USER MANUAL

for electronic trust services provided by a Qualified Trust Service Provider “Diia”

Version 1.0

Kyiv

2024

USER MANUAL
for electronic trust services provided by a Qualified Trust Service Provider “Diia”

Table of contents

Date	Version	Amendments
	Version 1.0	Approval of the User Manual for electronic trust services provided by the Qualified Trust Service Provider “Diia”

1. INTRODUCTION

This Manual contains a general description of the process of registration of users of electronic trust services (hereinafter referred to as the “users”) provided by the Qualified Trust Service Provider “Diia” (hereinafter referred to as the “QTSP “Diia”, “Provider”), as well as the procedure for using qualified electronic trust services by users.

Qualified electronic trust services are provided by the QTSP “Diia”, represented by the State Enterprise “DIIA”, which includes the Head Office and separate registration units of the QTSP “Diia”.

QTSP “Diia” provides qualified electronic trust services in accordance with:

- Law of Ukraine “On Electronic Identification and Electronic Trust Services” and other legislative acts in the field of electronic identification, electronic trust services, information and personal data protection;

- Policy of the QTSP “Diia” Certificate (Rules and Procedures of operation of the Qualified Trust Service Provider “Diia”);

- appropriate Provisions of Certification Practices of the QTSP “Diia” (Rules and Procedures of operation of the Qualified Trust Service Provider “Diia”).

- General terms and conditions for the provision of qualified electronic trust services of the user of the Qualified Trust Service Provider “Diia”;

- Agreement for the provision of qualified electronic trust services concluded with the QTSP “Diia” on behalf of the State Enterprise “Diia” in accordance with the Article 634 of the Civil Code of Ukraine by accession to all the terms and conditions of this Agreement under the Application for Accession.

Users of electronic trust services (hereinafter referred to as users) are free to use the results of the received electronic trust services, subject to the restrictions established by the legislation and by the QTSP “Diia”.

1.2. Name of the document and its identification

Name of the document: User Manual for electronic trust services provided by the Qualified Trust Service Provider “Diia”.

Version: 1.0.

1.3. Definition of terms

Electronic signature	Electronic data that is attached to other electronic data or logically linked to it and is used by the signatory as a signature.
Advanced electronic signature	An electronic signature generated using a Qualified Certificate of Electronic Signature issued by the QTSP "Diia" and does not contain data that the private key is stored in a qualified electronic signature tool
Qualified electronic signature	An advanced electronic signature generated using a qualified electronic signature tool and based on a Qualified Certificate of Electronic Signature issued by the QTSP "Diia"
Qualified Certificate of the Public Key	Certificate of Electronic Signature or Seal issued by the QTSP "Diia" and complies with the requirements established by Part two of the Article 23 of the Law of Ukraine "On Electronic Identification and Electronic Trust Services"
Separate registration unit	A subdivision of the QTSP "Diia" or a legal entity or natural person, including a Notary, who, based on the Order of the QTSP "Diia" (its Head) or an Agreement concluded with it, carries out the registration of signatories and generators of electronic seals in accordance with the requirements of the legislation.
Tariff plan	Tariff plan for the provision of qualified electronic trust services and related services by QTSP "Diia" is published on the QTSP "Diia" website at the following link: https://ca.diia.gov.ua.
Qualified electronic signature tool	Hardware or software device or software that are used to generate an electronic signature or seal (electronic signature or seal tool) that complies with the requirements established by Part one to four of the Article 19 of the Law of Ukraine "On Electronic Identification and Electronic Trust Services"

Private key	Unique data that is used by the signatory or electronic seal generator to generate an electronic signature or seal
Public Key	Data used to confirm an electronic signature or electronic seal
"User" software	"Software Complex "IIT User Key Certification Centre-1" software, which is a computer program used to manage the user's key pair (generation of a key pair, storage of a private key and generation of requests for the formation of the Qualified Certificates of the Public Key, etc.), access to the Qualified Certificates of the Public Key (searching for the Qualified Certificates of the Public Key, defining their status, etc.), protection of user files (signing, verification, encryption, decryption)
Signatory	Natural person who creates an electronic signature
Electronic seal	Electronic data used to ensure the authenticity of the origin and integrity of an electronic document
Qualified electronic time stamp	Electronic data that link other electronic data to a specific moment in time to certify the availability of such electronic data at that moment in time (electronic time stamp), which complies the requirements established by the Part two of the Article 26 of the Law of Ukraine "On Electronic Identification and Electronic Trust Services"
Encryption	Converting plaintext to ciphertext (encryption) and recovering plaintext from ciphertext (decryption) with known key data
File key	A private key stored in an electronic signature or seal tool that does not comply with the requirements for a qualified electronic signature or seal tool established by the Parts one to four of the Article 19 of the Law of Ukraine "On Electronic Identification and Electronic Trust Services"

Cancellation of the Public Key Certificate	Suspension of the Qualified Certificate of the Public Key
Electronic seal generator	Legal entity or natural person-entrepreneur who generates an electronic seal
Blocking the Public Key Certificate	Temporary termination of validity of the Qualified Certificate of the Public Key
Renewal of the Public Key Certificate	Re-establishment of the validity of a previously blocked Qualified Certificate of the Public Key
Mobile application “Diia”	Mobile application of the Unified State Web Portal of Electronic Services (“Diia”)
Diia.Signature (Diia ID)	Remote qualified electronic signature generated using the Unified State Web Portal of Electronic Services (“Diia”)
“E-Resident” information system	Information system created to enable foreigners to obtain e-resident status
Electronic cabinet of the “E-resident”	Personal automated workplace of an e-resident, which is a part of the “E-resident” information system, that allows the e-resident to receive electronic public services and ensures communication with the technical administrator, government authorities and banks that act as tax agents for e-residents.
Mobile application	A computer program that is a part of the “E-Resident” information system with an English interface that allows an applicant to apply for e-resident status and identify the e-resident based on the identification carried out in a foreign Diplomatic Establishment of Ukraine in accordance with the procedure defined by the Procedure for Acquiring and Cancelling the Status of Electronic Resident (E-Resident), identification of persons intending to acquire the status of an electronic resident (e-resident) and the provision of qualified electronic trust services to them, approved by the Resolution of the Cabinet of Ministers of Ukraine No. 970 dated September 5, 2023

Other terms are used in this Manual in the definitions given in the Civil Code of Ukraine, the Law of Ukraine “On Electronic Identification and Electronic Trust Services”, Resolution of the Cabinet of Ministers of Ukraine No. 764 dated June 28, 2024 “Some Issues of Compliance with Requirements in the Fields of Electronic Identification and Electronic Trust Services”, Resolution of the Cabinet of Ministers of Ukraine No. 970 dated September 5, 2023 “Some Issues of Electronic Residents (E-Residents) and Maintenance of the E-Resident Information System”, Resolution of the Cabinet of Ministers of Ukraine No. 1137 dated December 4, 2019 “Issues of the Unified State Web Portal of Electronic Services and the Register of Administrative Services”, and other legislative and regulatory acts on issues of cryptographic and technical protection of information.

2. LIST OF SERVICES PROVIDED BY THE PROVIDER AND TERMS OF USE OF THE PRIVATE KEY

2.1. List of services provided by the Provider

QTSP “Diia” provides users with the following services:

- a qualified electronic trust service for generating, verifying and confirming a qualified electronic signature or seal, including the qualified electronic signature “Diia.Signature”;

- a qualified electronic trust service for formation, verification and confirmation of the validity of a Qualified Certificate of the Electronic Signature or Seal, including a Qualified Certificate of Electronic Signature “Diia.Signature”;

- a qualified electronic trust service for the formation, verification and confirmation of a qualified electronic time stamp;

- other services that do not contradict the requirements of the legislation.

2.2. Terms of use of the private key by the user

Verification and use of the user's private key is carried out by using:

1) "User" software (version 1.3.1.51 or later) installed on a personal computer with an operating system of Microsoft Windows XP/2003 Server/Vista/2008 Server/2012 Server/2016 Server/7/8/8.1/10/11 or Apple macOS 10.0.4 or later;
2) QTSP "Diia" website, which can be accessed using web browsers such as Google Chrome, Mozilla Firefox, or Opera;
3) Mobile application "Diia", installed on an electronic device that complies with the following requirements:

- Android operating system, Android 6.0 or later;

- IOS operating system, IOS 13.0 or later.

For safe storage of private keys, a qualified electronic signature or seal tool is used, which is a hardware or software device or software used to create an electronic signature or seal and which complies with the requirements established by the Parts one to four of the Article 19 of the Law of Ukraine "On Electronic Identification and Electronic Trust Services".

Hardware and software of a qualified electronic signature or seal is usually made in the form of a token - a USB device (externally resembling a flash drive) or a smart card (a plastic card with a chip).

A private key stored in a qualified electronic signature or seal tool is protected against password guessing and copying and has a high level of trust.

A qualified electronic time stamp shall be used to certify the fact of affixing a qualified electronic signature or seal to electronic data (electronic document) at a specific time.

Use of a qualified electronic time stamp for the permanent storage of electronic data is mandatory.

QTSP "Diia" ensures the generation of advanced and qualified electronic signatures and seals based on Qualified Certificates of the Public Keys.

QTSP "Diia" forms Qualified Certificates of Electronic Signature or Seal according to the state (DSTU) and international (RSA and ECDSA) algorithms.

Document with an electronic signature can be downloaded in .p7s format (CAdES data storage and signature format) or ZIP-archive (ASiC-S or ASiC-E data storage and signature format).

Description and properties of the signature formats are provided in the table:

Electronic signature format ASiC-E	Allows to store one or more file objects with related electronic signatures and subsequently add file objects, electronic signature files, and electronic time stamps.
Electronic signature format ASiC-S	Allows to store a single file object with a related electronic signature and add new ones in the future. It also allows to add files to protect electronic time stamps.
Electronic signature format CAdES	Unified electronic signature, which allows you to sign electronic data of any format, as well as store electronic data and electronic signature in separate files. For further verification of the CAdES electronic signature, two files will be needed: the original (without an electronic signature) and the signed one. It is used for files up to 25 MB and more.
Electronic signature format PAdES	A unified electronic signature that allows to to sign electronic data in PDF format using software for PDF files. Does not support parallel signing of electronic data. For files up to 25 MB.
Electronic signature format XAdES	A unified electronic signature that allows you to sign electronic data of any format. It also stores the electronic signature in XML format, separately from or together with electronic data. Supports parallel and sequential signing of of one or more electronic documents. For files up to 25 MB.

