APPROVED
Order No. 4/1-OCH dated June 05, 2026
Director of the
Ukrainian Clearing House
Limited Liability Company

_____ Olena Velyka

PROCEDURE
for the use of electronic signature and electronic seal in UKRAINIAN CLEARING HOUSE Limited Liability Company

Kyiv – 2026

CONTENT

1. GENERAL PROVISIONS...…….....…….....3
2. DEFINITION OF TERMS... …….4
3. GENERAL PRINCIPLES OF THE USE OF ELECTRONIC SIGNATURES AND ELECTRONIC SEALS……. 6
4. TYPES OF ELECTRONIC SIGNATURES AND ELECTRONIC SEALS……8
5. CREATION, SENDING, RECEIVING AND STORAGE OF ELECTRONIC DOCUMENTS..……..…. 12
6. CREATION AND CERTIFICATE OF COPIES OF DOCUMENTS……...……..…….14
7. DETECTION OF ANY CHANGES IN AN ELECTRONIC DOCUMENT …….....15
8. FINAL PROVISIONS ……...……..….....15

1. GENERAL PROVISIONS

1.1. The procedure for using an electronic signature and electronic seal in the UKRAINIAN CLEARING HOUSE Limited Liability Company (hereinafter referred to as the Procedure) has been developed in accordance with the Civil Code of Ukraine, the Laws of Ukraine "On State Regulation of Capital Markets and Organized Commodity Markets", "On Capital Markets and Organized Commodity Markets", "On Electronic Documents and Electronic Document Management", "On Electronic Identification and Electronic Trust Services", the Procedure for the Use of Electronic Signature by Capital Market Participants and Professional Participants of Organized Commodity Markets, approved by the Decision of the National Securities and Stock Market Commission dated May 20, 2025 No. 17/21/2298/K03 (hereinafter referred to as the NSSMC Procedure).

1.2. This Procedure defines the legal, organizational and technical conditions for the use of an electronic signature (hereinafter referred to as the "ES") and an electronic seal during the creation, processing and storage of electronic documents by the UKRAINIAN CLEARING HOUSE Limited Liability Company (hereinafter referred to as the UCH) during electronic interaction with clients/counterparties, commodity exchanges (with which a clearing agreement has been concluded) and other persons who are subjects of electronic interaction.

1.3. The requirements of the NSSMC Procedure for information systems apply to the relevant components/modules of the clearing accounting system and other UCH systems used to receive, register, process, store, send electronic documents and ensure electronic interaction.

1.4. This Procedure applies to electronic interaction carried out through:

- official email of the UCH;
- UCH information and information-communication systems (including the clearing accounting system);
- information and information-communication systems of commodity exchanges with which UCH has entered into clearing agreements;
- external electronic document management services, in particular "Vchasno", "M.E.Doc" or other similar services used by the UCH;
- other channels of electronic interaction defined by the UCH or agreed upon between the parties to electronic interaction.

1.5. The procedure does not apply to documents that require notarization, as well as documents that, in accordance with the legislation of Ukraine, cannot be created in electronic form.

1.6. The requirements of this Procedure regarding the use of electronic means cannot be interpreted by subjects of electronic interaction as limiting the rights of subjects of electronic interaction to conclude transactions in the form of paper documents (to change, supplement or terminate the validity of electronic documents with paper documents or in another form not prohibited by the legislation of Ukraine and vice versa) or orally, unless the law establishes an obligation to conclude a transaction in writing.

1.7. In the event that the Procedure or its individual clauses contradict the requirements of the legislation of Ukraine, the legislation of Ukraine shall be applied with priority, and the Procedure shall be brought into line with the requirements of the legislation as soon as possible.

1.8. This procedure is mandatory for employees and authorized representatives of the UCH.
1.9. Clearing participants, counterparties and other persons who engage in electronic interaction with the UCH are obliged, when interacting with the UCH, to comply with the requirements of this Procedure in the part that regulates the procedure for creating, submitting, signing, processing and using electronic documents, as well as the use of electronic signatures and electronic seals. The application of the requirements of this Procedure in relations with such persons may be additionally determined by relevant agreements.

