic signature or seal shall only be provided by the qualified providers of electronic trust services, which:

ensure validation of the qualified electronic signature or seal in accordance with the requirements laid down in paragraph 2 of this Article;

give an opportunity to any persons to obtain the result of the verification process at least by means of the advanced electronic signature or the advanced electronic seal of the qualified provider of electronic trust services in an automated manner.

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

6. 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.

7. 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 linked.

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

9. 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 that 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. Qualified electronic signature or seal devices

1. The qualified electronic signature or seal devices by corresponding technical and procedural means shall ensure the following:

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

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

the reliable level of impossibility of calculation of the value of the personal key based on the public information, and reliable protection of the qualified electronic signature or seal from being forged with the existing technologies;

the possibility of reliable protection of the personal key from third-party use by the signatory or creator (authorised representative of the creator) of the electronic seal.

2. The qualified electronic signature or seal devices shall not modify the data in electronic form to which that qualified electronic signature or seal is linked or deny access to them by the signatory or the creator (authorised representative of the creator) of the electronic seal before the qualified electronic signature or seal is applied to them.

3. The key pair may only be generated and/or managed on behalf of the signatory or creator of the electronic seal by the qualified provider of electronic trust services.

4. The qualified provider of electronic trust services that manages the key pair on behalf of the signatory or creator of the electronic seal may back up the personal key of the signatory or creator of the electronic seal for storage thereof, provided that the requirement of the fifth indent of paragraph 1 of Article 19 of this Law as well as the following requirements are met:

the security level of the backup copy of the personal key has to conform to the security level of the original personal key;

the quantity of backup copies shall not exceed the minimum value necessary to ensure continuity of the service.

5. Conformity of the qualified electronic signature or seal devices to the requirements laid down in paragraphs 1 to 4 of this Article shall be confirmed with the conformity documents issued following the certification of such devices in accordance with the Law of Ukraine ‘On technical regulations and conformity assessment’.

The presumption of conformity to the requirements laid down in paragraphs 1 to 4 of this Article shall be implementation of the standards, including the compatibility ones, adopted by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

6. The conformity assessment authorities accredited to certify the qualified electronic signature or seal devices shall form, update and publish on their official websites the lists of their certified qualified electronic signature or seal devices, and shall also furnish the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services with the lists of their certified qualified electronic signature or seal devices.

The central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services shall form, update and publish on its official website the list of all the certified qualified electronic signature or seal devices certified by the conformity assessment authorities accredited to certify the qualified electronic signature or seal devices.

The requirements for the lists of the certified qualified electronic signature or seal devices shall be established by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

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

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

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

creating the qualified certificates for an electronic signature or seal in accordance with the requirements of this Law, and issuing them to the user of the electronic trust service;

cancelling, blocking and renewing the qualified certificates for an electronic signature or seal in the cases prescribed by this Law;

verifying and validating 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. Creation and issuance of the qualified certificates for an electronic signature or seal failing to meet the requirements of this Law shall be prohibited.

Creation and issuance of the qualified certificates for a public key for any use other than website authentication, creation of an electronic signature and electronic seal shall be carried out in accordance with the requirements of this Law with account of the special aspects laid down by the Cabinet of Ministers of Ukraine.

3. The requirements for providing the qualified electronic trust service of 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.

4. The special aspects of providing the qualified electronic trust service of creation, verification and validation of the qualified encryption certificate shall be established by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

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

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

creating the qualified certificate for website authentication in accordance with the requirements of this Law, and transferring it to the user of the electronic trust service;

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

cancelling, blocking and renewing the qualified certificate for website authentication in the cases prescribed by this Law;

verifying and validating the qualified certificate for website authentication by way of providing the information to third persons 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 requirements for providing the qualified electronic trust service of 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 creation and issuance of the qualified certificate for a public key

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

The person identification shall be carried out by the qualified provider of electronic trust services (its separate point of registration) by verifying and confirming the pertinence of the person identification data received by the qualified provider of electronic trust services (its separate point of registration) to the natural or legal person that has requested the service of creation of the qualified certificate for a public key.

2. The identification of the person that has requested the service of creation of a qualified certificate for a public key shall be carried out in one of the following methods:

1) in personal presence of the natural person, individual entrepreneur or authorised representative of the legal person — based on the verification of the personal data received as prescribed by the legislation from the Unified State Demographic Registry, based on the passport of a citizen of Ukraine or based on other documents issued 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;

2) remotely (without personal presence) with the concurrent use of the electronic identification means with the high or medium assurance level that has already been issued to the natural person, individual entrepreneur or authorised representative of the legal person during a personal visit, and multi-factor authentication;

3) based on the person identification data contained in the qualified certificate for an electronic signature or seal that has already been created and issued in accordance with point 1 or 2 of this paragraph, provided that the certificate is valid;

4) by using any other identification means prescribed by the law, the reliability of which is equivalent to personal presence and is confirmed by the conformity assessment authority.

{Article 22(2) as amended by Law No. 2801-IX of 01.12.2022}

{Article 22(3) is deleted in accordance with the Law No. 2801-IX of 01.12.2022}

4. If foreigners and stateless persons have no documents issued 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, their identification in the manner prescribed by point 1 of paragraph 2 of this Article shall be carried out based on the duly legalised passport document of the foreigner or the identification document of the stateless person.

{Article 22(4) as amended by Law No. 2801-IX of 01.12.2022}

5. During the verification of civil and legal capacity of the legal person (in order to create the qualified certificate for an electronic seal or website authentication) or the individual entrepreneur (in order to create the qualified certificate for an electronic seal), the qualified provider of electronic trust services shall use the information on the legal person or individual entrepreneur indicated in the Unified State Registry of Legal Persons, Individual Entrepreneurs and Civic Associations or the trade, bank or court registry kept by the country of residence of the foreign legal person, and shall also make sure that the scope of the civil and legal capacity of the individual entrepreneur is sufficient for creation and issuance of the qualified certificate for a public key or website authentication. The verification procedure under this paragraph shall be established by the Cabinet of Ministers of Ukraine.

Verification of civil and legal capacity of the legal person of international organisations data on which are not included into the Unified State Registry of Legal Persons, Individual Entrepreneurs and Civic Associations or the trade, bank or court registry kept by the foreign state at the location of the head office of the international organisation shall be carried out based on the information from the international treaty or another official document based on which the international organisation has been incorporated and/or operates.

{Article 22(5) as amended by Law No. 2801-IX of 01.12.2022}

6. The authorised representative of the legal person or individual entrepreneur shall sign the documents necessary to create and issue the qualified certificate for a public key to the employee of the legal person or individual entrepreneur. While creating and issuing the qualified certificate for a public key to the employee of the legal person or individual

entrepreneur, the qualified provider of electronic trust services shall establish the identity of the employee as well as the authorised representative of the legal person or individual entrepreneur in accordance with the requirements of this Article and shall verify the scope of his/her authority based on the document establishing the authority of the authorised representative of the legal person or individual entrepreneur, by means of the information indicated in the Unified State Registry of Legal Persons, Individual Entrepreneurs and Civic Associations or the trade, bank or court registry kept by the country of residence of the foreign legal person.

{The first indent of Article 22(6) as amended by Law No. 2801-IX of 01.12.2022}

If the legal person is represented by the collegial body, the qualified provider of electronic trust services shall be furnished with the document on the authority of the respective body and allocation of duties between 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 (hereinafter the 'qualified certificates for public keys') shall be used.