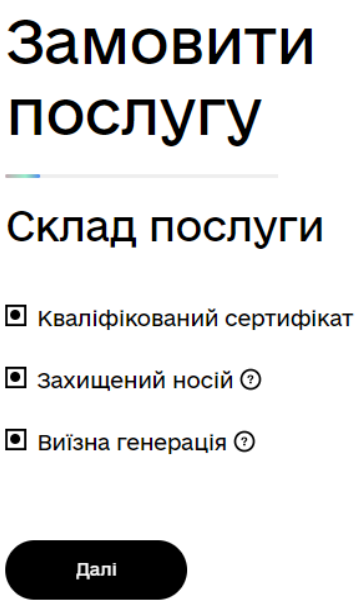
3. PROCEDURE FOR RECEIVING SERVICES PROVIDED BY THE PROVIDER

3.1. Ordering a Qualified Certificate of the Public Key on the Provider’s website

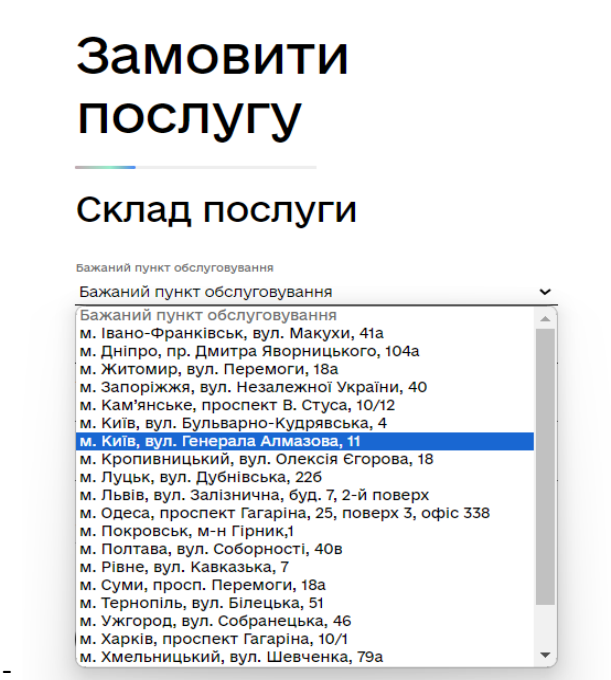
To order a Qualified Certificate of the Public Key (in the form of a file or on a secure medium), the user must fill out a form on the website of the QTSP “Diia” at https://ca.diia.gov.ua/askrav2/?page=supermarketa in the following sequence:

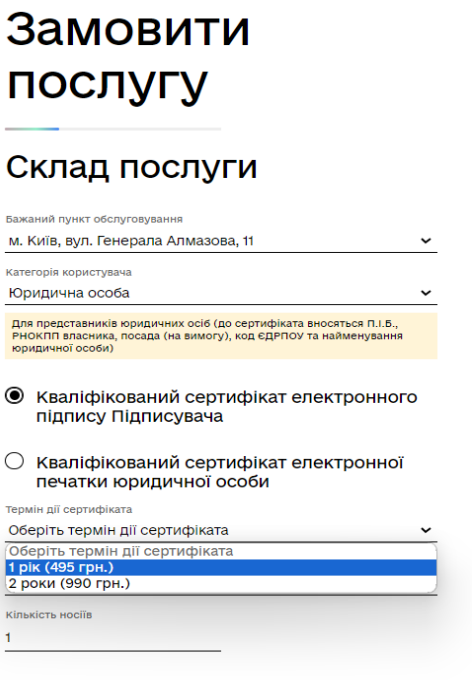
Select the components of the service:

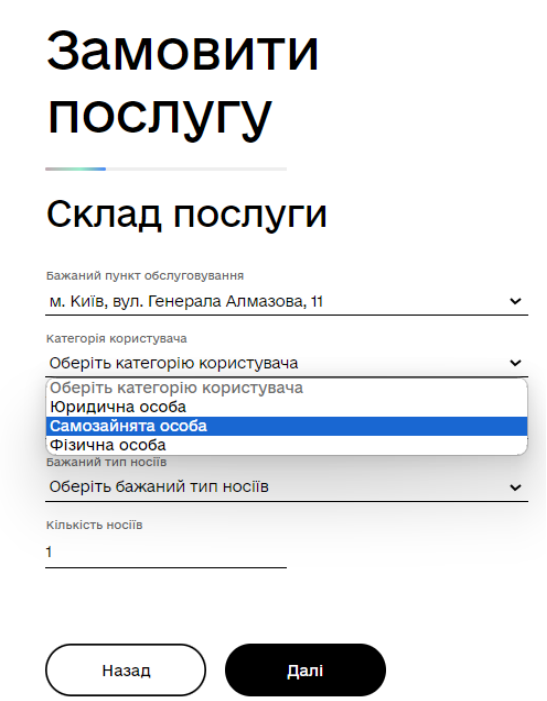
●qualified certificate and/or secure medium (if necessary, use a qualified electronic signature or seal tool to store a private key) and/or offsite generation (if necessary) and click “NEXT”



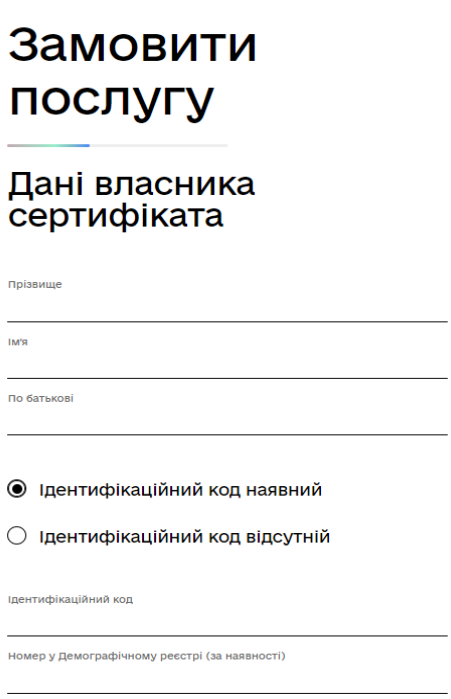
- separate registration unit, tariff plan and certificate validity period







- Fill in the identification data of the certificate owner (signatory):



According to the selected tariff plan (natural persons or legal entities) must fill in the required fields, moving to each following page. The order form filling is completed when the payment method is selected (online payment or at a bank branch). The list of required documents, the registration application is sent to the email specified by the user.

After ordering the service on the QTSP “Diia” website, the User shall visit the selected registration unit to receive the Services, except for users who have ordered the offsite generation service. When ordering offsite generation, QTSP “Diia” specialist will visit the client’s workplace (office) to provide the Services.

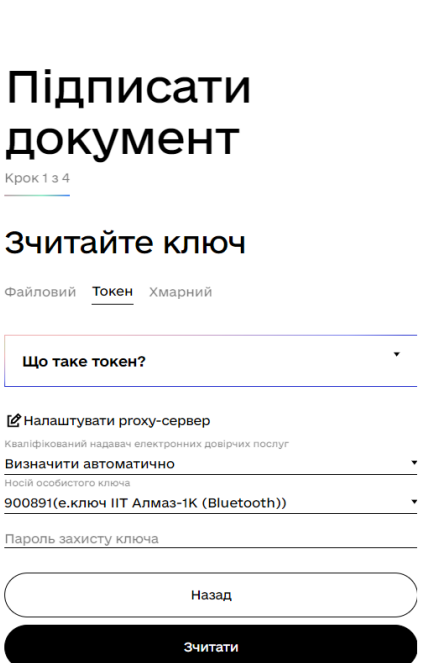
3.2. Signing documents

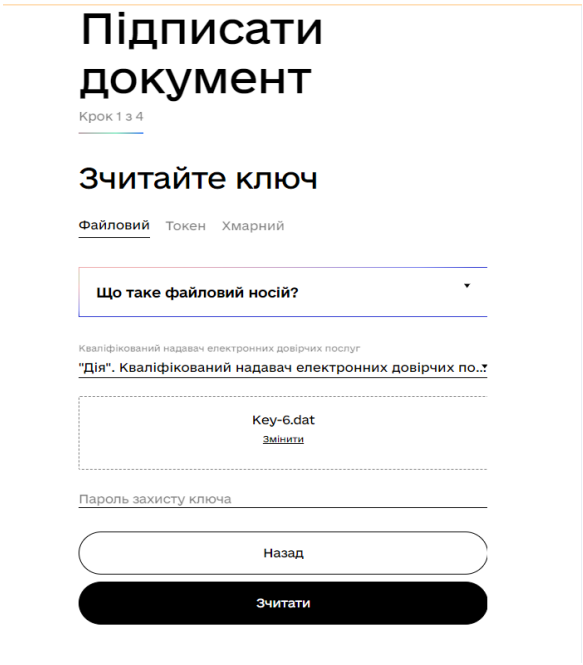
3.2.1. Signing documents on the Provider’s website

Documents can be signed on the QTSP “Diia” website in the section “Sign Documents” (file size not larger than 25 MB) using a file key or a private key stored in a qualified electronic signature or seal tool, Diia.Signature.

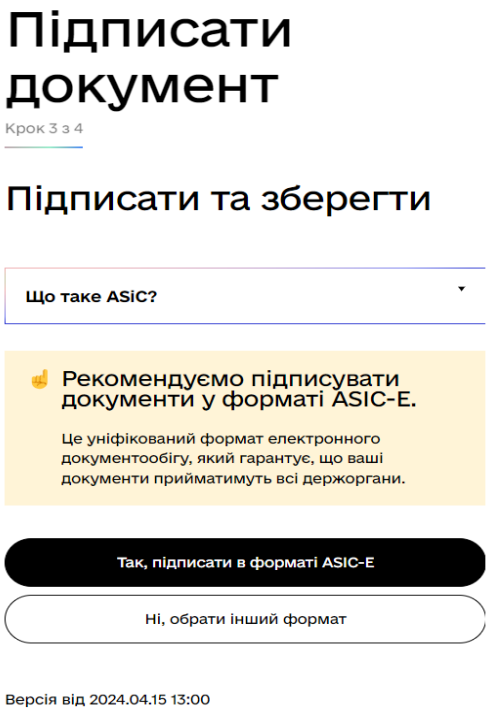
●On the Provider’s website, select the “Sign a Document” service and sign using the “Electronic Signature”.