2. DEFINITION OF TERMS

2.1. In this Procedure, the terms are used in the meanings:

1) **Analogue of handwritten signature (AHS) –** a type of simple electronic signature within the meaning of internal documents of the Clearing House, which is defined by the Clearing House as an electronic analogue of the handwritten signature of a clearing participant, a person who has been granted access to the clearing accounting system and allows identification of such participant (such person), and also to establish the absence of distortion of information in the documents of such a participant (such a person) in the clearing accounting system, which are considered to be signed by such a clearing participant (such a person) with an electronic signature within the meaning of the Law of Ukraine "On Electronic Documents and Electronic Document Management";

2) **Electronic document –** a document in which information is recorded in the form of electronic data, including mandatory document details;

3) **Electronic copy of a paper document –** a visual representation of a paper document in electronic form, obtained by scanning the original paper document, the correspondence of which to the original is certified by the electronic signature of the subject of electronic interaction;

4) **Qualified electronic trust service provider (QETSP) –** a legal entity, regardless of its organizational and legal form and form of ownership, an individual entrepreneur who provides one or more qualified electronic trust services, and whose information is included in the list of qualified electronic trust service providers with information about them and the qualified electronic trust services they provide;

5) **Qualified electronic signature (QES) –** an advanced electronic signature created using a qualified electronic signature tool and based on a qualified electronic signature certificate;

6) **Qualified electronic seal –** an advanced electronic seal created using a qualified electronic seal tool and based on a qualified electronic seal certificate;

7) **Client –** a client of UCH, a user of services provided by UCH on capital markets, including a clearing participant;

8) **Counterparty –** any legal entity or individual that has relations with the UCH related to capital markets activities;

9) **Non-resident –** a foreign legal entity, foreign organization, foreign individual, stateless person or other person who, in accordance with the legislation of Ukraine, has the status of a non-resident and enters or intends to enter into legal relations with the UCH;

10) **Verification of the integrity of an electronic document –** a procedure carried out by confirming an advanced or qualified electronic signature or seal in accordance with the legislation, and in the case of imposing an electronic signature or seal of another type on an electronic document, using other means and methods of information protection, in compliance with the requirements of legislation in the field of information protection, which make it possible to detect any changes in the electronic document after its signing;

11) **Signer –** a person who applies the ES to an electronic document;

12) **Simple electronic signature (simple ES) –** any type of electronic signature, except for a qualified electronic signature, a digital handwritten signature, an advanced electronic signature based on a qualified certificate;

13) **Subject of electronic interaction –** UCH, client, counterparty, authorized person of the client/counterparty (clearing account manager) or other person who creates, signs, sends, receives, processes, verifies, stores or uses electronic documents in interaction with UCH;

14) **Advanced electronic signature based on a qualified electronic signature certificate (AES with a qualified certificate)** – advanced electronic signature created using a qualified electronic signature certificate that does not contain information that the private key is stored in the qualified electronic signature device or seal;

15) **Advanced electronic seal based on a qualified electronic seal certificate (hereinafter referred to as an electronic seal with a qualified certificate)** – an advanced electronic seal created using a qualified electronic seal certificate, which contains a mark that this certificate was created as qualified for the use of an electronic seal, and there is no information that the private key is stored in the qualified electronic signature or seal device.

2.2. Other terms used in this Procedure are used in the meanings given in the Law of Ukraine "On Electronic Identification and Electronic Trust Services", the Law of Ukraine "On State Regulation of Capital Markets and Organized Commodity Markets", the Law of Ukraine "On Capital Markets and Organized Commodity Markets", the Law of Ukraine "On Electronic Documents and Electronic Document Flow" and regulatory legal acts of the NSSMC.