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

1) an indication (in a form suitable for automated processing) 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 that issued the qualified certificate for a public key (hereinafter the 'entity 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;

as applicable to an individual entrepreneur — the last name, 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 series (if any) and number of the passports of a citizen of Ukraine (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 tax authority to that effect and have the respective mark in the passport of a citizen of Ukraine indicating the right to make payments based on the passport series and number);

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

the last name, first name, patronymic (if any) or the pseudonym (with the indication that the pseudonym is used by the person) 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 series (if any) and number of the passports of a citizen of Ukraine (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 tax authority to that effect and have the respective mark in the passport of a citizen of Ukraine indicating the right to make payments based on the passport series and number), or the number of the passport document of the foreigner or stateless person;

the name or the last name, first 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 (code/number from the trade, bank or court registry kept by the country of residence of the foreign legal person, code/number from the registration certificate of incorporation of the legal person issued by the local authority of the foreign state), except for the international organisations data on which are not included into the Unified State Registry of Legal Persons, Individual Entrepreneurs and Civic Associations or the trade, bank or court registry kept by the foreign state at the location of the head office of the international organisation, 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 series (if any) and number of the passports of a citizen of Ukraine (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 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);

the last name, first name, patronymic (if any) or the pseudonym (with the indication that the pseudonym is used by the person) of the natural person or the name of the legal person to which the qualified certificate for website authentication has been issued, 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 series (if any) and number of the passports of a citizen of Ukraine (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 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 number of the passport document of the foreign or stateless person and the name of the competent authority of the foreign state or UN charter organisation that has issued such passport document, or the code under the Unified State Registry of Enterprises and Organisations of Ukraine (code/number from the trade, bank or court registry kept by the country of residence of the foreign legal person; code/number from the registration certificate of incorporation of the legal person issued by the local authority of the foreign state), except for the international organisations data on which are not included into the Unified State Registry of Legal Persons, Individual Entrepreneurs and Civic Associations or the trade, bank or court registry kept by the foreign state at the location of the head office of the international organisation;

5) the state and the settlement information on which is contained in the data on the place of residence (stay) of the natural person who has been issued the qualified certificate for website authentication, or in the data on the location of the legal person to which the qualified certificate for website authentication has been issued;

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

7) the information on 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) data on free access to the qualified certificate for an electronic signature or electronic seal by means of which the advanced electronic signature or seal specified in point 9 of this paragraph is verified;

11) data on the place where the service of verifying the status of the respective qualified certificate for a public key is provided;

12) the information that the personal key linked to the public key is stored in the qualified electronic signature or seal device (in a form suitable for automated processing);

13) the name(s) of the domain belonging to the natural or legal person to which the certificate for website authentication has been issued.

3. The list of the mandatory requirements applicable to the qualified certificates for public keys under paragraph 2 of this Article shall be exhaustive.

4. The qualified certificates for an electronic signature or seal may contain data on restrictions in the use of the qualified electronic signature or seal.

5. The qualified certificates for public keys may contain other 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 or seals.

6. The procedure of verifying compliance with the mandatory requirements for the qualified certificates for public keys shall be established by the Cabinet of Ministers of Ukraine.

7. A deed completed in electronic form may be held by court invalid if, during its completion, a qualified electronic signature or seal was used, but its qualified certificate failed to contain the information prescribed by paragraph 2 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 provided that, as of validity verification:

the period of validity 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 attributes, 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 shall not issue qualified certificates for public keys with the period of validity exceeding the period of validity 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 communication system, on a round-the-clock basis.

{Article 24(3) as amended by Law No. 1089-IX of 16.12.2020}

4. The access to the qualified certificates for public keys shall be granted by the entity that issued the certificate in accordance with the requirements of the Law of Ukraine 'On 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 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 certificate for the public key issued to it, which is submitted in any way that ensures the identification of the user;

submission of the application requesting to cancel the qualified certificate for the public key of the employee of the legal person or individual entrepreneur, signed by the authorised representative of the corresponding legal person or individual entrepreneur;

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

death of the natural person who is a signatory or has been issued the qualified certificate for website authentication, or of the individual entrepreneur who has created the electronic seal;

state registration of winding-up of the legal person or termination of commercial activities of the individual entrepreneur that has created the electronic seal;

change of the identification data of the user of electronic trust services contained in the qualified certificate for a public key;

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;

compromise of the personal key of the user of electronic trust services detected independently by the user or by the supervisory authority during the state control over compliance with the requirements of the legislation in the field of electronic trust services;

entry into force of the court judgement cancelling the certificate for a public key, declaring the natural person who is a signatory or who has been issued the qualified certificate for website authentication or the individual entrepreneur who has created the electronic seal deceased, missing, legally incapable, limiting his/her civil capacity, or declaring the provider of electronic identification services bankrupt.

2. The central validation authority or the validation centre shall, within 24 hours, inform the qualified providers of electronic trust services of the personal key of the central validation authority or validation centre being compromised in case of the following:

confirmation of the compromise of the personal key of the central validation authority or validation centre detected independently or by the supervisory authority during the state control over compliance with the requirements of the legislation in the field of electronic trust services;

entry into force of the court judgement on compromise of the self-signed certificate of the electronic seal of the central validation authority or validation centre.

The central validation authority shall set the status ‘cancelled’ in the Trusted List for:

the qualified electronic trust service that has been provided by means of the compromised personal key of the central validation authority or the validation centre;

all the qualified electronic trust services of the qualified providers of electronic trust services whose certificates have been created by means of the compromised personal key of the central validation authority or the validation centre.

3. In case the qualified provider of electronic trust services takes a 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 provider in accordance with this Law.

4. The qualified certificate for a public key shall cease to have effect from the moment the entity that issued the certificate changes the status of the qualified certificate for a public key for being cancelled.

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

6. The qualified certificate for a public key shall, 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 certificate for the public key issued to it, which is submitted in any way that ensures the identification of the user;

submission of the application requesting to block the qualified certificate for the public key of the employee of the legal person or individual entrepreneur, signed by the authorised representative of the corresponding legal person or individual entrepreneur;

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

entry into force of the court decision on blocking the qualified certificate for a public key;

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

7. The qualified certificate for a public key of the qualified provider of electronic trust services shall also be blocked by the entity that issued the certificate in the event the supervisory authority adopts the decision on blocking the corresponding qualified certificate for a public key based on the results of the state control in accordance with the requirements of the legislation in the field of electronic trust services pursuant to this Law.

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

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

10. The blocked certificate for a public key shall, within two hours, be renewed 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 renew its blocked qualified certificate for the public key, which is submitted in any way that ensures the identification of the user (if the blocking has been based on the application requesting to block the qualified certificate for a public key);

submission of the application requesting to renew the qualified certificate for the public key of the employee of the legal person or individual entrepreneur, signed by the authorised representative of the corresponding legal person or individual entrepreneur;

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;

receipt by the entity that issued the certificate of the notification that the court judgement has been granted on the renewal of the qualified certificate for a public key and has entered into 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;

entry into force of the court decision in favour of the provider of electronic trust services.

12. The qualified certificate for a public key that has been blocked shall regain 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 changes the status of the qualified certificate for a public key for being renewed.

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

The procedure for cancelling, blocking and renewing cancelled qualified certificates for public keys shall be established by the operating regulation of the entity that issued the corresponding certificate.