●Select an existing private key (file, token or cloud signature), enter the password for the private key and click “Read”. To work with tokens (secure media), if necessary, install the web signature library in your browser.

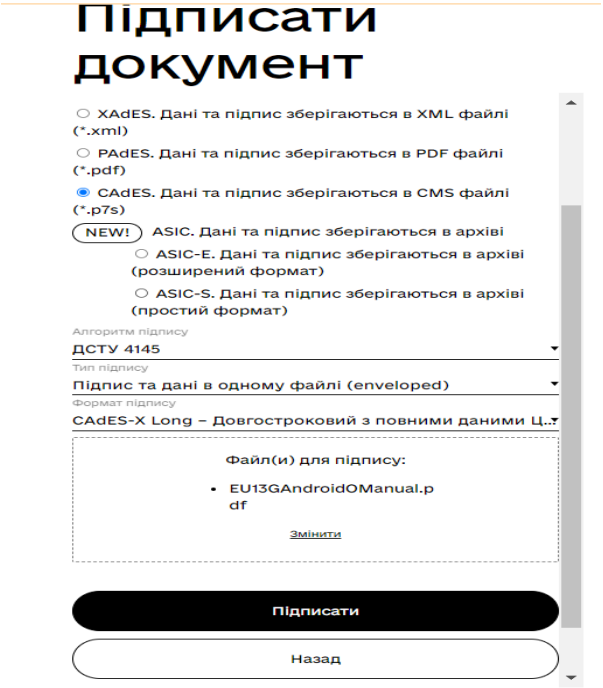




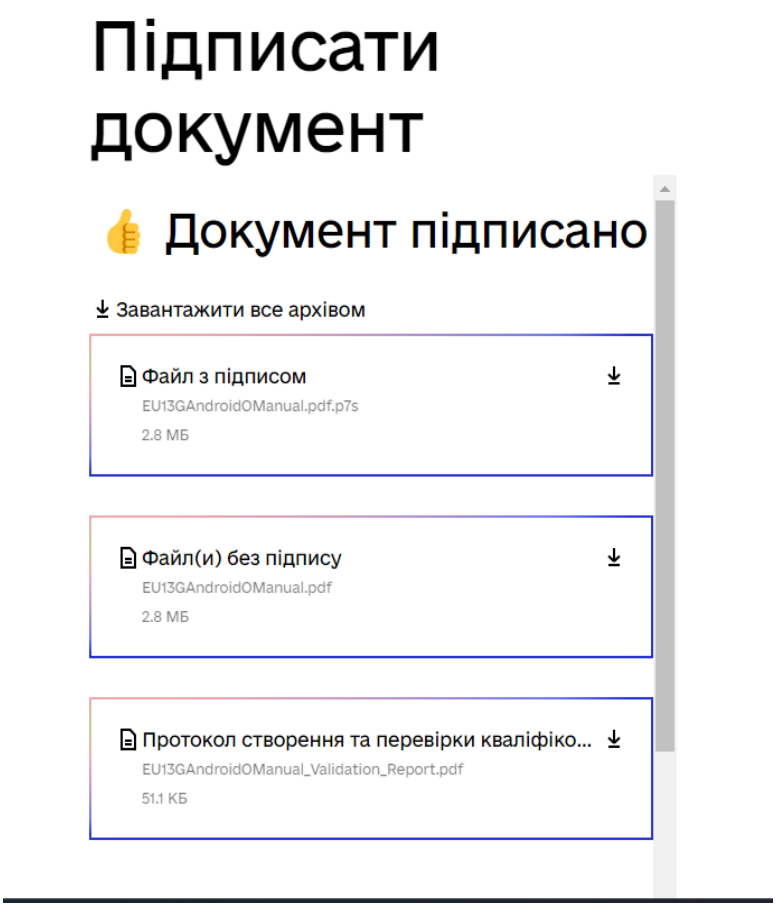
●After successfully reading the private key, click “Next” and select the format of the electronic signature.



●Select the format, type and algorithm of the electronic signature, the required document to be signed and click “Sign”.



●After signing documents, the signed file is displayed in the browser, as well as a file without an electronic signature and the protocol for generating an electronic signature, in which the time stamp and the signatory’s data are indicated. To save these files, click on the arrows and download the required document to your computer.

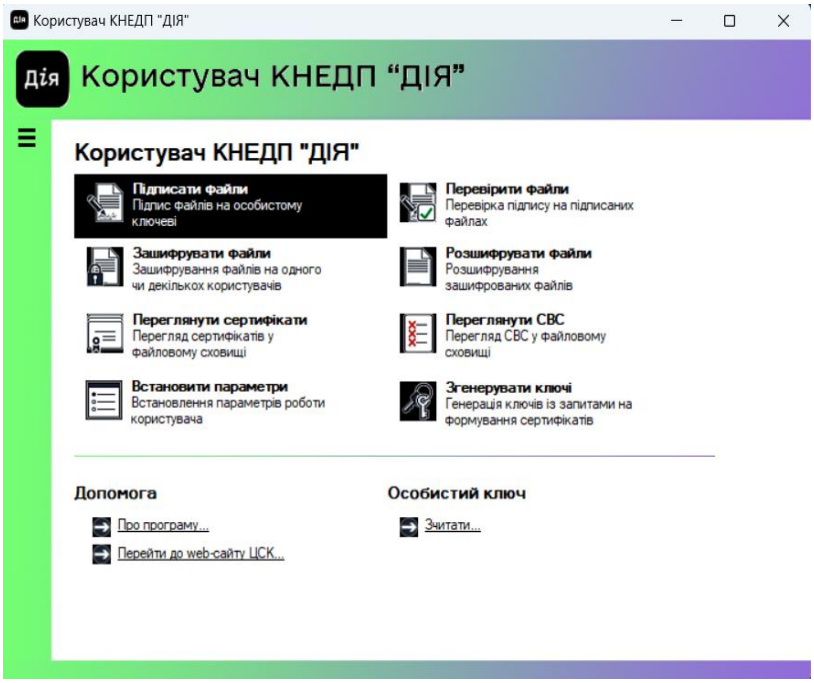


3.2.2. Signing documents using the “User” software

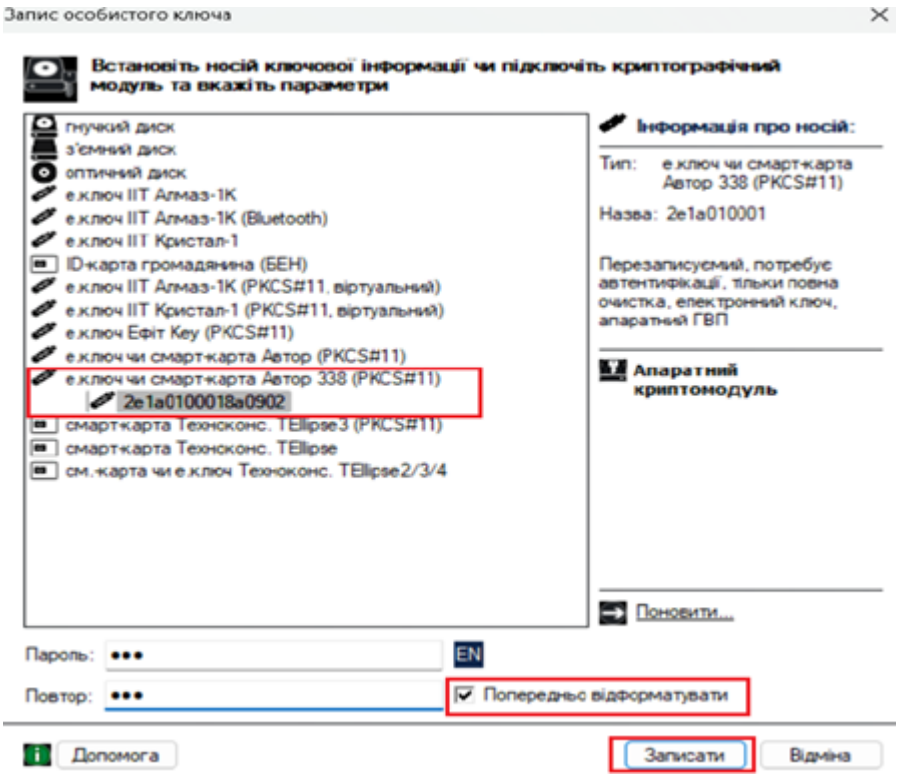
Using the “User” software, the signatory may use a file key or a private key stored in a qualified electronic signature or seal tool to sign files larger than 25 MB on a personal computer.

The “User” software can be downloaded from the website of the QTSP “Diia” at the following link: **https://ca.diia.gov.ua/download-all**

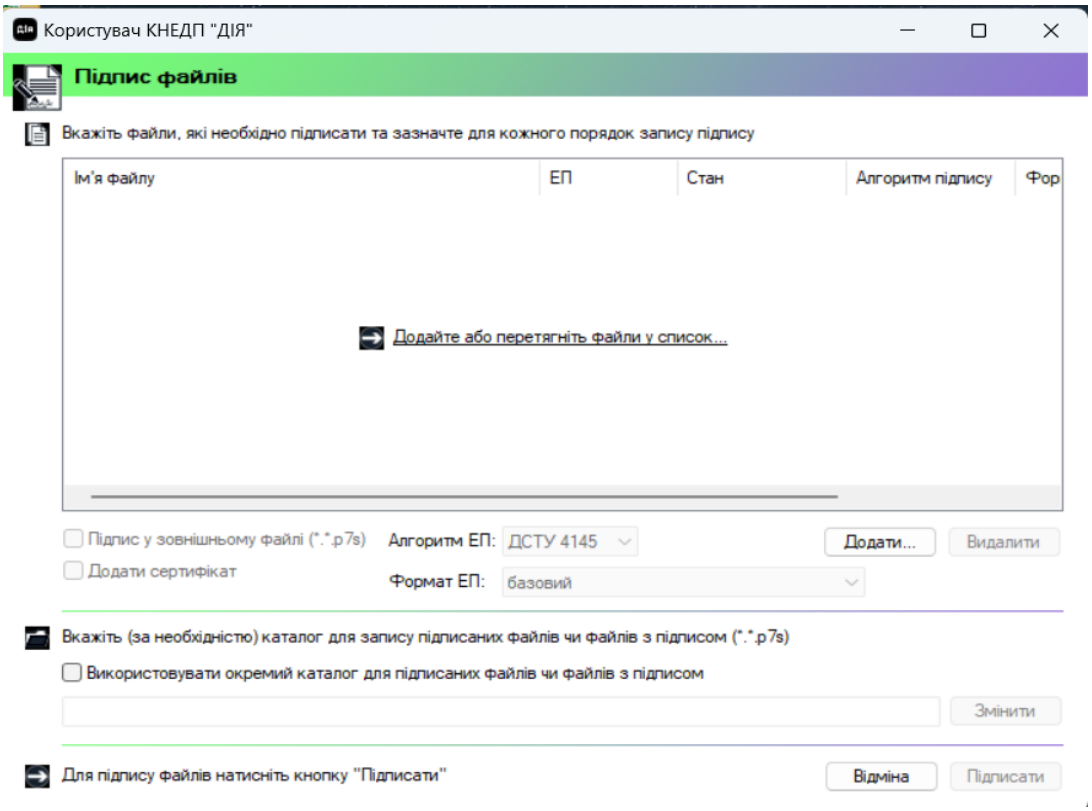
●After installing the “User” software on your personal computer and opening it, select “Sign files”.