3. GENERAL PRINCIPLES OF THE USE OF ELECTRONIC SIGNATURES AND ELECTRONIC SEALS

3.1. UCH organizes the use of electronic signatures and electronic seals in the processes of creating, signing, certifying, accepting, registering, processing, sending, storing and verifying electronic documents in accordance with the legislation of Ukraine, this Procedure, other internal documents of UCH and agreements concluded by UCH.
3.2. The use of electronic signatures and electronic seals in the activities of the UCH is carried out for the purpose of:

- creation, signing, approval, certification, submission, acceptance, processing, registration, storage and verification of electronic documents;
- confirmation of legally significant actions performed electronically within the framework of UCH processes;
- confirmation of the origin of electronic data;
- ensuring the integrity of electronic documents and electronic data;
- confirmation of the powers of the signatory or representative of a legal entity in cases provided for by the legislation of Ukraine, agreements or this Procedure;
- certification of electronic copies of paper documents;
- ensuring the provability of electronic interaction between the UCH, clients, counterparties and other persons.

3.3. The UCH independently determines the permissible types of electronic signatures and electronic seals for individual types of electronic documents, electronic actions, information systems, areas of activity and channels of electronic interaction, taking into account the requirements of the legislation of Ukraine, this Procedure, other internal documents of the UCH and relevant agreements.

3.4. The use of a separate type of electronic signature or electronic seal is not allowed if the legislation of Ukraine, a contract or internal documents of the UCH establish the mandatory use of another type of electronic signature or electronic seal for the relevant document, transaction, electronic action or method of electronic interaction.

3.5. The procedure for creating an electronic document is established taking into account the requirements of the legislation of Ukraine, this Procedure, other internal documents of the UCH and/or relevant agreements. The creation of an electronic document is considered complete from the moment the last electronic signature is applied.

3.6. An electronic signature is a mandatory requirement of an electronic document.

3.7. A person who has signed an electronic document with an electronic signature hereby certifies that he/she has read the entire text of the document, fully understood its content, has no objections to the text of the document (or his/her objections are entered as a separate requisite of the document) and has knowingly used his/her electronic signature in the context provided for by the document (signed, approved, agreed, endorsed, certified, familiarized himself/herself with).

3.8. Verification of the integrity, authenticity of origin and belonging of electronic documents bearing an electronic signature and/or electronic seal is carried out by the UCH using qualified electronic trust services, software and hardware, and information and communication systems that meet the requirements of the legislation of Ukraine in the field of electronic identification and electronic trust services. Verification of an electronic signature and/or electronic seal may be carried out, in particular, using the services of qualified electronic trust service providers, the official website of the Central Certification Authority of Ukraine or other technical means that provide the possibility of such verification in accordance with the requirements of the legislation of Ukraine. Based on the results of the verification, a protocol or other electronic document may be generated confirming the results of the verification of the electronic signature and/or electronic seal.

3.9. UCH ensures the recording of legally significant electronic actions, actions of users of information and information and communication systems of UCH, as well as actions related to the provision, review, change, cancellation and control of access rights to such systems in cases and

to the extent determined by this Procedure, other internal documents of UCH and relevant agreements.

3.10. The specified actions are recorded using event logs, technical logs, registers, electronic messages, information system records or other electronic evidence that allows establishing the fact, date, time, subject, content and/or result of the relevant electronic action.

3.11. The volume of information to be recorded in the information and information and communication systems of the UCH is determined taking into account the technical capabilities of such systems, as well as the requirements of the legislation of Ukraine and internal documents of the UCH.

3.12. The procedure for granting, changing, revising, revoking and controlling access to information and information and communication systems of the UCH, as well as other systems used for receiving, registering, processing, storing and transmitting electronic documents, including issues of identification, authentication, authorization, managing access rights, determining user functionality, controlling granted access rights and recording actions during access management, is determined by internal UCH documents.

3.13. The UCH receives, processes, stores, and sends electronic documents and information necessary for creating electronic documents, in compliance with the requirements of the legislation of Ukraine regarding the protection of restricted information, including: personal data, professional secrets, and commercial secrets.