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

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

creation of the qualified electronic time stamp;

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 meet the following requirements:

connect the date and time with the data in electronic form in such a way that reasonably rules out unnoticed modification of the data in electronic form;

be based on the source of the accurate time synchronised to within one second of Coordinated Universal Time (UTC);

the qualified electronic time stamp shall be accompanied by the designated advanced electronic signature or advanced electronic seal of the qualified provider of electronic trust services, or another method equivalent to adding the advanced electronic signature or advanced electronic seal to the qualified electronic time stamp may be used, provided that it ensures the same level of security of the qualified electronic time stamp and meets the requirements of this Law.

3. (Deleted)

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

5. The requirements for providing the electronic trust service of creation, verification and validation of 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. Qualified electronic trust service of the registered electronic delivery

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

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

identification of the sender shall be ensured;

identification of the recipient shall be ensured before data in electronic form are delivered;

the data in electronic form being sent and received shall be accompanied by the designated advanced electronic signature or advanced electronic seal or the qualified electronic signature or qualified electronic seal of the qualified provider of electronic trust services in such a way that rules out unnoticed modification of the data in electronic form;

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 for the qualified 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 court proceedings solely based on the fact that they are in electronic form, provided that such data meet 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 receipt

by the identified recipient, as well as the accuracy of the date and time of sending and receiving the data in electronic form, which are indicated during the provision of this service.

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

1. The qualified electronic trust service of storage of the qualified electronic signatures, seals and 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 qualified electronic trust service of storage of the qualified electronic signatures, seals and certificates connected with such services shall only be provided by the qualified providers of electronic trust services that use the procedures and technologies capable of ensuring long-term reliability of the qualified electronic signatures or seals.

3. The requirements for providing the qualified electronic trust service of storage of the qualified electronic signatures, seals, electronic time stamps and 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 aspects of provision of qualified electronic trust services by the central validation authority

1. The central validation authority shall provide the qualified electronic trust service of 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 an electronic seal of the central validation authority based on the agreement concluded by the administrator of the information and communication system of the central validation authority and the corresponding provider for free, with account of paragraph 2 of Article 7^1 of this Law.

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

the procedure for providing services in accordance with the requirements of this Law and the legislative and regulatory acts adopted in pursuance hereof, and the rules of procedure of the central validation authority;

its period of validity;

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

The ground for terminating the agreement on the provision by the central validation authority of the qualified electronic trust service of creation, verification and validation of the qualified certificate for an electronic signature or seal shall be cancellation of the status of the qualified provider of electronic trust services.

3. While providing the qualified electronic trust service of creation, verification and validation of the qualified certificate for an electronic signature or seal of the provider of electronic trust services, the central validation authority shall carry out identification of legal and natural persons and shall verify their civil and legal 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 provider of the electronic trust services.

4. While providing the qualified electronic trust services, the central validation authority shall meet the requirements established for the qualified providers of electronic trust services.

5. The software and hardware system of the central validation authority used by it to provide the qualified electronic trust serviced shall meet the requirements established for the software and hardware system of the qualified providers of electronic trust services.

6.6. The organisational and methodological, technical and technological conditions of the activities of the central validation authority in provision of the qualified electronic trust services, the procedure of interaction of the providers and users of electronic trust services with the central validation authority in provision of the qualified electronic trust services shall be established by the rules of procedure of the central validation authority.

The rules of procedure of the central validation authority shall be approved by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

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 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 case electronic trust services are provided by banks, other entities operating on the financial services markets subject to state regulation and supervision by the National Bank of Ukraine, payment system operators and/or payment system participants, technical payment service providers).

In order to obtain the administrative services of entry of information on the legal persons and individual entrepreneurs that intend to provide the qualified electronic trust services into the Trusted List, the applicant shall submit documents in hard or soft copy to the central validation authority or the validation centre. The procedure for submitting the documents to the validation centre shall be established by the National Bank of Ukraine.

2. The legal persons, individual entrepreneurs that intend to provide the qualified electronic trust services shall submit to the central validation authority or the validation centre the following for the data thereon to be included into the Trusted List:

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

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

3) the original document on conformity to the requirements for the qualified providers of electronic trust services and their services issued following the conformity assessment procedure in the field of electronic trust services, or a copy thereof duly certified under the procedure established by the legislation;

4) documents on conformity of the qualified electronic signature or seal devices that will be used to provide the qualified electronic trust services to the requirements established by this Law, issued following the certification of such devices;

5) 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 to be used for the placing of components of the software and hardware system that will ensure the provision of qualified electronic trust services;

6) the list and the positions 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 to be used to provide the qualified electronic trust services;

8) the original agreement on insurance of civil liability or a copy thereof duly certified under the procedure established by the legislation, 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, or the account with the National Bank of Ukraine — for the banks being qualified providers of electronic trust services, the qualified provider of electronic trust services established by the National Bank of Ukraine) 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) the original rules of procedure of the qualified provider of electronic trust services, as approved by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services, or by 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 meets the requirements for the rules of procedure of the qualified provider of electronic trust services, or copies thereof duly certified under the procedure established by the legislation;

10) the original plan for terminating the activities of providing the qualified electronic trust services or a copies thereof duly certified under the procedure established by the legislation, in the format established by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

In case the legal persons and individual entrepreneurs that intend to provide the qualified electronic trust services submit documents for data thereon to be entered into the Trusted List in hard copy, they shall also submit copies of the documents specified in this paragraph in soft copy.

The entities specified in the first indent of paragraph 1 of Article 9 hereof shall submit the documents for data thereon to be entered into the Trusted List to the validation centre.

3. In the event a legal person, an individual entrepreneur intends to provide the qualified electronic trust services via separate points of registration, the data 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 paragraph 2 of this Article.

4. The central validation authority or the validation centre shall, following consideration of the submitted documents, within fifteen 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 to the Trusted List, or send a substantiated refusal to the applicant.

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 data thereon to the Trusted List, submit to the central validation authority or the validation centre the documents to create the qualified certificates for public keys of the qualified provider of electronic trust services (separately for each qualified electronic trust service) 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 refusing to add the data to the Trusted List in the event of the following: submission of the incomplete package of the documents specified in paragraph 2 of this Article; violation of the requirements for the documents submitted; detection of unreliable information, defects that hinder unambiguous interpretation of the content, corrections or additions in the application requesting to be added to the Trusted List and the documents attached thereto.

7. Where there are any changes in the data in the Trusted List, the qualified provider of electronic trust services shall, within five business days following the day when such changes occurred, submit to the authority that has taken the decision to enter the data thereto into the Trusted List an application requesting to make amendments to the Trusted List, together with the documents confirming the corresponding changes.

In case the deadline for submission of the documents being a basis for amendments to the Trusted List is missed, the qualified provider of electronic trust services may not provide the qualified electronic trust services until the respective amendments to the Trusted List are made.

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 to the applicant.

The central validation authority or the validation centre shall provide a substantiated refusal to make 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, or violation of the requirements established for the documents submitted;

detection of unreliable information, defects that hinder unambiguous interpretation of the content, corrections or additions in the application requesting to make amendments to the Trusted List and the documents attached thereto.

8. The validation centre shall, within three business 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 within five business days 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 five business 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 to cancel the status of the qualified provider of electronic trust services by changing the status of the qualified electronic trust service provided by the qualified provider of electronic trust services for the status of being cancelled in case the following is received:

a statement of the qualified provider of electronic trust services of its decision to terminate provision of all the qualified electronic trust services specified in the Trusted List;

an application from the validation centre requesting to cancel the status of the qualified provider of electronic trust services;

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

information on termination of the activities of the qualified provider of electronic trust services (state registration of termination of commercial activities of the individual entrepreneur or winding-up of the legal person);

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

information on the entry into force of the court judgement on cancelling the status of the qualified provider of electronic trust services and declaring the qualified provider of electronic trust services deceased, declaring him or her missing, legally incapable, limiting his or her civil capacity, declaring the qualified provider of electronic trust services bankrupt.