●Select your private key, enter the password and click “Read”



●Click “Add” and select the required file to be signed or several files from the computer’s catalogue and click “Sign”. After that, the signed files are saved to the catalogue where the corresponding files without an electronic signature are stored. The file containing the electronic signature has the extension “*p7s” and the electronic signature format CAdes.



3.3. Verification of signed files

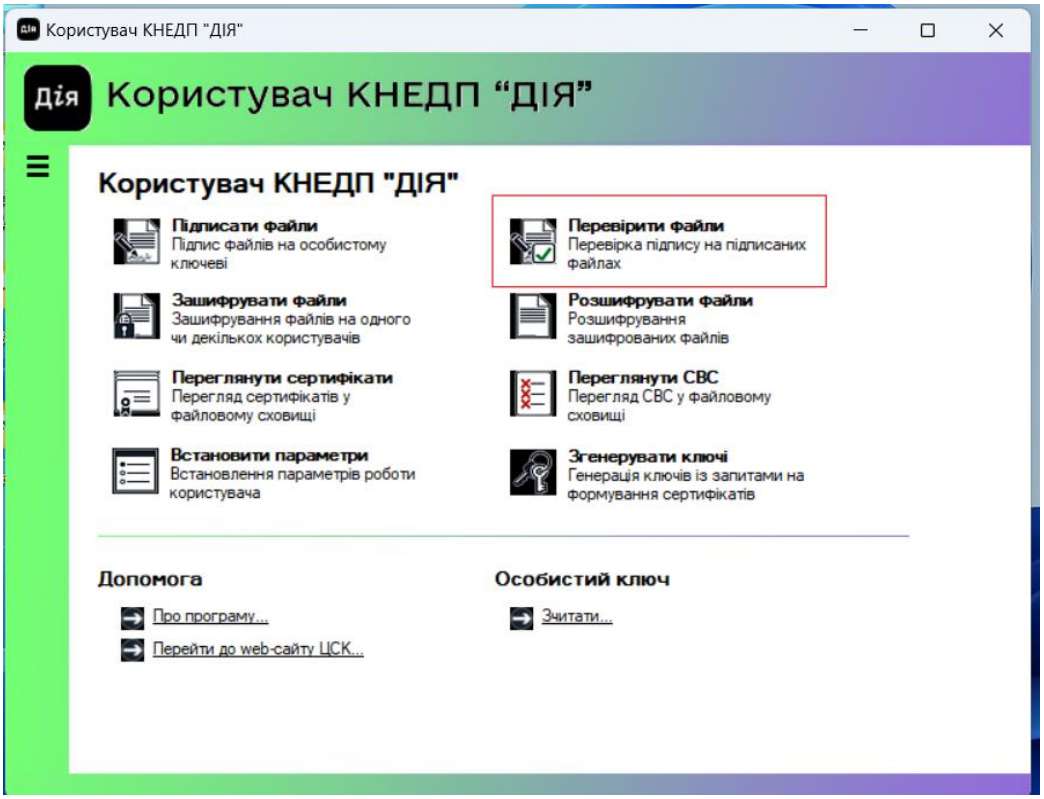
3.3.1. Verification of signed files on the Provider’s website

To verify a signed file, select the “Verify signature” service on the Provider's website and drag or upload the file with an electronic signature

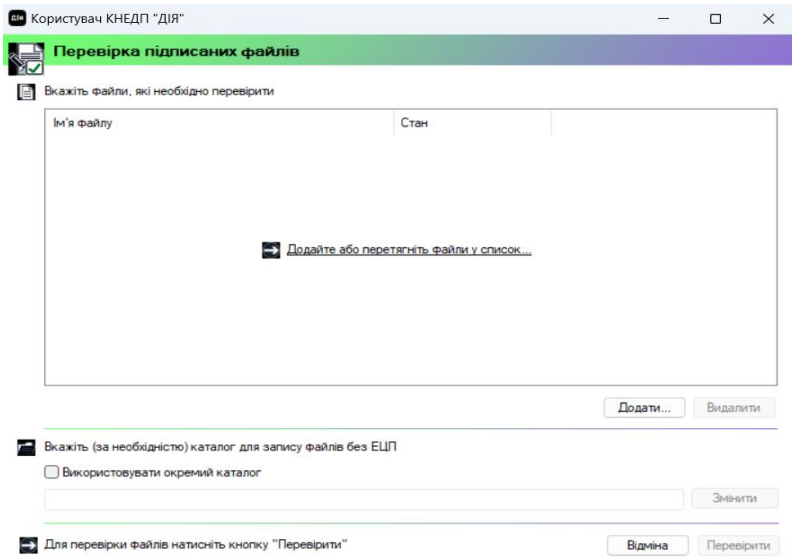
After verification of the signed file, the following documents are formed: a file with an electronic signature and a file without an electronic signature, an electronic signature verification protocol and information about the signatory/s, electronic signature format, the Provider, certificate serial number, electronic signature type, time stamp, etc. These documents can be downloaded to the user’s computer if necessary.

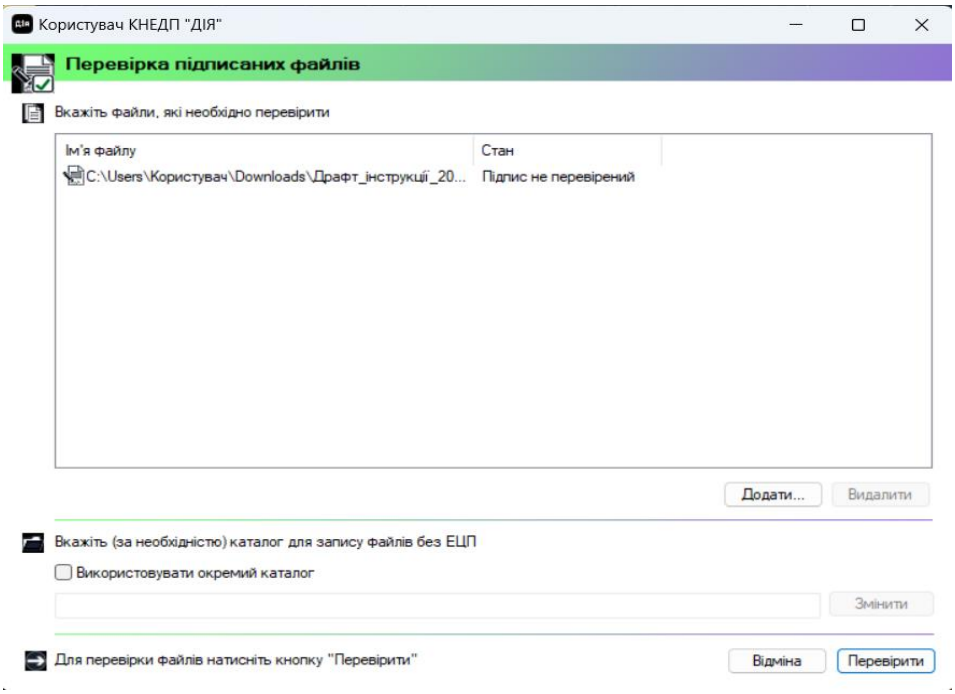
3.3.2. Verification of signed files using the “User” software

●The verification of signed files (larger than 25 MB) is possible by using the “User” software. To do this, launch this software, select the “Verify file” section in the main menu.

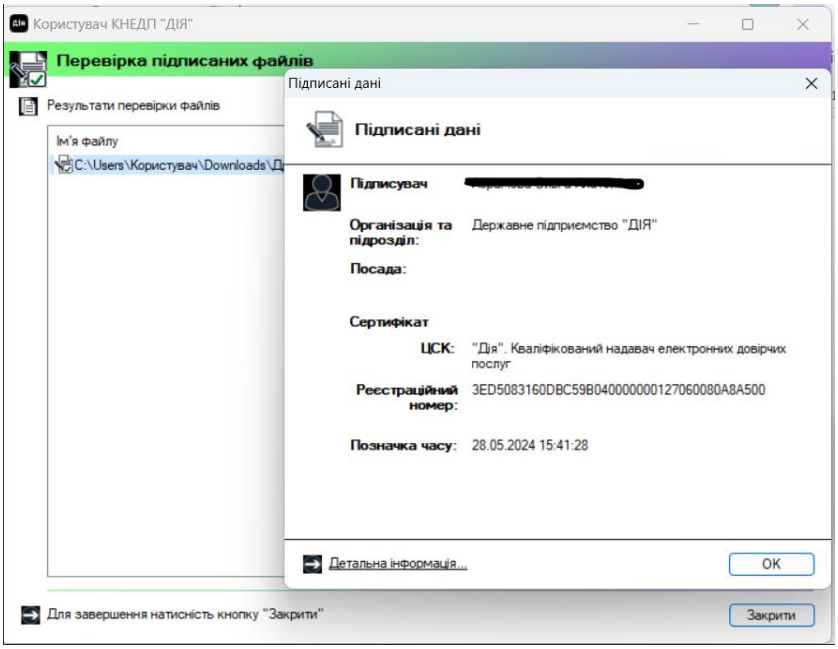


●Drag or add file from your computer’s catalogue and click “Verify”