3.14. UCH has the right to use open network services to receive/provide/send information that may be classified as restricted information (including: personal data, professional secrets and commercial secrets), provided that the following conditions are met:

1) electronic interaction is carried out exclusively between the UCH and the client/counterparty;

2) The UCH has previously received written permission from the client/counterparty to carry out such actions or the contract with the client/counterparty contains such permission from the client/counterparty;

3) The UCH ensures compliance with the requirements of Ukrainian legislation in the field of information protection, information security and cyber defense.

3.15. The UCH may determine in internal documents the technology of using open network services to obtain/provide information with limited access (including: personal data, professional secrets and commercial secrets).

3.16. UCH is liable for damage caused to the client / counterparty during the use of the open network service technology implemented by UCH. In the event that the client/counterparty denies the fact of voluntary transfer of information through an open network service, UCH ensures proof of such voluntary transfer using a contract, statement, electronic message, technical logs, event logs, confirmations from the relevant information system or other appropriate evidence.

3.17. Responsibility for organizing the use of electronic signatures and electronic seals in the activities of the UCH lies with the Director of the UCH in accordance with the requirements of the legislation of Ukraine.

3.18. The Director of the UCH ensures the organization of the use of electronic signatures and electronic seals of the UCH by employees of the UCH, authorized representatives of the UCH and authorized persons acting on behalf of the UCH.

4. TYPES OF ELECTRONIC SIGNATURES AND ELECTRONIC SEALS

4.1. When interacting with the UCH, clients/counterparties may use a qualified electronic signature (hereinafter referred to as a QES), an advanced electronic signature (hereinafter referred to as an AES with a qualified certificate), a simple electronic signature, a qualified electronic seal, an advanced electronic seal with a qualified certificate.

4.2. In the activities of the UCH and in interaction with the UCH, a digital handwritten signature, as well as an advanced electronic signature not based on a qualified electronic signature certificate, an advanced electronic seal, are not used, unless otherwise provided for by the legislation of Ukraine, regulatory legal acts of the NSSMC or a separate internal document of the UCH.

4.3. When interacting electronically with a client/counterparty, the UCH uses a QES or AES with a qualified certificate and a qualified electronic seal or an advanced electronic seal with a qualified certificate.

4.4. The conclusion of a separate agreement regarding the use by the client/counterparty of a QES, an AES with a qualified certificate, a qualified electronic seal, an electronic seal with a qualified certificate is not required, provided that the requirements of the legislation of Ukraine and this Procedure are met.

4.5. The use of a simple electronic signature is carried out on the basis of an agreement between the UCH and the client, counterparty. The contract is concluded in writing after identification and verification of the person (in accordance with the requirements of the legislation of Ukraine) with whom such a contract is concluded:

1) in the form of a paper document with handwritten signatures of the parties, or
2) as an electronic document with the parties' QES, or
3) as an electronic document with a AES with a qualified certificate of the client/counterparty and the QES of the authorized representative of the UCH, or
4) as an electronic document using any types of electronic means for which an agreement has already been concluded between the UCH and the client/counterparty in accordance with the requirements of one of subparagraphs 1 - 3 of this paragraph of the Procedure.

4.6. Documents for which the legislation of Ukraine or the regulatory legal acts of the NSSMC stipulate the mandatory use of a qualified electronic signature or another specified type of electronic signature cannot be signed with another type of electronic signature.

4.7. UCH has the right to demand re-signing of an electronic document with an appropriate type of electronic signature if the document was signed in violation of the requirements of the legislation of Ukraine, this Procedure, the contract or other internal documents of UCH.

4.8. **Using the QES:**

4.8.1. The QES is created using a qualified electronic signature tool and is based on a qualified electronic signature certificate.

4.8.2. Verification and confirmation of the QES is carried out in accordance with the requirements of the Law of Ukraine "On Electronic Identification and Electronic Trust Services".

4.8.3. A qualified public key certificate must comply with the requirements of the Law of Ukraine "On Electronic Identification and Electronic Trust Services".

4.8.4. The signer is prohibited from signing an electronic document if the signer's qualified public key certificate is invalid or it is impossible to obtain information about its status.

4.8.5. The signatory is obliged to use a qualified electronic time stamp when signing an electronic document of the QES, and the relevant electronic interaction system must ensure verification of the presence of a qualified electronic time stamp.