In case the status of the qualified provider of electronic trust services is cancelled, the information on such provider and the qualified electronic trust services it has provided shall be kept in the Trusted List in order to verify the qualified certificates for public keys of the provider and its users.

10. In order to ensure continuous provision of the qualified electronic trust services to their users, the central validation authority may decide to make amendments to the Trusted List as regards replacement of the qualified provider of electronic trust services by replacing the data on the qualified provider of electronic trust services with the data on another qualified provider of electronic trust services if the respective rights and obligations are transferred upon mutual consent of such providers, on a contractual basis or on other legal succession grounds prescribed by the legislation.

The procedure for making amendments to the Trusted List as regards replacement of the qualified provider of electronic trust services as well as special aspects of obtaining and cancelling the status of the qualified provider of electronic trust services in case of replacement of the qualified provider of electronic trust services shall be established by the Procedure for Keeping the Trusted List approved by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

Article 31. Termination of the activities of 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:

decision of the central validation authority to cancel the status of the qualified provider of electronic trust services;

its decision to terminate provision of the qualified electronic trust services specified in the Trusted List;

termination of the activities of the qualified provider of electronic trust services (state registration of termination of commercial activities of the individual entrepreneur or winding-up of the legal person), except for the cases of legal succession laid down in paragraph 10 of Article 30 of this Law;

entry into force of the court judgement on cancelling the status of the qualified provider of electronic trust services, declaring him or her deceased, 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 its decision on terminating the provision of qualified electronic trust services within five business days from the day of such decision.

3. The central validation authority and/or the validation centre shall make publicly available the information on the decision of the central validation authority or the validation centre accordingly on the termination of provision of qualified electronic trust services by the qualified provider of electronic trust services, including in connection with cancellation of the status of the qualified provider of electronic trust services, at latest on the next business day after the day of such decision, by:

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 thereof.

4. The central validation authority and/or the validation centre shall 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 at latest on the next business day following the day of receiving the notification of the grounds specified in the third to fifth indents of paragraph 1 of this Article.

The notification of the central validation authority or the validation centre on the termination of provision of 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 in three months from the day of publication of the notification on the termination of provision of qualified electronic trust services by the qualified provider of electronic trust services on the official website of the central validation authority or the validation centre.

6. From the day of publication of the notification on the termination of provision of qualified electronic trust services by the qualified provider of electronic trust services on the official website of the central validation authority or the validation centre 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.

The qualified provider of electronic trust services that terminates provision of qualified shall transfer the servicing of users of qualified with which it has made agreements on the provision of the electronic trust services to another qualified provider of electronic trust services in accordance with the procedure established by the Cabinet of Ministers of Ukraine.

7. In case a user of electronic trust services refuses to keep being serviced under the agreement on the provision of the electronic trust services made with the qualified provider of electronic trust services that is terminating provision of qualified provider of electronic trust services, by another qualified provider of electronic trust services until expiration of the corresponding agreement, the qualified provider of electronic trust services that is terminating

provision of electronic trust services shall refund the user for the services that cannot be provided in the future if the user has paid for them in advance.

In case a user of electronic trust services agrees to keep being serviced under the agreement on the provision of the electronic trust services made with the qualified provider of electronic trust services that is terminating provision of qualified provider of electronic trust services, by another qualified provider of electronic trust services until expiration of the corresponding agreement, the qualified provider of electronic trust services that is terminating provision of electronic trust services shall pay for further provision of qualified electronic trust services to such user at the rates established by the corresponding qualified provider of electronic trust services.

8. The central validation authority shall, on the day determined in accordance with paragraph 5 of this Article as the date of terminating provision of qualified electronic trust services, make the relevant amendments to the Trusted List.

9. The qualified provider of electronic trust services that is terminating provision of qualified electronic trust services shall transfer the documented information of the users of the electronic trust services of electronic trust services specified in paragraph 1 of Article 9 of this Law to another qualified provider of electronic trust services that intends to keep servicing the users of the electronic trust services until expiration of the corresponding agreements on the provision of the qualified electronic trust services, or to the central validation authority or the validation centre.

10. The procedure of storing the documented information and transferring it 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.

11. The procedure for transferring the documented information to the validation centre in the event of termination of the activities of the qualified provider of electronic trust services data on which has been added to the Trusted List by the decision of the validation centre shall be established by the National Bank of Ukraine.

Title V

SUPERVISION AND CONTROL IN THE FIELDS OF ELECTRONIC IDENTIFICATION AND ELECTRONIC TRUST SERVICES

Article 32. Conformity assessment in the fields of electronic identification and 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 shall, at their own expense, undergo the conformity assessment procedure in the field of electronic trust services.

2. The providers of electronic identification services shall, at their own expense, undergo the conformity assessment procedure in the context of electronic identification schemes to establish the low, medium or high assurance level.

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

4. The central validation authority shall create, update and publish on its official website the list of the conformity assessment authorities, with the hyperlink to the register of the accredited conformity assessment authorities published on the official website of the national accreditation authority of Ukraine as well as foreign conformity assessment authorities duly accredited by the foreign accreditation authorities that are signatories to the International Accreditation Forum Multilateral Recognition Arrangement and/or the European Accreditation (EA MLA).

5. Assessment of conformity to the requirements applicable to the qualified providers of electronic trust services and to the services they provide shall be carried out with account of the legislative requirements concerning the procedure for provision and use of the qualified electronic trust services as well as the requirements in the field information protection.

In case electronic trust services are provided in the banking system of Ukraine and on the markets of non-bank financial services subject to state regulation and supervision by the National Bank of Ukraine, and payment services are provided, assessment of conformity to the requirements applicable to the qualified providers of electronic trust services and to the services they provide shall be carried out with account of the requirements established by the National Bank of Ukraine.

6. The qualified providers of electronic trust services that 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, shall, 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 in the field of electronic trust services.

7. After they undergo the procedure for assessing conformity of electronic identification means in the context of electronic identification schemes, the providers of electronic identification services shall submit an auditor’s opinion to the central validation authority for the decision on approval of such schemes to be adopted.

8. As prescribed by the law, the supervisory authority may submit a request to the conformity assessment authority for the auditor’s opinion on the conformity assessment procedure of the provider of electronic trust services at the expense of the latter in order to confirm that the provider and electronic trust services it provides meet the requirements in the field of electronic trust services.

9. The qualified providers of electronic trust services shall inform the supervisory authority of the results of conformity assessment in the field of electronic trust services by submitting a copy of the document on conformity to the requirements applicable to the

qualified providers of electronic trust services and to the services they provide, within three business days from the day of receipt thereof.

10. The conformity assessment procedure in the fields of electronic identification and electronic trust services shall take place under the procedure approved by the Cabinet of Ministers of Ukraine.

The conformity assessment procedure in the banking system of Ukraine and on the markets of non-bank financial services subject to state regulation and supervision by the National Bank of Ukraine as well as during provision payment services shall be carried out with account of the requirements established by the National Bank of Ukraine.

Article 33. State supervision (control) over compliance with the requirements of the legislation in the fields of electronic identification and electronic trust services

1. The state supervision (control) over compliance with the requirements of the legislation in the fields of electronic identification and 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 fields of electronic identification and electronic trust services shall be carried out in accordance with this Law.