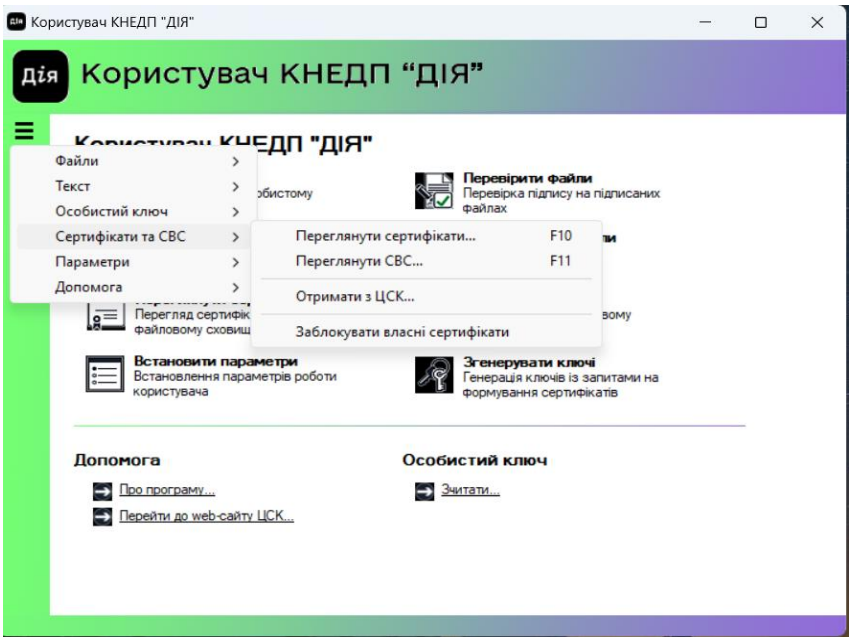
●After successful verification, the file without an electronic signature is sent to the catalogue on the computer where the signed file was stored; by clicking on the file name, you can get information about the signatory, certificate number, time stamp and the Provider who issued the Qualified Certificate.



3.4. Procedure for blocking, renewing and cancelling the Qualified Certificates of the Public Key

3.4.1. Blocking the Qualified Certificates of the Public Key using the “User” software

Blocking the Certificates of the Public Keys is possible using the “User” software if you have a private key and password to it. To do this, in the main menu of the “User” software, select “Certificates and CRLs” and “Block private certificates”, enter the password to the private key and click “OK”.

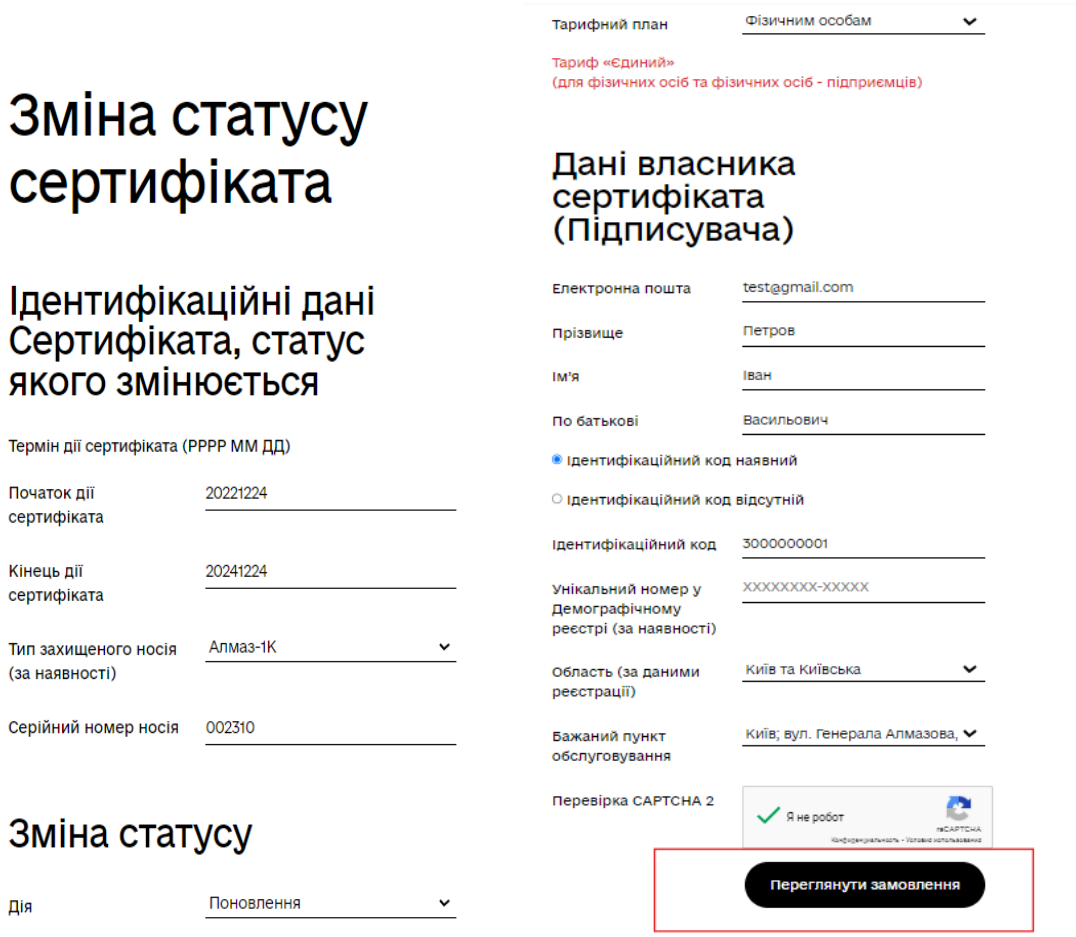


*In case of loss of the key or password, the certificates are blocked upon verbal request of the signatory to the Services Provider, where the electronic signature/seal certificates are blocked by the voice authentication phrase.

3.4.2. Renewal of the Qualified Certificates of the Public Key

Renewal of a Qualified Certificate of the Public Key is carried out by written application, which the user must form on the QTSP “Diia” website at the following link: https://ca.diia.gov.ua/faq14, and then personally apply to the registration unit of the QTSP “Diia” for renewal of the appropriate certificate.

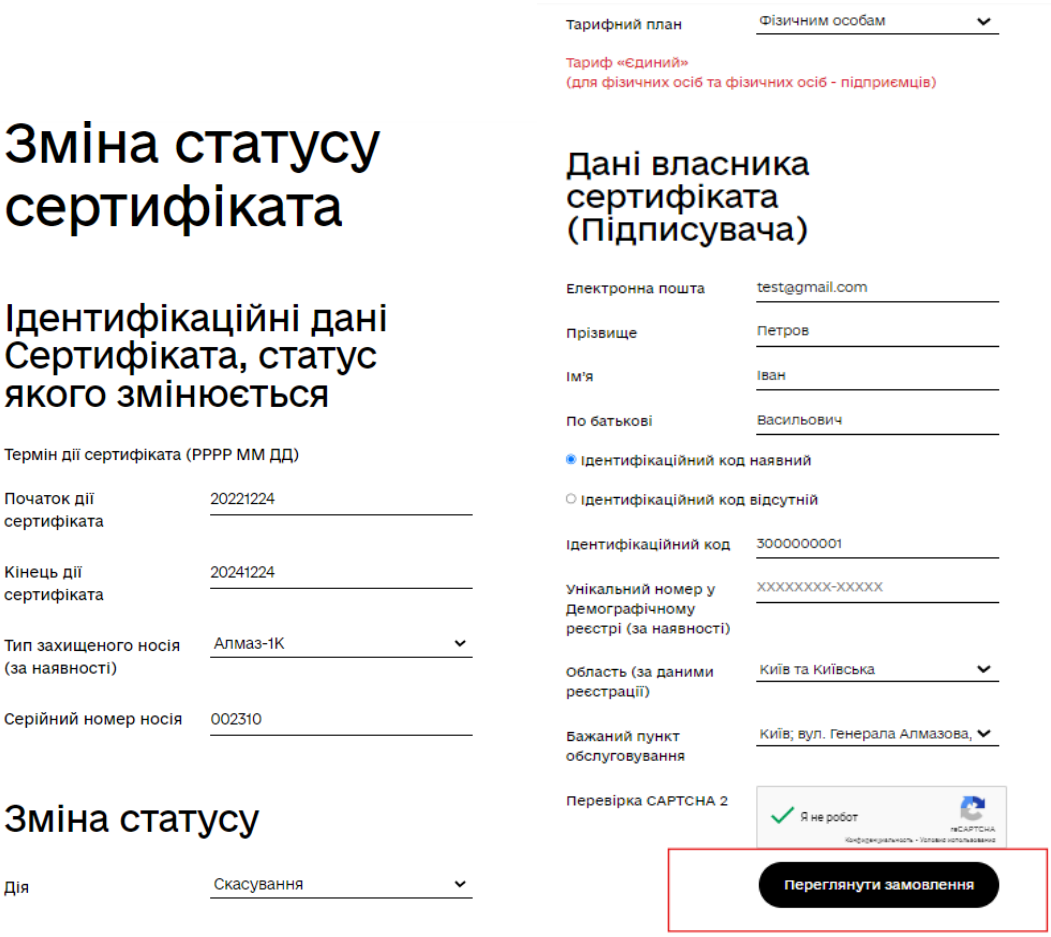
After the procedure of blocking a Qualified Certificate of the Public Key, its status can be renewed within 30 (Thirty) calendar days. Upon expiry of the specified period, the Qualified Certificate of the Public Key will be automatically cancelled by the QTSP “Diia”.



3.4.3. Cancellation of the Qualified Certificates of the Public Key

Cancellation of the Qualified Certificates of the Public Key is carried out by written application, which the user must form on the QTSP “Diia” website at the following link: https://ca.diia.gov.ua/faq14, and then personally apply to the registration unit of the QTSP “Diia” to cancel the appropriate certificate.

Cancelled certificates cannot be renewed.

