

**creditwest bank**

APPROVED

By the decision of the Board of  
CREDITWEST BANK JSC

Minutes of the Board of Directors of the Bank  
No.3 dated January 15, 2020

**Procedure  
of processing of electronic documents in terms of electronic trust services of  
CREDITWEST BANK JSC**

**Kyiv 2020**

**Content**

1.	Introduction	4
2.	Terms and Definitions	4
3.	Goal and Objectives	5
4.	Scope of Application	5
5.	General Provisions	5
6.	Rules of Electronic Interaction	5
7.	Creation and Certification of Electronic Copy from a Paper Document	6
8.	Creation and Certification of a Paper Copy from the Electronic Document	7
9.	Detection of Any Changes in an Electronic Document	7
10.	Detection of Any Changes of Electronic Signature after Singing of an Electronic Document	7
11.	Final Provisions	7

History of the document:

<b>Version of the document, date of the version:</b>	1.00 dated <b>January 15, 2020</b>
<b>Registration number of the document:</b>	ir_483
	Department of Business Development  Department of Bank Business Processes Management  Foreign Exchange Control Division
<b>Developing subdivision:</b>	Information Security Division
<b>Access level:</b>	Public information

<b>Version No.</b>	<b>No. and date of the document on approving</b>
1.00	Minutes of the Board of Directors of the Bank No.3 dated January 15, 2020

## **Introduction**

- 1.1. The Procedure of processing electronic documents in terms of electronic trust services of CREDITWEST BANK JSC (hereinafter – the Procedure) determines the measures and means of electronic documents managing by participants of electronic trust services.
- 1.2. The Procedure is developed in accordance with the current legislation of Ukraine and the requirements of the National Bank of Ukraine in the field of electronic trust services.
- 1.3. The Bank provides clients and potential clients with free access to the internal regulatory document “Procedure of processing electronic documents in terms of electronic trust services of CREDITWEST BANK JSC” by placing the document on the Bank’s website on the Internet.

## **2. Terms and Definitions**

2.1. Terms and definitions are used in the following meanings in the Procedure:

**Bank** is CREDITWEST BANK JSC

**Other party** means a client, potential client, individual or interested person who on the basis of the contract on electronic interaction intends or performs transactions or legal actions using a qualified electronic signature obtained from a qualified provider of electronic trust services.

**Electronic document** means a document where information is recorded in the form of electronic data, including mandatory document details;

**Electronic interaction** means a regulated list of processes for creating, sending, transmitting, receiving, processing, using, storing, destroying electronic documents and copies of paper documents in electronic form using a qualified electronic signature or a qualified electronic seal.

**Client-Bank system** means a system of remote control of Bank accounts, applying of an electronic signature and sending of an electronic document with an applied EDS to the Bank;

**Identification of a person** means a procedure of using the identification data of a person from the documents created on tangible media and/or electronic data, in the result of implementation of which an unambiguous identification of an individual, legal entity or representative of a legal entity is provided;

**Qualified electronic seal** means an advanced electronic seal that is created using the qualified electronic seal tool and is based on a qualified electronic seal certificate;

**Qualified electronic signature** means an advanced electronic signature that is created using the qualified electronic signature tools and is based on a qualified public key certificate;

**Qualified provider of electronic trust services** is a legal entity, regardless of its legal form and form of ownership, an individual entrepreneur who provides one or more electronic trust services whose activities meet the requirements of this law and whose information is included in the trust list;

**Private key** is a parameter of an asymmetric cryptographic conversion algorithm that is used as unique electronic data for creation of an electronic signature or seal, available only to the signer or the e-sealer, and for purposes defined by the standards for qualified public key certificates;

**Verification** is the process of authenticating and confirming that an electronic signature or seal are valid;

**Subscriber** is an individual who creates an electronic signature and applies it to an electronic document;

**Qualified electronic signature tool** is a hardware-software or hardware device or software that implements cryptographic algorithms for generating of key pairs and/or creation of a qualified electronic signature, and/or verifying a qualified electronic signature, and/or storing of a personal key of a qualified electronic signature that meets the requirements of the Law On Electronic Trust Services.

2.2. Other terms and definitions are used in this document in accordance with the Laws of Ukraine On Electronic Trust Services and On Electronic Documents and Electronic Document Management.

### **3. Goal and Objectives**

3.1. According to the requirements of the current legislation and legal acts of the document to determine the order of:

- 3.1.1. Creating and certifying of an electronic copy from a paper document;
- 3.1.2. Creating and certifying of a paper copy from an electronic document;
- 3.1.3. Identifying of any changes in an electronic document;
- 3.1.4. Identifying of any changes to the ES after signing an electronic document;
- 3.1.5. Works with an advanced electronic seal and qualified electronic seal of the Bank.

3.2. Provide the unhindered access to regulated information from clients, partners, and stakeholders.

### **4. Scope of Application**

4.1. The provisions of this Procedure apply to the processes of processing and converting of electronic documents certified with an electronic digital signature in the course of performing legal actions.

4.2. In order to achieve the goal and objectives, the requirements of the Procedure are mandatory for all employees of the Bank, clients and interested parties who are participants of electronic interaction in terms of electronic trust services.

### **5. General Provisions**

5.1. Electronic interaction with the Bank, in terms of electronic trust services, is implemented exclusively using a qualified electronic signature and/or a qualified electronic seal.

5.2. Channels of transmitting electronic documents with a qualified electronic signature (hereinafter – certified documents) from the client to the Bank are determined by the terms of the Bank's Public offer to conclude an additional agreement to the contract on providing services under the CLIENT-BANK system "Procedure for handling, storing and destroying of electronic documents in CREDITWEST BANK JSC" (hereinafter – the Public offer).