3. The functions of the supervisory authority shall be performed by the State Service of Special Communication and Information Protection of Ukraine.

Article 33[1]. Measures of the state supervision (control) over the compliance with the requirements of the legislation in the fields of electronic identification and electronic trust services

1. The results of conformity assessment in the fields of electronic identification and electronic trust services shall be analysed by the supervisory authority. In case the results of conformity assessment or recommendations given by the conformity assessment authority are negative, the supervisory authority may decide to designate the additional conformity assessment after all the defects specified in the auditor’s opinion are eliminated.

2. Scheduled measures of control are not taken by the supervisory authority.

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

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

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

3) inspection of the providers of electronic identification services and providers of electronic trust services upon receipt of the information or notice of violation of the requirements of the legislation in the fields of electronic identification and electronic trust services from the validation centre, the central validation authority, the court, users of the electronic trust services or third parties;

4) inspection of the providers of electronic identification services and providers of electronic trust services based on the justified decision of the supervisory authority.

Article 33[2]. Response to violation of the legislation in the fields of electronic identification and electronic trust services

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

1) demand that the qualified providers of electronic trust services, the validation centre, the central validation authority eliminate 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 blocking the qualified certificate for the public key of the qualified provider of electronic trust services if the personal key was suspected to have been compromised during the inspection;

3) adopt a decision on cancelling the qualified certificate for the public key of the qualified provider of electronic trust services if the personal key was established to have been compromised during the inspection.

The decision on blocking or cancelling the qualified certificate for the public key of the qualified provider of electronic trust services shall be sent by the supervisory authority to the central validation authority on the day of its adoption.

4) send to the central validation authority an application requesting to revoke the status of the qualified provider of electronic trust services or the service provided by the qualified provider of electronic trust services, the validation centre, the central validation authority in the Trusted List in the event of the following:

the provision of qualified electronic trust services by the qualified provider of electronic services with no valid documents as prescribed by the legislation, confirming the conformity of the integrated information protection system of the information and communication system of the qualified provider of electronic services and the information protection means within that system to the requirements of the legislative and regulatory acts in the field of technical and cryptographic protection of information, or with 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 communication system of the qualified provider of electronic trust services in the event of

modernisation of the hardware, hardware and software or software within the software and hardware system, which is not provided for by the design or maintenance documentation to the integrated information protection system of the information and communication 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 paragraph 5 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 provider of the electronic trust services of its obligations;

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

provision of the qualified electronic trust services by the qualified provider of electronic trust services without valid documents as prescribed by the legislation, confirming the title to and/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 in the documents submitted by the qualified provider of electronic trust services for the information thereon to be added to the Trusted List;

the failure to eliminate the violations detected during the inspection within the time period established by the instruction;

blocking or cancellation of the qualified certificate for a public key of the qualified provider of electronic trust services.

2. Within a month from the day of generation of the key pairs by the central validation authority and creation of the relevant self-signed certificates for electronic seals of the central validation authority, the supervisory 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 case violations of the requirements established by the legislation for the central validation authority are detected, the supervisory authority shall notify the Cabinet of Ministers of Ukraine of the detected violations and shall propose to the central validation authority solutions thereto.

3. Based on the results of inspections of the providers of electronic identification services, the supervisory authority shall apply the following response measures:

1) demand that the providers of electronic identification services eliminate the violations of the legislative requirements in the field of electronic identification and electronic trust services, within the time period established by the instruction;

2) adopt the decision to suspend provision of electronic identification services by the provider of electronic identification services if the violation affecting security of such services is detected during the inspection, until the violations are fully eliminated.

4. 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 identification and electronic trust services in terms of compliance with the legislative requirements.

Article 34. Powers of the officials of the supervisory authority during the state supervision (control) over the compliance with the requirements of the legislation in the fields of electronic identification and electronic trust services

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

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

2) in case violations of the requirements of the legislation in the fields of electronic identification and electronic trust services are detected, to issue binding instructions and to set the time frames for elimination of such violations;

3) to impose administrative sanctions upon guilty persons for violation of the requirements of this Law and other legislative and regulatory acts adopted in pursuance hereof;

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

5) to exercise other powers as prescribed by law.

Article 34[1]. On-site measures of the state supervision (control) over the compliance with the requirements of the legislation in the fields of electronic identification and electronic trust services

1. The supervisory authority shall take on-site measures of the state supervision (control) over compliance with the requirements of the legislation in the field of electronic trust services by analysing:

1) operation of the website of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre;

2) content of the website of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre,

due notification of users of electronic identification services or electronic trust services of provision of the services;

3) list, procedure for provision and content of the services, electronic trust services via the website of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre;

4) notices of the provider of electronic identification services, the qualified provider of electronic trust services, the central validation authority, or the validation centre;

5) documents on conformity following the procedures for assessing conformity of the provider of electronic identification services, the qualified provider of electronic trust services, the central validation authority or the validation centre, and the services they provide;

6) other information on operation, organisation and provision of electronic identification services, electronic trust services by the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre;

Article 34[2]. Decision on the unscheduled inspection

1. The supervisory authority adopts a decision on the inspection in order to conduct an unscheduled inspection. The decision on the inspection shall be signed by the head of the supervisory authority or his/her deputy in accordance with allocation of functional duties.

2. The decision on the inspection shall contain:

1) name of the supervisory authority;

2) name (last name, first name, patronymic (if any)) of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre;

3) location or place of residence of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre;

4) ground for the inspection;

5) scope of the inspection;

6) dates of commencement and end of the inspection;

7) names and positions of the inspection committee members.

3. A notice of the decision on the unscheduled inspection shall be sent (delivered) to the provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre at least ten business days before the start of the inspection, by registered mail and/or communication means (including via the electronic account or another information system used by the supervisory authority and the entity being inspected), or delivered in person against signature to the head of authorised representative of the entity being inspected.

4. The duration of the unscheduled inspection shall not exceed ten business days.

5. The unscheduled inspection shall be conducted during the working hours of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre in accordance with its internal work regulations.

6. The provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre shall have the right not to admit the officials of the supervisory authority to the unscheduled inspection in case a notice of the decision on the inspection is not received within the timeframes set by paragraph 3 of this Article.

Article 34[3]. Inspection committee

1. The inspection committee shall comprise the head and the members of the committee.

The inspection committee may involve representatives of the central validation authority (upon their consent).

2. Based on the inspection decision, an inspection mandate shall be issued to be signed by the head or deputy head of the supervisory authority in accordance with allocation of functional duties and sealed.

The format of the inspection mandate shall be approved by the regulatory authority.

3. The inspection mandate shall specify:

1) name of the supervisory authority;

2) name (last name, first name, patronymic (if any)) of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre;

3) location or place of residence of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre;

4) details of the decision on the inspection;

5) names and positions of the inspection committee members;

6) dates of commencement and end of the inspection;

7) ground for the inspection;

8) inspection checklist.

The inspection mandate shall be valid only during the inspection period indicated therein.

4. The inspection committee members shall:

1) conduct the inspection in an objective and unprejudiced manner;

2) comply with the requirements of the legislation in the fields of electronic identification, electronic trust services, information protection and personal data protection;

3) perform their official duties and assignments of the head of the inspection committee in a diligent, timely and quality manner;

4) comply with business ethics in relations with the senior executive and staff of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre;

5) bring the findings of the inspection to the notice of the senior executive of the provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre or his/her authorised representative;

6) render advisory assistance in connection with the inspection to the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre;

7) avoid disclosing sensitive that came to their knowledge in connection with performance of their official duties.