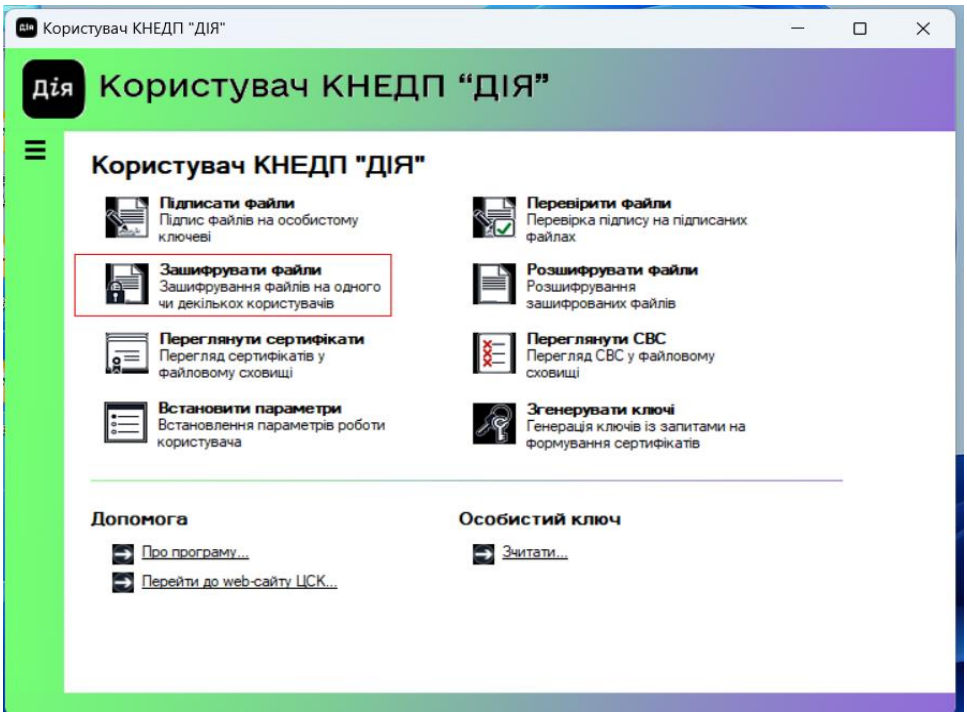


3.5. Files ciphering

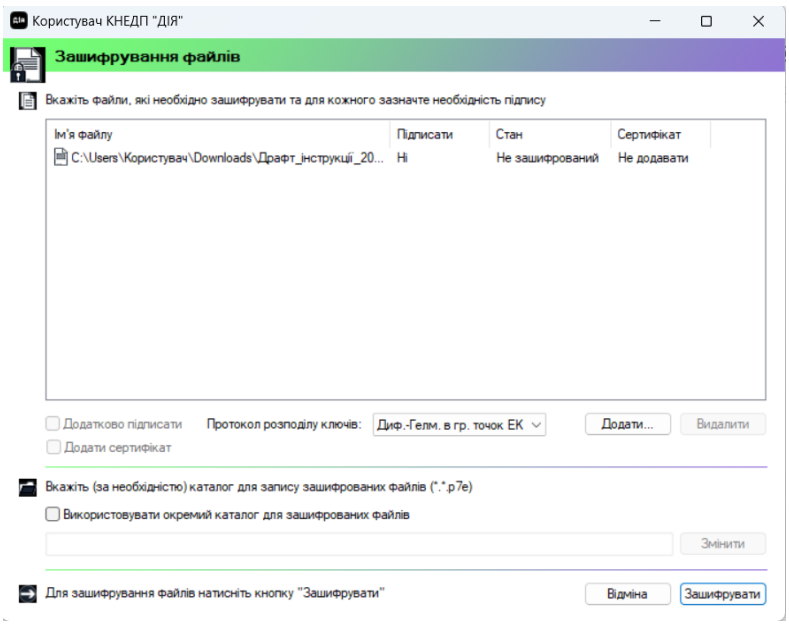
3.5.1. Files encryption

File encryption is carried out using a cryptographic algorithm by encoding data with aim to hide information. As a result of file encryption, a person who does not have a special “key” can only see a set of numbers or a damaged file.

●Files can be encrypted using the “User” software and availability of a Certificate of the signatory with whom the encoded data will be exchanged. To encrypt files, select “Encrypt files” in the main menu of the “User” software.



●Select the file to encrypt by dragging it or adding it from your computer’s catalogue, and click “Encrypt”.



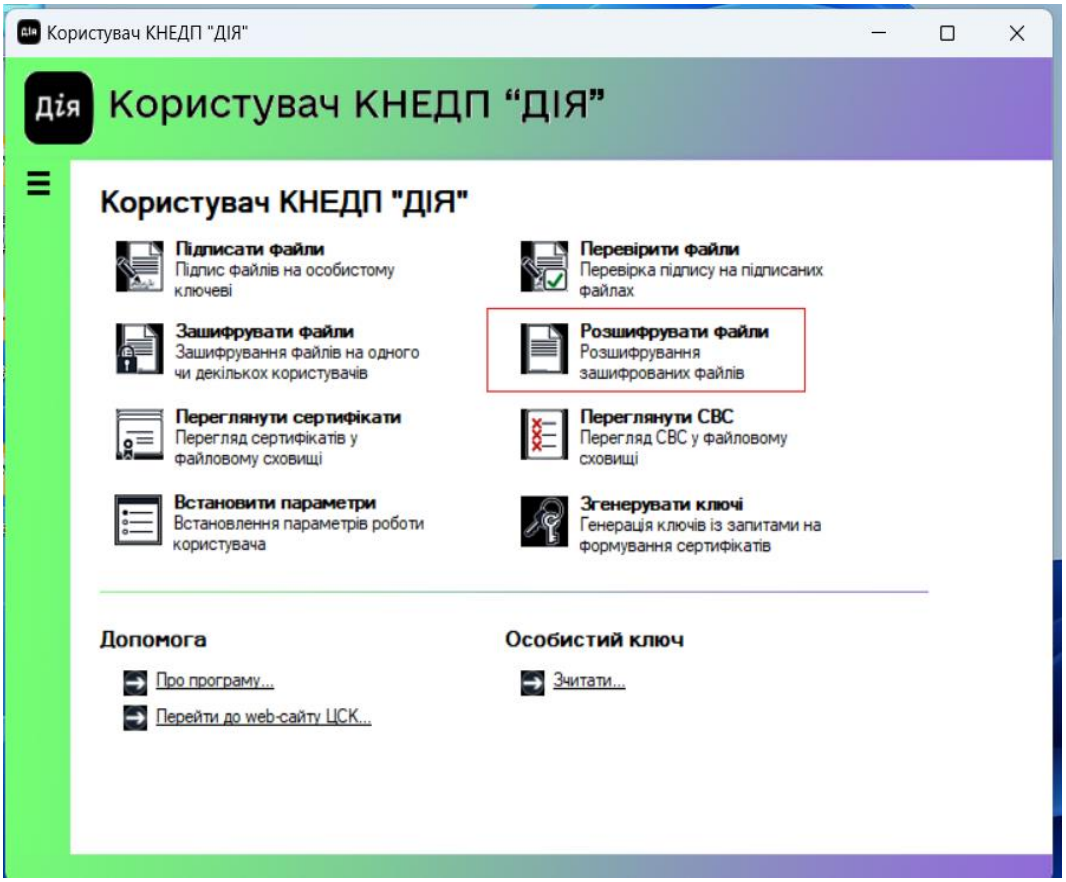
●Select the required certificate from the list of available certificates in the window and click “OK”. If the required certificate is not available, click “Import” and upload the certificate to the certificate store.

*After the file is encrypted, the file is sent to the catalogue where the unencrypted file was stored. The encrypted file has the extension *.p7e.