4.9. **Using AES with a qualified certificate:**

4.9.1. An AES with a qualified certificate is created using a qualified electronic signature certificate issued by a qualified electronic trust service provider and does not contain information that the private key is stored in the qualified electronic signature device.

4.9.2. Verification and confirmation of an advanced electronic signature with a qualified certificate are carried out using qualified electronic trust services in accordance with the requirements of the legislation of Ukraine. The validity of such a signature is confirmed by the results of its verification in accordance with the legislation of Ukraine in the field of electronic trust services.

4.9.3. When applying the AES with a qualified certificate, the signatory is obliged to check the validity of his qualified public key certificate in accordance with the requirements of the Law of Ukraine "On Electronic Identification and Electronic Trust Services".

4.9.4. The signer is prohibited from imposing an AES with a qualified certificate if the signer's qualified public key certificate is invalid or it is impossible to obtain information about its status.

4.9.5. In the process of confirming an AES with a qualified certificate, the validity of such a signature is confirmed if all of the following conditions are met:

1) use to create an AES with a qualified certificate of a qualified public key certificate of the signatory, which meets the requirements established by the Law of Ukraine "On Electronic Identification and Electronic Trust Services";

2) issuance of a qualified public key certificate of the signer by a qualified electronic trust service provider and its validity at the time of creation of the AES with a qualified certificate;

3) the correspondence of the public key value to its value contained in the signer's qualified public key certificate;

4) correct inclusion of a unique set of data that identifies the signer in the signer's qualified public key certificate;

5) indication in the qualified certificate of the signer's public key about the use of a pseudonym in it (if it was used by a person at the time of creation of the AES with a qualified certificate);

6) the integrity of the electronic data to which this AES with a qualified certificate is linked has not been compromised;

7) compliance with the requirements established by the Law of Ukraine "On Electronic Identification and Electronic Trust Services".

4.9.6. The signatory is obliged to use a qualified electronic time stamp when signing an electronic document of the AES with a qualified certificate, and the relevant electronic interaction system must ensure verification of the presence of a qualified electronic time stamp.

4.10. **Using a simple ES:**

4.10.1. Clients/counterparties who are non-residents of Ukraine have the right to use a simple electronic signature in interaction with UCH in cases provided for by this Procedure, other internal documents of UCH LLC and subject to concluding an agreement with UCH on the use of a simple electronic signature.

4.10.2. The contract for the use of a simple electronic device must necessarily contain:

- conditions and order/procedure for the recognition by the UCH and the client/counterparty of transactions, electronic documents or legally significant electronic actions using a simple electronic document;
- conditions for the allocation of risks of losses that may be caused to signatories or third parties in the event of the use of a simple electronic signature.

4.10.3. Simple ES is used exclusively in interaction with the UCH and using technology specified or agreed upon by the UCH.

4.10.4. Simple ES must provide unambiguous identification of the signatory in accordance with the legislation of Ukraine, the agreement concluded with the UCH regulating the procedure for electronic interaction, this Procedure and other internal documents of the UCH.

4.10.5. The electronic data used to create a simple ES must be unique, uniquely linked to the signatory and not linked to any other person.

4.10.6. The technology for using simple electronic signatures must provide the signatory, when signing or confirming a legally significant electronic action, with control over the electronic data being signed or confirmed, as well as control over the electronic data used to create the simple electronic signature.

4.10.7. Simple electronic signature is not applicable to documents, transactions or legally significant electronic actions for which the legislation of Ukraine, the contract, the internal documents of the UCH provide for the use of a QES, a AES with a qualified certificate or another specified type of electronic signature.

4.10.8. In its activities, the UCH may ensure the use of various types, forms or technologies of simple electronic information used in the relevant UCH information systems.

4.10.9. Simple electronic signatures include AHSs, which are used to confirm legally significant electronic actions in information and information and communication systems of the UCH.