5. When performing their duties in the course of the inspection, the inspection committee members shall have the right to:

1) have access to the special premises, all the documents and information of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre, in connection with provision of electronic identification services or qualified electronic trust services;

2) study the operation of the information and communication system as well as other technical facilities, electronic identification means, qualified electronic signature or seal devices used by the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre in order to provide the electronic identification services and/or qualified electronic trust services;

3) obtain from the employees of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre, information and explanations, including written ones, on their activities in connection with provision of electronic identification services and/or electronic trust services that are necessary for the inspection;

4) obtain from the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre and attach to the inspection files the records which may be evidence of breach of the legislation in the fields of electronic identification services and/or electronic trust services in hard or soft copy.

Article 34[4]. Obligations of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre during the inspection

1. The senior executive of the provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre shall create the conditions necessary for the inspection, namely:

1) grant the head and members of the inspection committee access to the premises associated with provision of the services for the period of the inspection of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre, and exit from such premises;

2) provide the head and members of the inspection committee with an office facility (individual workstation) equipped with necessary furniture, computer and document storage facility on the day of the start of the on-site inspection;

3) organise the meeting between the head and members of the inspection committee with the employees of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre whose duties are directly associated with provision of electronic identification services and/or electronic trust services;

4) ensure access of the head and members of the inspection committee to all the records and information on the activity of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre as provided for by the legislation in the fields of electronic identification and/or electronic trust services;

5) ensure that the documents on the activity of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre (oral and written explanations by the head and the employees) are furnished in hard or soft copy within the time frames necessary to fulfil the assignment, which do not exceed the period designated for the state supervision (control);

6) ensure adequate conduct of employees of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre during the inspection.

Article 34[5]. Rights of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre during the inspection

1. The senior executive of the provider of electronic trust services, the central certification authority or the validation centre, or its authorised representative shall have the right to the following during the inspection:

1) require that the head and members of the inspection committee comply with the law;

2) check the availability of official IDs of the head and members of the inspection committee and obtain a copy of the inspection mandate;

3) not admit the head and members of the inspection committee to the inspection in case the head and members of the inspection committee have not presented their official ID and the inspection mandate executed in accordance with the law;

4) be present during the inspection;

5) require that the head and members of the inspection committee meet the requirements for non-disclosure of the restricted information obtained by them during the inspection;

6) obtain and review the inspection report;

7) provide written explanations, comments and objections to the inspection report;

8) obtain explanations on the committee's actions related to the inspection from the head of the inspection committee;

9) in case of objection to the actions of the head and/or members of the inspection committee, submit written complaints to the supervisory authority or challenge the inspection committee's actions in court;

10) obtain consultations from the head and members of the inspection committee to prevent violations in the course of the inspection.

Article 34[6]. On-site inspection process

1. Before the start of the inspection, the head of the inspection committee shall make an entry in the relevant log of the provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre (if any).

2. The inspection shall be conducted in the presence of the senior executive of the provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre or his/her authorised representative.

3. The inspection shall be conducted through review of documents, information contained in the databases, interviews with the employees of the provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre, analysis of the state of compliance with the legislation in the fields of electronic identification and/or electronic trust services and with the guidelines related to provision of electronic identification services and/or electronic trust services.

4. The inspection is conducted in two stages:

1) the inspection process;

2) presentation of inspection results.

5. Preparation for the inspection shall be made through:

1) processing of the material of the previous inspection for follow-up control over the areas of activity where breaches were identified earlier;

2) analysis of the information designated for the remote state supervision (control) under Article 34[1] of this Law;

3) examination of the rules of procedure of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre.

6. During the inspection, the head and members of the inspection committee shall have the right to request the materials and information necessary for the inspection in writing from the provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre.

7. The provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre shall provide the supervisory authority with all requested information within fifteen business days following the date of registration of the relevant request.

8. On the first day of the inspection, the head and members of the inspection committee shall present to the senior executive of the provider of electronic identification services, the provider of electronic trust services, the central certification authority or the validation centre or his/her authorised representative the inspection mandate and their official IDs that identify the head and members of the inspection committee as officials of the supervisory authority, and provide a copy of the inspection mandate.

9. The head and members of the inspection committee shall have no right to conduct the inspection without presenting their official IDs and the inspection mandate.

Article 34[7]. Presentation of inspection results

1. The results of the inspection of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre shall be presented by the inspection committee as the inspection report in the format approved by the supervisory authority.

2. The inspection report shall contain the following data:

1) name of the supervisory authority;

2) names and positions of the inspection committee members;

3) initials and last name of senior executive of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre;

4) details of the inspection mandate;

5) dates of commencement and end of the inspection;

6) address of the premises of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre where the inspection was conducted;

7) results of the previous inspection;

8) information on the results of the last conformity assessment in the fields of electronic identification and electronic trust services before the inspection;

9) name and summary of the documents provided during the inspection;

10) qualitative and quantitative indicators established during the inspection that characterise the activity of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre in connection with provision of electronic identification services and/or electronic trust services;

11) breaches and deficiencies (if any) identified in the course of the inspection, and explanations of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre on the reasons for failure to meet the legislative requirements (if any);

12) inspection conclusions;

13) instances of hampering the inspection (if any);

14) recommendations on remedy of identified breaches (if any);

15) date of the report;

16) signatures of the head and members of the inspection committee;

17) signature of the senior executive of the provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre or his/her authorised representative, which confirms that he/she has read the inspection report.

3. As for the breaches specified in the inspection report, references to the specific clauses of this Law, other legislative acts in the field of cybersecurity, information protection, personal data protection, electronic identification and/or electronic trust services.

Arbitrary interpretation of legislative and regulatory acts shall be prohibited.

Reference information or information on breaches and deficiencies that can be grouped by subject matter may be presented in annexes to the inspection report.

If documents or copies thereof are attached to the inspection report, their titles and details shall be specified.

4. The inspection report shall be made in two copies and signed at latest the last day of the inspection, by the head and all members of the inspection committee and by the senior executive of the provider of electronic identification services, the provider of electronic trust

services, the central validation authority or the validation centre, or his/her authorised representative.

5. The inspection committee member who dissents from the inspection committee's conclusions indicated in the inspection report shall sign it and provide a written dissent to be attached to the inspection report. In this case, the entry 'With dissent attached' shall be made above the signature block in the inspection report.

6. In case the senior executive of the provider of electronic identification services, the provider of electronic trust services, the central certification authority or the validation centre, or his/her authorised representative has any comments to the facts and conclusions contained in the inspection report, the entry 'With comments attached' shall be made above the signature block.

7. Comments to the inspection report shall be executed as a separate document and signed by the senior executive of the provider of electronic identification services, the provider of electronic trust services, the central certification authority or the validation centre, or his/her authorised representative.

8. Comments on the inspection report as well as a dissent of the inspection committee member shall constitute an integral part of the inspection report.

9. If the senior executive of the provider of electronic identification services, the provider of electronic trust services, the central certification authority or the validation centre, or his/her authorised representative refused to review the inspection report or sign it after its review, the head of the inspection committee shall make relevant mark to be signed by the head and a member of the inspection committee, preceding the signature of the senior executive of the provider of electronic identification services, the provider of electronic trust services, the central certification authority or the validation centre, or his/her authorised representative.

10. One copy of the inspection report shall be provided to the senior executive or authorised person of the provider of electronic identification services, the provider of electronic trust services, the central validation authority, or the validation centre on the last day of the inspection whereas the second one shall be kept at the supervisory authority.