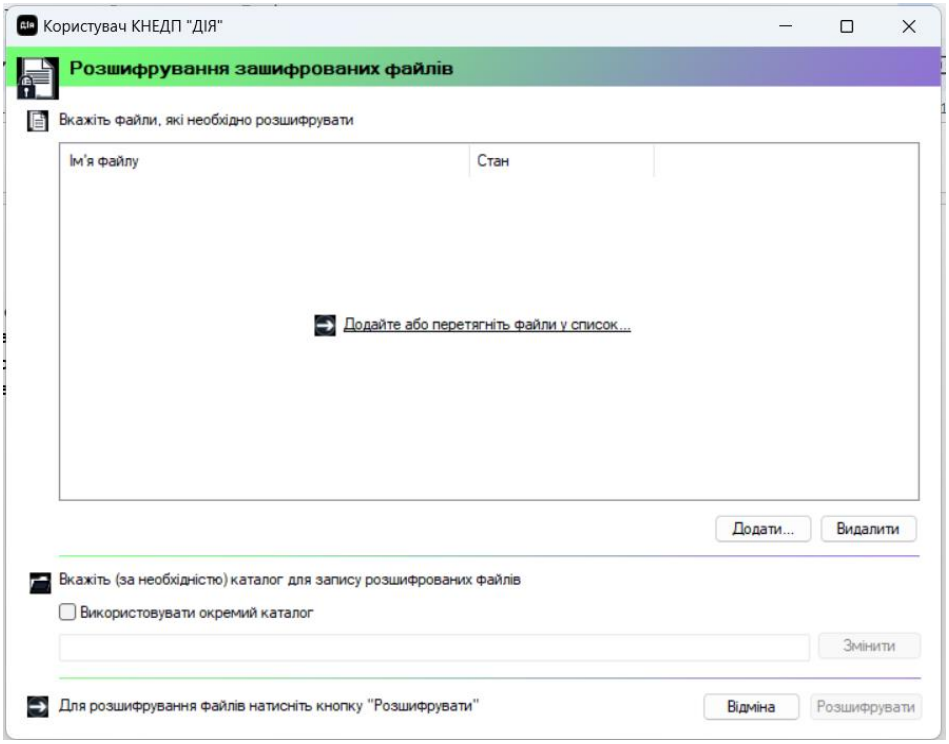
3.5.2. Files decryption

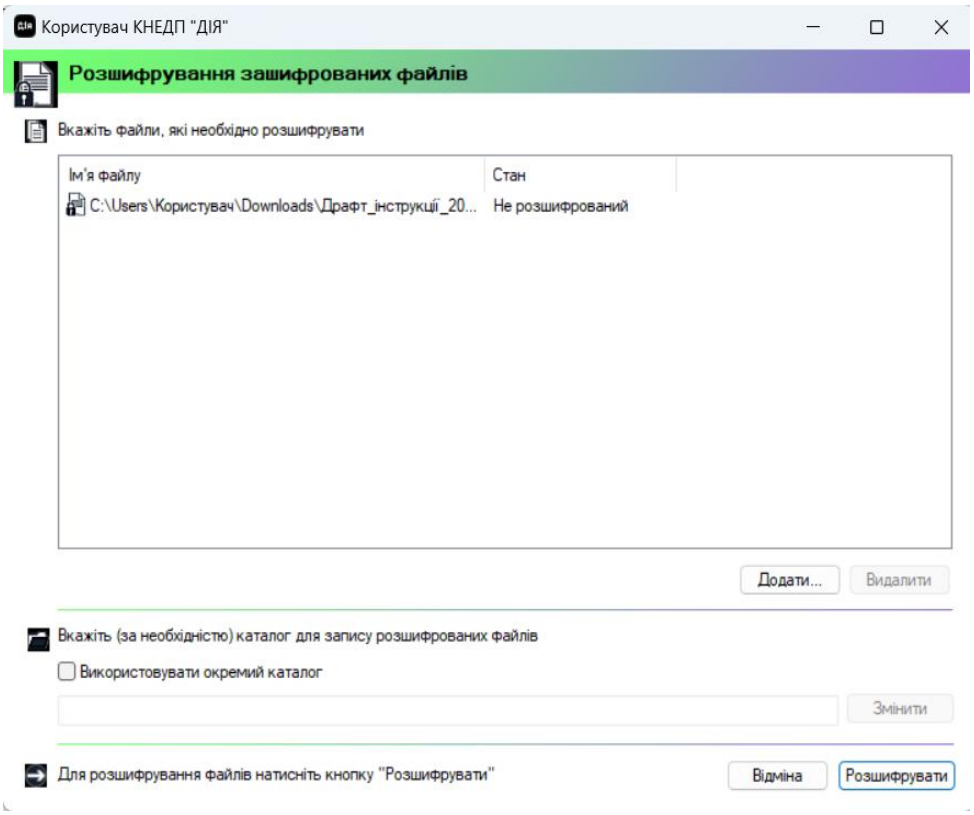
Decryption of an encrypted file is possible only when the encryption key of the user whose certificates were used for encryption is available. This option is carried out by using the “User” software, in the main menu of the “User” software.

●Select “Decrypt files” and read the encryption key:



●In the next window, drag or, as the method of adding, select the encrypted file and click “Decrypt”:





*After decryption is complete, the file that is available for viewing is sent to the catalogue where the encrypted file was stored.

4. PECULIARITIES OF GENERATING, USING, AND DEACTIVATING DIIA.SIGNATURE (DIIA ID)

4.1. Generation of a Diia.Signature (Diia ID)

Validity period of the Diia.Signature (Diia ID) is one year or until it is deleted.

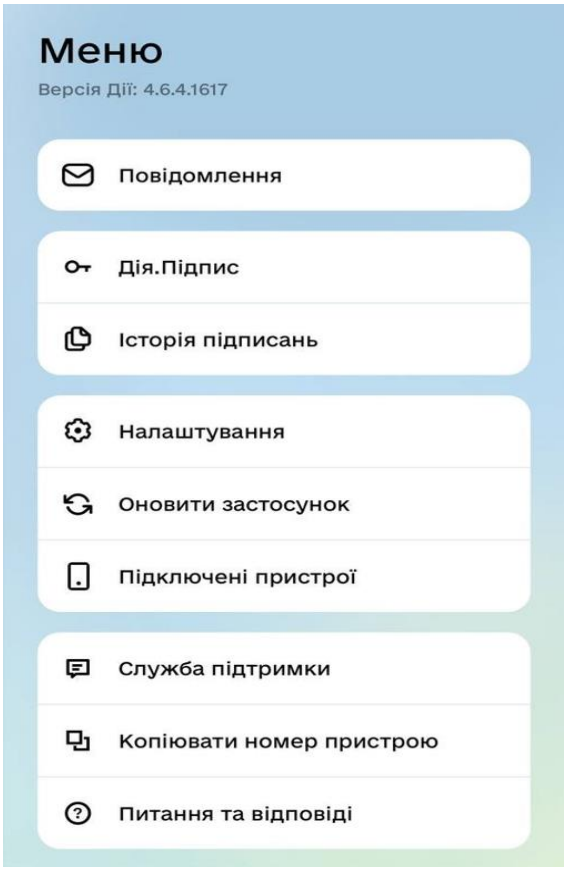
Diia.Signature private key can be based on a national cryptographic algorithm (DSTU) or an international cryptographic algorithm (ECDSA).

The creation of a private key “Diia.Signature” is free of charge using the mobile application “Diia”.

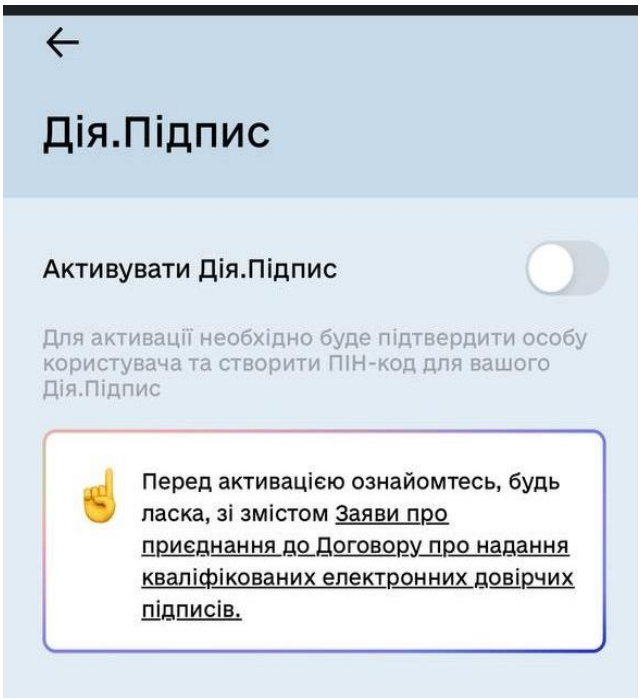
Steps to get a Diia.Signature:

● Log in to the mobile application “Diia”. Select an authorisation method from the proposed ones and use the video instructions to follow the authorisation steps https://www.youtube.com/watch?v=Tt-GKqDaZN8 or https://youtu.be/3ikx_ot7Dpwhttps://youtu.be/Tt-GKqDaZ

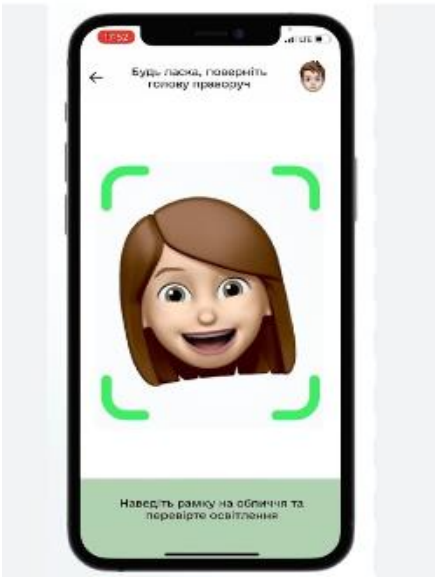
● Go to the Menu and select “Diia.Signature”:



● Learn about the terms of the Agreement and click “Activate Diia.Signature” by dragging the slider to the right:



●Confirm your identity through photo verification:

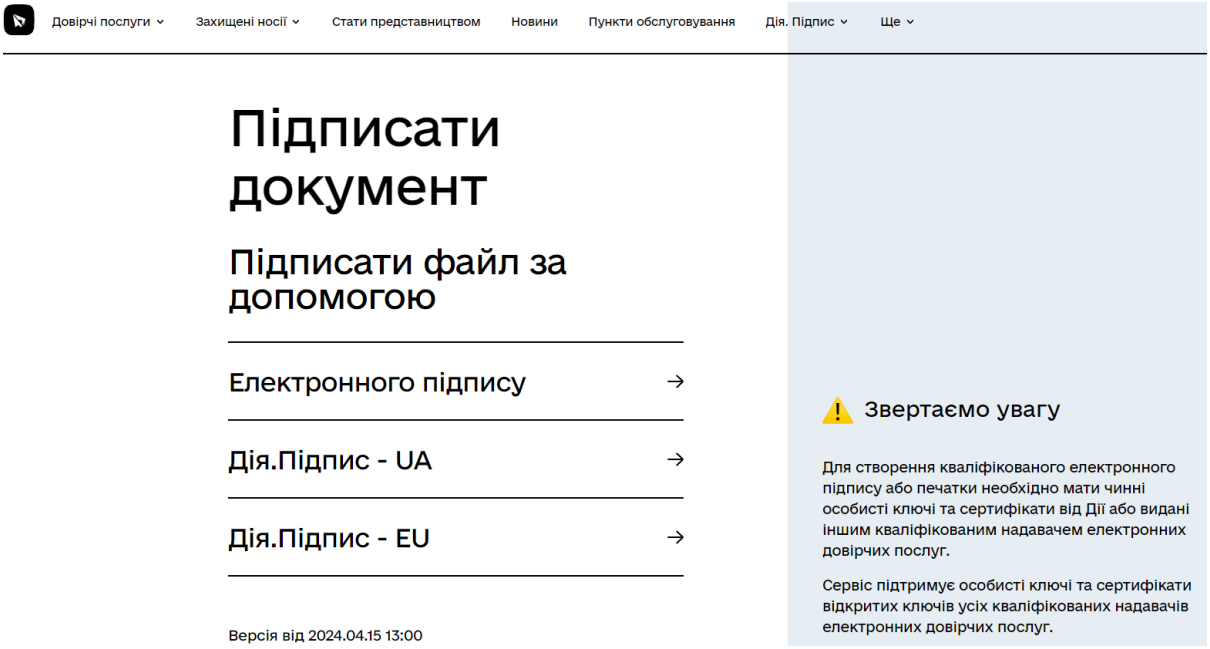


●Set a 5-character password for Diia.Signature:

* This Manual additionally provides video instructions on how to generate a “Diia Signature” Diia.Signature // Full instructions on how to get a Diia.Signature (youtube.com).