4.10.10. AHS can be used as a simple electronic signature in the relevant information and information and communication systems of the UCH, in particular to confirm the actions of a clearing participant (clearing account manager) who has been granted access to the relevant information and information and communication system of the UCH, provided that such person consents to the use of an analogue of a handwritten signature and signs an agreement with the UCH on the use of a simple electronic signature.

4.10.11. Proof of the integrity of electronic data and electronic documents on which a simple ES is applied is provided by means of information systems, information and communication systems, software and hardware complexes and other means of electronic interaction of UEEX LLC, in which the creation, processing, transmission and storage of electronic documents are carried out.

4.10.12. To prove the fact of the signer's identification when using a simple ES, the UCH can use a set of data from the relevant information systems of the UCH, including the account, user role, date and time of action, registers, electronic messages, session identifier, IP address (if available), technical log and other data that record the content and result of the electronic action.

4.11. **Use of electronic seals:**

4.11.1. The following types of electronic seals may be used in the activities of the UCH and in interaction with the UCH:

- qualified electronic seal;
- advanced electronic seal with a qualified certificate.

4.11.2. UCH uses a qualified electronic seal in cases specified by the legislation of Ukraine (including regulatory legal acts of the NSSMC), these Procedures, and other internal documents of UCH.
4.11.3. A qualified electronic seal has a presumption of the integrity of electronic data and the authenticity of the origin of the electronic data to which it is linked, and is used in cases in accordance with the legislation of Ukraine, if:

1) it is necessary to ensure the authenticity of the origin of the related electronic data, to certify the validity of the electronic signature on the electronic document;

2) affixing a seal is required to certify that copies of documents correspond to the originals;

3) it is necessary to confirm the authority of the representative of the legal entity to use the EP in the context provided for by the document (signing, approval, consent, endorsement, certification, familiarization).

4.11.4. An advanced electronic seal with a qualified certificate may be used by a UCH in cases where the legislation of Ukraine, the contract, or the internal documents of the UCH do not provide for the mandatory use of exclusively a qualified electronic seal.
4.11.5. A qualified electronic seal certificate must comply with the requirements of the Law of Ukraine "On Electronic Identification and Electronic Trust Services" and contain a mark that such a certificate has been generated as qualified for the use of an electronic seal.
4.11.6. The UCH has the right to use more than one qualified electronic seal and/or more than one advanced electronic seal with a qualified certificate.
4.11.7. When applying a qualified electronic seal or an advanced electronic seal with a qualified certificate, the subject of electronic interaction is obliged to verify the validity of the corresponding qualified electronic seal certificate in accordance with the Law of Ukraine "On Electronic Identification and Electronic Trust Services".
4.11.8. The subject of electronic interaction is prohibited from applying a qualified electronic seal if the qualified electronic seal certificate is invalid, or it is impossible to obtain information about its status.
4.11.9. The subject of electronic interaction is obliged to ensure the use of a qualified electronic time stamp in cases of affixing a qualified electronic seal/electronic seal with a qualified certificate.
4.11.10. Verification and confirmation of a qualified electronic seal are carried out in accordance with the requirements of the Law of Ukraine "On Electronic Identification and Electronic Trust Services".
4.11.11. Verification and confirmation of an advanced electronic seal with a qualified certificate are carried out using qualified electronic trust services for creating, verifying and confirming a qualified electronic signature or seal in accordance with the requirements of the Law of Ukraine "On Electronic Identification and Electronic Trust Services".

5. CREATION, SENDING, RECEIVING AND STORAGE OF ELECTRONIC DOCUMENTS

5.1. Electronic documents in the activities of the UCH are created, signed, sent, received, registered, processed and stored in compliance with the requirements of the legislation of Ukraine, this Procedure, and other internal documents of the UCH.
5.2. The electronic document must contain mandatory details stipulated by the legislation of Ukraine, internal documents of the UCH and the contract.