11. In case the inspection of the provider of electronic identification services, the provider of electronic trust services is conducted, a copy of the inspection report shall be sent to the central validation authority or the validation centre within five days after completion thereof.

Article 34[8]. Notice of remedial action in the fields of electronic identification and/or electronic trust services

1. A notice of remedial action shall be made by the inspection committee in duplicate within five business days following the completion of the inspection. A copy of the notice shall be sent to the provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre within five business

days following the date of the inspection report whereas the second copy signed by the senior executive of the provider of electronic identification services, the qualified provider of electronic trust services, the central certification authority or the validation centre, or his/her authorised representative, which refers to the agreed time limits for remedy of breaches of the legislation in the field of electronic trust services, shall remain with the supervisory authority.

2. The template of the notice of remedial action shall be approved by the supervisory authority.

3. The notice of remedial action shall be signed by the head and members of the inspection committee, who conducted the inspection.

4. In case the senior executive of the provider of electronic identification services, the provider of electronic trust services, the central validation authority or the validation centre or his/her authorised representative refused to receive the notice of remedial action, it shall be sent by registered mail, with the corresponding reference number and date of dispatched stamped in a copy of the notice kept by the supervisory authority.

5. The senior executive of the provider of electronic identification services, the provider of electronic trust services, the central certification authority or the validation centre shall take measures to remedy deficiencies and breaches specified in the notice of remedial action within the period indicated therein.

6. The provider of electronic identification services, the provider of electronic trust services, the central certification authority or the validation centre shall provide furnish the supervisory authority with written information on remedy of the breaches accompanied by supporting documents, within the period indicated in the notice of remedial action.

Article 34[9]. Decision on blocking or cancelling the qualified certificate for the public key of the qualified provider of electronic trust services, changing the status of the service of the qualified provider of electronic trust services, the central validation authority or validation centre

1. The decision on blocking or cancelling the qualified certificate for the public key of the qualified provider of electronic trust services shall be adopted by the supervisory authority and shall contain:

1) name of the supervisory authority;

2) date of adoption and sequence number;

3) names and positions of the inspection committee members;

4) name (last name, first name, patronymic (if any)) of the qualified provider of electronic trust services;

5) location of the qualified provider of electronic trust services;

6) name (last name, first name, patronymic (if any)) of the senior executive of the qualified provider of electronic trust services;

7) circumstances under which breaches were identified (type, inspection period, date and number of the inspection report or reference to other data source);

8) justified grounds for the decision on blocking the qualified certificate for the public key of the provider of electronic trust services;

9) request to block the qualified certificate for the public key of the qualified provider of electronic trust services;

10) signature of the head or deputy head of the supervisory authority in accordance with allocation of functional responsibilities.

2. The decision on changing the status of the service of the qualified provider of electronic trust services, the central validation authority or validation centre shall be adopted by the supervisory authority and shall contain:

1) name of the supervisory authority;

2) date of adoption and sequence number;

3) names and positions of the inspection committee members;

4) name (last name, first name, patronymic (if any)) of the qualified provider of electronic trust services, the central validation authority or the validation centre;

5) address of the qualified provider of electronic trust services, the central certification authority or the validation centre;

6) last name, first name, patronymic (if any) of the senior executive of the qualified provider of electronic trust services, the central validation authority or the validation centre;

7) circumstances under which breaches were identified (type, inspection period, date and number of the inspection report or reference to other data source);

8) justified grounds for adopting the decision on changing the status of the service of the qualified provider of electronic trust services, the central validation authority or validation centre;

9) signature of the head or deputy head of the supervisory authority in accordance with allocation of functional responsibilities.

3. Based on the decision of the supervisory authority on blocking or cancelling, the central certification authority or the validation centre shall change the status of the qualified certificate for the public key of the qualified provider of electronic trust services for the blocked or cancelled one accordingly.

4. The application for changing the status of the service of the qualified provider of electronic trust services, the central validation authority or validation centre in the Trusted List shall be prepared by the supervisory authority and sent to the central validation authority on the day of being signed by the head or deputy head of the supervisory authority in accordance with allocation of functional responsibilities.

5. The application for changing the status of the service of the qualified provider of electronic trust services, the central validation authority or validation centre in the Trusted List shall contain:

1) name of the supervisory authority;

2) name (last name, first name, patronymic (if any)) of the qualified provider of electronic trust services, the central validation authority or the validation centre;

3) location or place of residence of the (place of registration) of the qualified provider of electronic trust services, the central validation authority or the validation centre;

4) last name, first name, patronymic (if any) of the senior executive of the qualified provider of electronic trust services, the central validation authority or the validation centre;

5) circumstances under which breaches were identified (type, inspection period, date and number of the inspection report or reference to other data source);

6) justified grounds for adopting the decision on changing the status of the service of the qualified provider of electronic trust services, the central validation authority or validation centre in the Trusted List;

7) name of the service and the request to change the status of the service of the qualified provider of electronic trust services, the central validation authority or validation centre in the Trusted List;

8) date of signing;

9) signature of the head or deputy head of the supervisory authority in accordance with allocation of functional responsibilities.

Article 34[10]. Termination and cancellation of use of the electronic identification scheme

1. In case the electronic identification scheme, its components have been compromised, and/or the procedures determined within the electronic identification scheme are breached, which affects reliability of authentication or poses a threat for integrity of user identification data, the supervisory authority shall adopt a decision and submit an application for termination of use of such electronic identification scheme to the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

The decision on termination of use of the electronic identification scheme is adopted by the supervisory authority and shall contain:

1) name of the supervisory authority;

2) date of adoption and sequence number;

3) names and positions of the inspection committee members;

4) name (last name, first name, patronymic (if any)) of the provider of electronic identification services;

5) address of the provider of electronic identification services;

6) last name, first name, patronymic (if any) of the senior executive of the provider of electronic identification services;

7) circumstances under which breaches were identified (type, inspection period, date and number of the inspection report or reference to other data source);

8) justified grounds for the decision on termination of use of the electronic identification scheme;

9) request to terminate use of the electronic identification scheme;

10) signature of the head or deputy head of the supervisory authority in accordance with allocation of functional responsibilities.

2. The central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services shall terminate use of the electronic identification scheme based on the decision of the supervisory authority on termination of use of the electronic identification scheme.

3. The application for termination of use of the electronic identification scheme shall be prepared by the supervisory authority and sent to the central validation authority on the day of being signed by the head or deputy head of the supervisory authority in accordance with allocation of functional responsibilities.

4. The application for termination of use of the electronic identification scheme shall contain:

1) name of the supervisory authority;

2) name (last name, first name, patronymic (if any)) of the provider of electronic identification services;

3) location or place of residence of the (place of registration) of the provider of electronic identification services;

4) last name, first name, patronymic (if any) of the senior executive of the provider of electronic identification services;

5) circumstances under which breaches were identified (type, inspection period, date and number of the inspection report or reference to other data source);

6) justified grounds for the decision on termination of use of the electronic identification scheme;

7) name of the electronic identification scheme;

8) date of signing;

9) signature of the head or deputy head of the supervisory authority in accordance with allocation of functional responsibilities.

5. If the breach or compromise specified in paragraph 1 of this Article has been remedied, the supervisory authority shall submit an application for resumption of use of the corresponding electronic identification scheme to the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

6. If the supervisory authority has not submitted an application for resumption of use for three months after the application for termination of the electronic identification scheme, the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services shall cancel use of the electronic identification scheme based.