5.3. Certified documents sent to the Bank are considered to be received by the Bank only if authorized employees of the Bank provided confirmation in electronic form on their receipt.

5.4. The Bank has the right to reject or not to accept incoming electronic documents if they contain incomplete or unreliable information, which makes it impossible or raises doubts about the legitimacy of the transaction or operations.

## **6. Rules of Electronic Interaction**

- 6.1. The client, individual or a stakeholder has the right to switch to electronic interaction with the Bank in the terms of financial, economic or business activities.
- 6.2. Electronic interaction with the Bank requires the other party to have a qualified electronic signature provided by one of the following qualified providers of electronic trust services:
- Central certification body-Ministry of Justice of Ukraine
  - National Bank of Ukraine
  - State Treasury Service of Ukraine
  - Ukrainian Special Systems, State enterprise
  - Ministry of Internal Affairs of Ukraine
  - National Depository of Ukraine, Public Joint-Stock Company
  - Art-Master, Limited Liability Company
  - Center of Key Certification “Ukraine”, Limited Liability Company
- 6.3. The other party has the right to use the following means of electronic trust services for making a transaction or other legal actions in accordance with the legislation:
- Qualified electronic signature;
  - Qualified electronic seal.
- 6.4. Initial identification of the client is carried out directly in the Bank’s premises and is accompanied by the conclusion/acceptance of the Public offer by the Client.
- 6.5. The other party bears full personal responsibility for providing or late provision of information about changes in activities, officials, personal data and other data specified by law, which must be provided to the Bank.
- 6.6. By concluding the Public offer, the other party confirms that it is familiar with the requirements of the Law of Ukraine On Electronic Trust Services and the rules for using information security tools provided by an accredited provider of electronic trust services and undertakes to strictly comply with them.
- 6.7. The subscriber is not allowed to create a qualified ES if the subscriber’s qualified public key certificate is invalid or it is not possible to obtain information about its status

## **7. Creation and Certification of Electronic Copy from a Paper Document**

- 7.1. The Bank accepts certified electronic copies of a paper document from the other party under the following conditions:
- Copies of documents in electronic form are created by scanning only the original paper document.
  - Completely all pages of a paper document are included in the form and in the order of the document scanning process and are an integral part of a single PDF file and created from the original paper document.
  - All pages of a single document are scanned in a single file in black-and-white / color format (for example: contract - 1 file, additional agreement - 1 file, letter of explanation - 1 file, etc.);
  - The text, seals, and signatures on an electronic document are completely clear, and do not contain tinting or lost characters or signs while scanning;

- The text of the electronic document does not contain any signs of hand corrections or other physical damages;
- The size of one scanned document must not exceed 10 MB.
- The Bank does not accept scanned copies of documents that are not created from the original, with obvious signs of damage of the documents (they contain crossed out words, erasures, distortions, poured pages, changes made by hand, as well as other mechanical errors);
- To scan the documents that will be sent to the Bank, you must configure the scanner to meet the following requirements:
  - Resolution of at least 300 DPI (dots per inch), if the original document is of poor quality – the text is pale, blurred, smeared, not clear seal impressions, etc. scanning is performed with a higher resolution.
- The valid format for scanned electronic files is **PDF ONLY**.

7.2. The electronic document has an electronic qualified signature of the official and, if necessary, a qualified electronic seal of the legal entity.

7.3. A certified document can be verified for integrity and authenticity using the tools of AKCC of the Ukrainian justice authorities or other AKCC defined in section 6.

7.4. The Bank reserves the right not to accept a certified electronic document if it does not meet the above requirements.

## **8. Creation and Certification of a Paper Copy from the Electronic Document**

8.1. If it is necessary to create a paper copy of a certified electronic document, the Bank's employee must follow the following procedure:

- 8.1.1. To verify the integrity of an electronic document with the software of the provider of electronic trust services or at the website of AKCC of bodies of justice of Ukraine.
- 8.1.2. If there are no signs of violation of the integrity of the electronic document, the employee has the right to print it.
- 8.1.3. A hard copy of the certified document must be signed by an authorized employee in accordance with the Order of the Chairman of the Bank's Management Board.
- 8.1.4. A hard copy signed by an authorized employee must be certified with the Bank's seal.
- 8.1.5. In case of using a hard copy of a certified document within the Bank, it is allowed to apply it without additional certification with the Bank's seal.
- 8.1.6. If any marks and corrections are made to the hard copy of an electronic document, or if it is damaged, it is considered invalid due to a violation of its integrity.

## **9. Detection of Any Changes in an Electronic Document**

9.1. Verification of the integrity of electronic documents is carried out in accordance with the procedure defined by the provider of qualified electronic trust services.

9.2. To check the integrity of an electronic document, the website of AKCC of bodies of justice of Ukraine <https://ca.informjust.ua/> can be used.

**10. Detection of Any Changes of Electronic Signature after Singing of an Electronic Document**

- 10.1. Verification of the validity of qualified public key certificates is carried out exclusively by means of a qualified ES or seal in accordance with the requirements of the Law of Ukraine On Electronic Trust Services
- 10.2. Verification of the electronic signature of the other party is carried out using the Bank's software and hardware.
- 10.3. If there are any factors that call into question the authenticity and validity of the electronic signature used to sign the electronic document, the Bank refuses to accept it and returns it with a brief description of the reasons for rejection.

**11. Final Provisions**

- 11.1. The other party is obliged to notify the Bank of any changes that occur in the process of electronic trust services within one business day from the date of such changes.
- 11.2. The other party is obliged to adhere to the requirements of the current legislation of Ukraine in the process of electronic interaction with the Bank.
- 11.3. The Bank is not responsible for any consequences resulting from improper use or compromise of the personal key of the other party participating in electronic interaction with the Bank.