5.3. An electronic document to be signed is created with an electronic signature of the appropriate type in accordance with the requirements of this Procedure and other internal documents of the UCH.
5.4. If the legislation of Ukraine, internal documents of the UCH provide for the use of a certain type of electronic signature or electronic seal for a relevant electronic document, transaction or electronic action, the use of another type of electronic signature or electronic seal is not allowed.
5.5. A person who affixes an electronic signature to an electronic document must, before affixing such a signature, have the opportunity to familiarize themselves with the content of the electronic document or legally significant electronic action being signed or confirmed.
5.6. A person who puts an electronic signature and/or an electronic seal on an electronic document confirms that he has read the text of the electronic document, understands its content, has no objections to it (or his objections are entered as a separate requisite of the document), and knowingly used the electronic signature and/or electronic seal in the context provided by the document (signed, approved, agreed, endorsed, certified, read).
5.7. A unilateral electronic document certified by an electronic signature is considered created from the moment of its signing, unless the legislation of Ukraine establishes the mandatory use of an electronic seal.
5.8. The moment of applying an electronic signature and/or electronic seal to an electronic document is recorded in the time stamp of the corresponding signature or seal.
5.9. An electronic document that is subject to signing by two or more parties is considered created from the moment of the last electronic signature of the party (its representative) who signs the document last.
5.10. If such an electronic document is signed by the parties at different times, the date and time of its conclusion shall be the date and time of the last electronic signature, determined by the corresponding time stamp.
5.11. Sending and receiving electronic documents in interaction with the UCH is carried out through official or agreed channels of electronic interaction.
5.12. The UCH ensures the acceptance, registration and confirmation of receipt of electronic documents certified by a qualified electronic signature or an advanced electronic signature with a qualified certificate in compliance with the requirements of the legislation of Ukraine in the field of electronic document management.
5.13. An electronic document is considered to have been submitted to the UCH through an appropriate electronic interaction channel if such a channel is defined or agreed upon for the relevant type of document, transaction, electronic action or process.
5.14. Acceptance of an electronic document for execution is carried out after verification of such document, electronic signature, electronic seal, signatory's authority and integrity of the electronic document in the cases and in the manner specified by this Procedure.
5.15. After creating an electronic document, the UCH sends the client/counterparty a copy of such an electronic document with all the necessary details to the email address specified by the client/counterparty, or provides the electronic document in another way agreed with the client/counterparty.
5.16. Electronic documents are stored by the UCH for the periods specified by the legislation of Ukraine, internal documents of the UCH, and the contract.

5.17. Storage of an electronic document must ensure the possibility of its reproduction, verification of integrity, authenticity, electronic signature, electronic seal and other details during the storage period of such a document, unless otherwise provided for by the legislation of Ukraine.
5.18. Storage of electronic documents containing restricted information, personal data, professional or commercial secrets is carried out in compliance with the requirements of the legislation of Ukraine, internal documents of the UCH.
5.19. Storage of electronic documents of permanent and long-term storage (over 10 years) is carried out taking into account the requirements of the legislation of Ukraine regarding the possibility of verifying the relevant electronic signatures and/or electronic seals in the long-term period.
5.20. The procedure for storing, transferring to the archive, backing up, restoring and destroying electronic documents after the expiration of their storage period is determined by the legislation of Ukraine and internal documents of the UCH.

6. CREATION AND CERTIFICATE OF COPIES OF DOCUMENTS

6.1.**Creating and certifying an electronic copy of a paper document**
6.1.1. An electronic copy of a paper document is created exclusively from the original paper document by scanning the paper document or a photo of the paper document into electronic form in compliance with the requirements of the legislation of Ukraine, this Procedure and other internal documents of the UCH.
6.1.2. The UCH accepts electronic copies of paper documents provided that such copies:

- created directly from the original document;
- contain all pages of the document and its integral annexes;
- ensure the possibility of a complete and unambiguous perception of the content of the document;
- allow the identification of the document details, signatures, seals (if any) and other information necessary for its use;
- comply with the requirements of the legislation of Ukraine and this Procedure.

6.1.3. UCH does not accept electronic copies of paper documents for work:

- that are not created from the original or from an improperly certified paper copy of the document (except for cases provided for by the legislation of Ukraine, internal documents of the UCH);
- with obvious signs of mechanical damage or distortion of content (corrections, erasures, filled pages, etc.);
- that do not meet the requirements of this Procedure.