Article 35. 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 automated processing.

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

2. The requirements applicable to the Trusted List shall be established by the Cabinet of Ministers of Ukraine.

3. The procedure for maintaining the Trusted List shall be adopted by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services.

Article 36. Liability for violation of the legislation in the fields of electronic identification and electronic trust services

1. The persons guilty of the violation of the requirements of the legislation in the fields of electronic identification and electronic trust services, shall bear liability in accordance with the law.

2. The damage caused to the user of electronic identification services by the provider of electronic identification services that implements the electronic identification scheme(s), by the central executive authority ensuring the formation of and implementing the public policy in the fields of electronic identification and electronic trust services, or the supervisory authority shall be compensated in full under the procedure established by the law.

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 the law.

3. The provider of electronic trust services, the validation centre or the central validation authority shall be liable for the damages inflicted through its fault (either intentionally or through negligence) upon a natural or legal person as a result of non-performance or improper performance of its duties under this Law.

The burden of proof of the guilt (intention or negligence) of the non-qualified provider of electronic trust services in inflicting damages as a result of non-performance of improper performance of its duties under this Law shall be borne by the natural or legal person that claims compensation for the damages.

The qualified provider of electronic trust services, the validation centre or the central validation authority shall be deemed guilty of the damages inflicted upon the natural or legal person as a result of non-performance or improper performance of its duties under this Law unless it proves that damages have not been inflicted through its fault (either intentionally or through negligence).

If the provider of electronic trust services, the validation centre or the central validation authority duly informs users of the electronic trust services in advance of restrictions in use of the electronic trust services it provides, provided that such restrictions are understandable by users, it shall not be liable for the damages as a result of use of the electronic trust services in breach of such restrictions.

4. The persons guilty of information confidentiality and/or integrity breaches that affect provision of electronic trust services or electronic identification services or are associated with personal data of the users of the electronic trust services or electronic identification services shall be held liable in accordance with the Law of Ukraine ‘On personal data protection’.

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

Title VI

INTERNATIONAL COOPERATION

Article 37. Participation in the international cooperation in the fields of electronic identification and electronic trust services

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

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

3. The supervisory authority shall, on the grounds and in accordance with the procedure prescribed by the laws and international treaties of Ukraine and within its competence, cooperate with the foreign competent authorities, render assistance to them and request their

assistance in the matters of supervision and control over compliance with the requirements of the legislation in the field of electronic trust services.

4. Where an international treaty of Ukraine ratified by the Verkhovna Rada of Ukraine provides for the rules other than those provided for in this Law, the rules of the international treaty of Ukraine shall prevail.

Article 37[1]. Recognition of foreign electronic identification schemes and means

1. The electronic identification schemes used in other states and/or electronic identification means issued within the framework of such electronic identification schemes shall be recognised in Ukraine in accordance with the international treaties of Ukraine on mutual recognition of the electronic identification schemes and/or means ratified by the Verkhovna Rada of Ukraine.

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 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 on the markets of non-bank financial services subject to state regulation and supervision by the National Bank of Ukraine as well as when providing payment services).

{Article 38(1) as amended by Law No. 1591-IX of 30.06.2021 — in force from 01.08.2022}

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 for recognition of the foreign certificates for public keys, electronic signatures, as well as use of the information and telecommunication system of the central validation authority in order to ensure recognition in Ukraine of electronic trust services, foreign certificates for public keys used to provide legally valid electronic services in the process of interaction between entities of different states shall be established by the Cabinet of Ministers of Ukraine.

{Article 38(3) as amended by Law No. 1089-IX of 16.12.2020}

Title VII

FINAL AND TRANSITIONAL PROVISIONS

1. This Law shall enter into force in a year from the date of its official publication, save for Article 10, which shall enter into force on the day of the publication of this Law.

2. The Law of Ukraine ‘On electronic digital signature’ shall cease to have effect (Bulletin of the Verkhovna Rada of Ukraine, 2003, No. 36, Article 276; 2009, No. 24, Article 296; 2013, No. 37, Article 488; 2015, No. 23, Article 158; 2016, No. 47, Article 800).

3. The following Laws of Ukraine shall be amended:

1) in Article 7 of the Law of Ukraine ‘On the National Bank of Ukraine’ (Bulletin of the Verkhovna Rada of Ukraine, 1999, No. 29, Article 238 as amended):

point 26 shall be replaced by the following:

“26) create the validation centre in order to ensure the adding of the information on legal persons, individual entrepreneurs that intend to provide electronic trust services within the banking system of Ukraine and when making transfer of funds, to the Trusted List in accordance with the Law of Ukraine ‘On electronic trust services’;”

point 26^{-1} shall be added as follows:

“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’ (Bulletin of the Verkhovna Rada of Ukraine, 2003, No. 36, Article 275; 2014, No. 24, Article 885; 2015, No. 45, Article 410):

a) paragraph 3 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’;”

b) paragraph 1 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 details, 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’;”

c) 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’ (Bulletin of the Verkhovna Rada of Ukraine, 2014, No. 25, Article 890, No. 29, Article 946):

a) the third indent 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);”

b) in paragraph 1 of Article 14:

point 2 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 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 and 43 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 communication systems, special connection systems, electronic document exchange systems (in the context of information protection), within which the state information resources and the information to be protected as prescribed by the law will be processed, 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), organising the expert assessment thereof;”

c) in paragraph 1 of Article 15:

the fourth indent 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 shall be replaced by the following:

"19) apply to court where disputes arise on the matters of organising special communication and information protection, cryptographic and technical protection of the state information resources and the information to be protected as prescribed by the law, disputes in the field of electronic trust services, as well as where other disputes arise, under the procedure established by the law."

{Point 3 of the Title 'Final and Transitional Provisions' as amended in accordance with Law No. 1089-IX of 16.12.2020}

4. The accredited centres for keys certification established under the Law of Ukraine '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 'On electronic digital signature' prior to the effective date of this Law, shall be used by the users of electronic trust services, the qualified providers of electronic trust services continuing to provide services to them, as 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 in any case 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 with the advanced certificate for a public key, shall be considered, after the Law of Ukraine 'On electronic trust services' enters into force, but in any case within two years from the date this Law enters into force, to be the data in electronic form with the created qualified electronic signature.

6^{-1}. On a temporary basis, until Ukraine and the European Union mutually recognised the electronic trust services, as an exception to the clauses of paragraph 1 of Article 38 of this Law, to recognise the following in Ukraine:

1) deliverables of the qualified electronic trust services provided by the qualified provider of electronic trust services, data on which and on their qualified electronic trust services are added to the Trusted List of the Member State of the European Union or the Member State of the European Free Trade Association (hereinafter the 'European qualified providers');

2) the status of the European qualified providers, which is equal to the status of the qualified providers of electronic trust services in accordance with this Law;

3) the status of the qualified electronic signature or seal devices used by the European qualified providers to provide their electronic trust services and added to the list of certified qualified electronic signature creation devices kept by the European Commission in accordance with Article 31 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, which is equivalent to the status of the qualified electronic signature or seal means in accordance with this Law;

4) the list if the trusted lists of the Member States of the European Union information on which is published by the European Commission in accordance with paragraph 4 of Article 22 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

{Title VII 'Final and Transitional Provisions' is supplemented with point 6[-1] in accordance with Law No. 2801-IX of 01.12.2022}

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 consistent with 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 will be brought into compliance with this Law.

President of Ukraine **P. POROSHENKO**

Kyiv

5 October 2017

No. 2155-VIII