4.2. Signing documents with Diia.Signature (Diia ID)

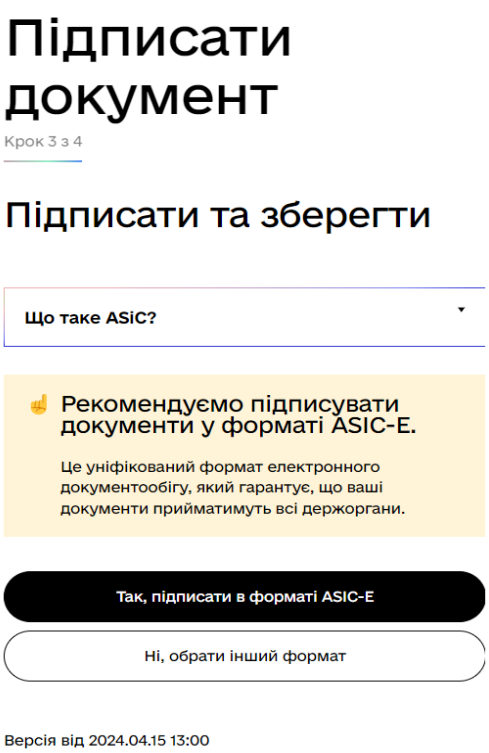
On the Provider’s website, select “Sign the document” using “Diia.Signature-UA” (for signing according to the DSTU algorithm) or “Diia.Signature-EU” (for signing according to the international algorithm):



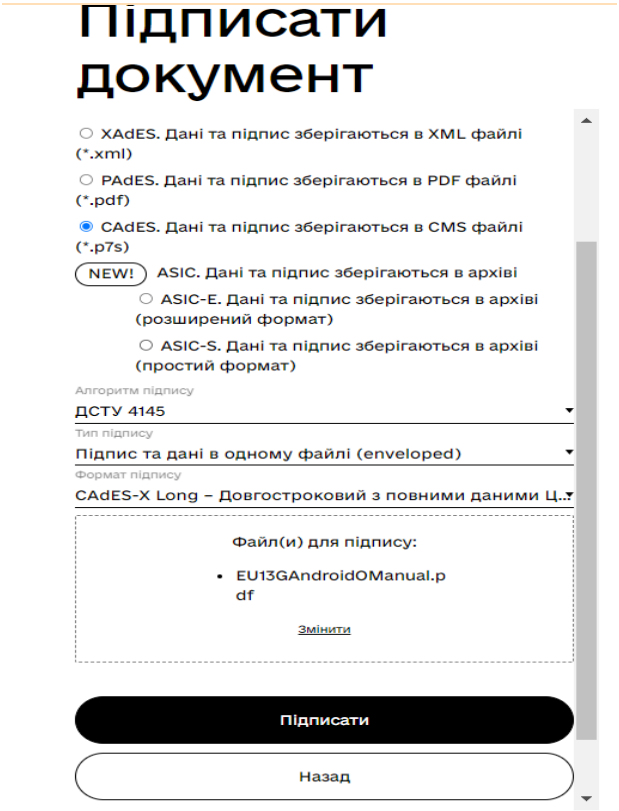
●Open the mobile application “Diia” and scan the QR code on the website with the scanner:

●Confirm the reading request:

●After successfully reading the private key, return to the Provider’s website and select the signature format:



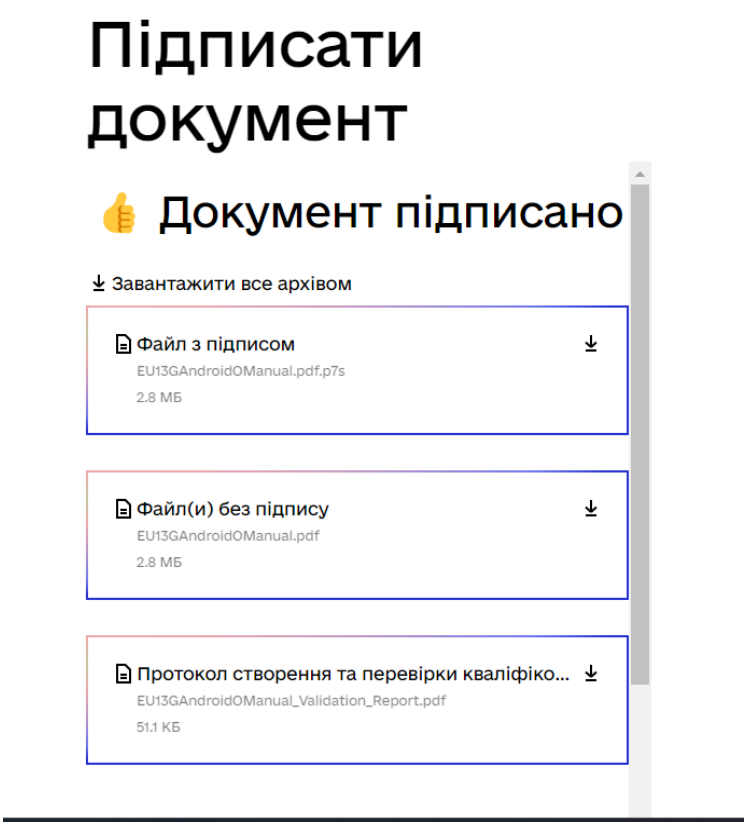
●Select the format, type and algorithm of the electronic signature, the required document to be signed and click “Sign”:



●Go to the mobile application “Diia” and scan the QR code with the scanner:

●After signing documents, the signed file is displayed in the browser, as well as a file without an electronic signature and the protocol for generating an electronic signature, in

which the time stamp and the signatory’s data are indicated. To save these files, click on the arrows and download the required document to your computer:

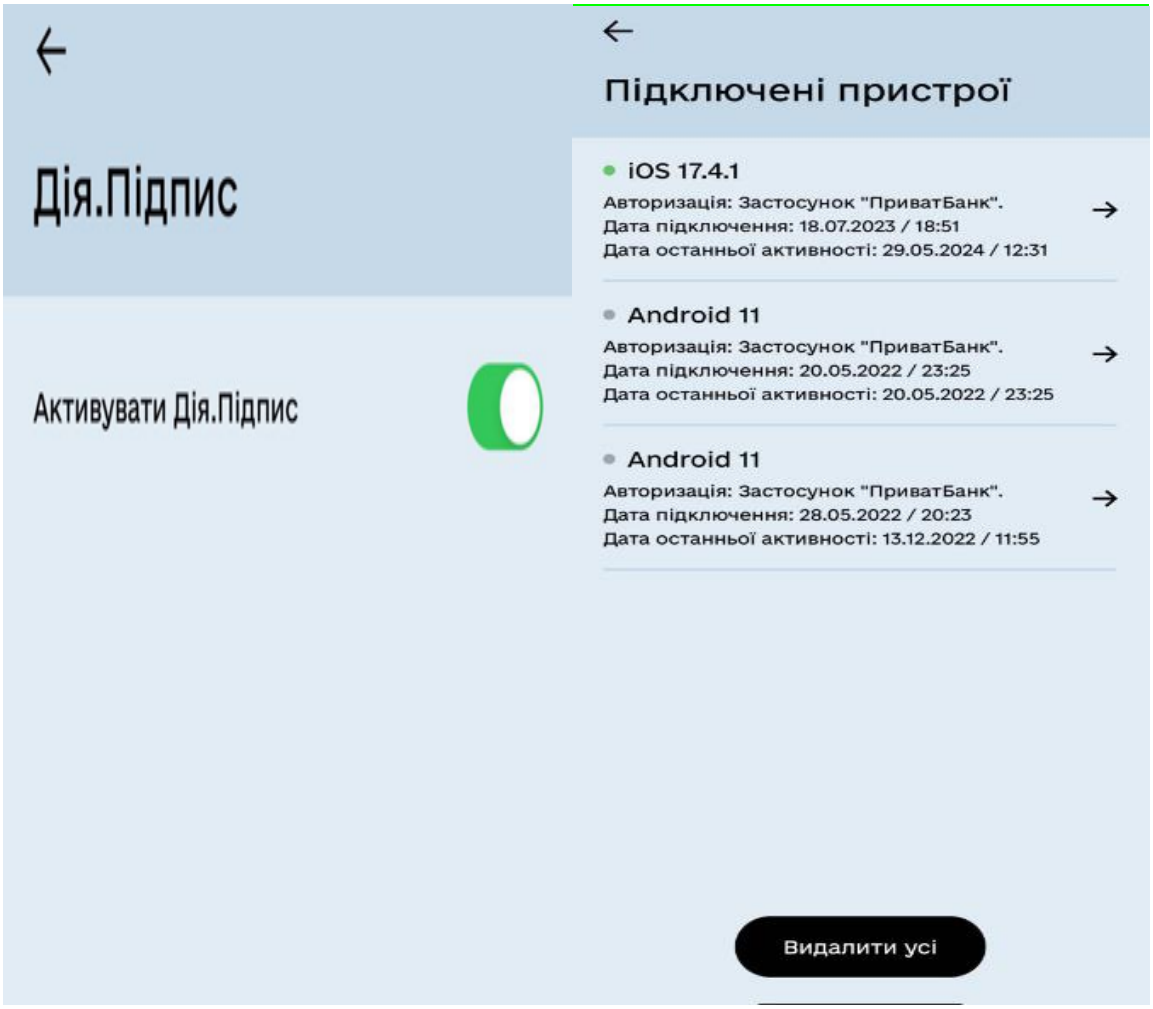


* Signed files using Diia.Signature are not stored in the mobile application “Diia”. Only the signature history is kept in the mobile application “Diia” itself.

This Manual contains a link to a video on how to sign a document with the Diia.Signature https://www.youtube.com/watch?v=txNZx8uqsH8

4.3. Deactivation of a Diia.Signature (Diia ID)

To deactivate Diia.Signature, go to the Menu of the mobile application “Diia”, select “Diia.Signature” and drag the green slider to the left, or select “Delete all” in the “Connected Devices” Menu:



4.4. Generation of a Diia.Signature for E-residents (Diia ID)

Generation of the private key “Diia.Signature” of the E-resident is free of charge using the mobile application “Diia”.

Steps to receive a Diia.Signature:

●applicant is authenticated in the mobile application using a one-time QR code generated by the information system “E-Resident” by scanning it.

●perform step-by-step actions to generate the Diia.Signature stated in the clause 49.1 of this Manual.