6.1.4. An electronic copy of a paper document is certified by an electronic signature of the subject of electronic interaction that meets the requirements of this Procedure for the relevant type of electronic signature, the use of which is determined by the Code of Conduct or provided for by the legislation of Ukraine.
6.1.5. An electronic copy of a paper document is certified with an electronic seal in cases where such certification is mandatory in accordance with the legislation of Ukraine.
6.1.6. Certification of an electronic copy of a paper document confirms its conformity with the original paper document from which it was created.

6.2. **Creation and certification of a paper copy of an electronic document**

6.2.1. A paper copy of the original electronic document is created by reproducing the electronic document in paper form.

6.2.2. A paper copy of an electronic document must ensure a complete and accurate reproduction of the content of the corresponding electronic document, its details and information necessary for the identification of such a document, as well as allow for the unambiguous identification of the electronic document on the basis of which it was created.

6.2.3. Certification of a paper copy of an electronic document is carried out by an authorized person of the UCH by affixing a mark on the conformity of the copy to the original, which must contain the words "According to the original", the title of the position, surname and initials of such person, his/her handwritten signature and date of certification, as well as, if necessary, an imprint of the UCH seal.

6.2.4. If a paper copy of an electronic document consists of several sheets, such sheets shall be numbered and bound in a manner that ensures the integrity of the document. On the back of the last sheet, a note shall be made about the number of sheets, which shall be certified by the signature of an authorized person and, if necessary, by the seal of the UCH.

6.2.5. Certification of a paper copy of an electronic document confirms the correspondence of such a copy to the electronic document from which it was created.

7. DETECTION OF ANY CHANGES IN AN ELECTRONIC DOCUMENT

7.1. Verification of the integrity, authenticity and authorship of electronic documents is carried out by the UCH using software and hardware tools for verifying electronic signatures and, if necessary, using qualified public key certificates in accordance with the requirements of the legislation of Ukraine in the field of electronic trust services. To verify the integrity of electronic documents certified by a qualified electronic signature, state and other available electronic signature verification resources that ensure the use of cryptographic algorithms and meet the requirements of Ukrainian legislation can be used, in particular.

7.2. If it is established that changes have been made to an electronic document or electronic copy after an electronic signature or electronic seal has been affixed, such a document is considered to have compromised its integrity and is not subject to acceptance or use by the UCH.

7.3. The UCH records the facts of checking electronic documents, as well as cases of detecting violations of their integrity or other inconsistencies identified during the check.

7.4. Electronic documents or their copies, for which integrity violations, invalidity of the electronic signature or non-compliance with the requirements of this Procedure have been established, are not subject to acceptance, processing and further use by the UCH.

7.5. Violation of the integrity of an electronic document or an electronic copy of a paper document after affixing an electronic seal is established based on the results of checking the validity of the electronic seal and the integrity of the document. In the event of changes to the document after affixing an electronic seal, such a seal does not confirm the integrity of the document.

7.6. If it is impossible to confirm the integrity, authenticity or authorship of an electronic document, the UCH has the right to require re-submission of the document, submission of the document in a different form or provision of additional information necessary for verification.

8. FINAL PROVISIONS

8.1. This Procedure shall enter into force on the date of its approval by the Director of the UCH, unless another date of entry into force is specified in the decision on its approval.
8.2. UCH ensures unhindered access of (potential) clients/counterparties to this Procedure by posting it on the official UCH website.
8.3. The Procedure, as well as all amendments and additions to it, are approved by the Director of the UCH.
8.4. In the event of any part of this Procedure not complying with the current legislation of Ukraine, including in connection with the adoption of new acts of Ukrainian legislation (in particular, regulatory legal acts of the NSSMC), this Procedure will be valid only in that part that does not contradict the current legislation of Ukraine.
8.5. Termination or invalidity of any of the clauses of this Procedure shall not entail the invalidity or termination of the validity of other clauses of the Procedure.