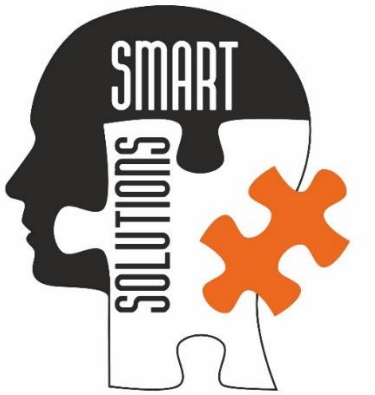


Настанова оператора.

"Модуль клієнтський" зі складу "Комплексу програмного криптографічного захисту інформації "Крипто Автограф 2.0"

Інструкція користувача
Версія 2.3.8/2022

UA.ОВСТ.00002-01 34 01-1

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 4
ВСТУП 5
СКЛАДОВІ КОМПОНЕНТИ ЗАСОБУ 5
МІНІМАЛЬНІ ТЕХНІЧНІ ВИМОГИ 5
СУМІСНІСТЬ З ОПЕРАЦІЙНИМИ СИСТЕМАМИ 5
ВСТАНОВЛЕННЯ КЛІЄНТСЬКОЇ КОМПОНЕТИ ЗАСОБУ 6
ЛІЦЕНЗУВАННЯ КЛІЄНТСЬКОЇ КОМПОНЕНТИ ЗАСОБУ 10
НАЛАШТУВАННЯ КЛІЄНТСЬКОЇ КОМПОНЕНТИ ЗАСОБУ 13
РОБОТА В ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ 18
Перевірка наявності оновлень 18
Підключення особистого ключа 18
Підписання/ шифрування документів 25
Підпис 25
Процес підпису в стандартному форматі «CMS» 26
Процес підпису в форматі CAdES 28
Процес підпису в форматі XAdES 29
Процес підпису в форматі ASiC 29
Шифрування 32
Печатка 35
Перевірка ЕП/ розшифрування 39
Перевірка підпису 39
Розшифрування файлу 41
Перевірка електронної печатки 43
ФОРМУВАННЯ КРИПТОГРАФІЧНИХ КЛЮЧІВ 46
Формування запиту на сертифікат на смарт-карту (USB-токен, ЗНКІ) 46
Формування запиту на сертифікат юридичної особи - підписувача 46
Формування запиту на сертифікат фізичної особи - підписувача 51
Формування запиту на сертифікат фізичної особи-підписувача, що є співробітником юридичної особи, або суб'єктом підприємницької діяльності 57
Формування запиту на сертифікат у файловий носій 63
Формування запиту на сертифікат юридичної особи - підписувача 63
Формування запиту на сертифікат фізичної особи - підписувача 70
Формування запиту на сертифікат фізичної особи-підписувача, що є співробітником юридичної особи, або суб'єктом підприємницької діяльності 77
РОБОТА З ЗНКІ 85

ЗНКІ, що підтримуються Засобом 85
Налаштування електронних ключів «Алмаз-1К» для роботи в Засобі. 86
Налаштування ЗНКІ "Алмаз - 1К" для роботи в Засобі КЗІ Крипто Автограф за умови ВІДСУТНОСТІ ключів на носії 86
Налаштування ЗНКІ "Алмаз - 1К" для роботи в Засобі КЗІ Крипто Автограф за умови НАЯВНОСТІ ключів на носії 90
Налаштування ЗНКІ "Кристал - 1" для роботи в Засобі КЗІ Крипто Автограф за умови ВІДСУТНОСТІ ключів на носії 93
Налаштування ЗНКІ "Кристал - 1" для роботи в Засобі КЗІ Крипто Автограф за умови НАЯВНОСТІ ключів на носії 96
СЕРТИФІКАТИ 100
Імпорт сертифікатів 100
Перегляд сертифікатів 104
Автоматичне завантаження кореневих сертифікатів КНЕДП 111
ЗМІНА ПАРОЛЮ 111
ДОВІДКА 113
Версія Засобу 113
Допомога 113
ПРОТОКОЛЮВАННЯ ПОДІЙ КЛІЄНТСЬКОЇ КОМПОНЕНТИ ЗАСОБУ 113
КОНФІГУРАЦІЯ ЗАСОБУ 116
ЗАВЕРШЕННЯ РОБОТИ 119

ПЕРЕЛІК СКОРОЧЕНЬ

ЕП	Електронний підпис чи електронна печатка
КЕП	Кваліфікований електронний підпис
УЕП	Удосконалений електронний підпис
ОС	Операційна система
КНЕДП	Кваліфікований надавач електронних довірчих послуг
TSP	Time stamp protocol
OCSP	Online certificate status protocol
CMP	Certificate management protocol
HTTP	Hypertext transfer protocol
HTTPS	Hypertext transfer protocol secure
WSS	Web Socket Secure
p7s	Розширення файлу, який підписано за допомогою ЕП
p7e	Розширення зашифрованого файлу
ДРФО	Державний реєстр фізичних осіб
УНЗР	Унікальний номер запису в реєстрі
ЄДРПОУ	Єдиний державний реєстр підприємств та організацій України
ЗНКІ	Захищений носій ключової інформації (особистого ключа); смарт-карта; USB-токен
ПЗ	Програмне забезпечення
API	Прикладний програмний інтерфейс

ВСТУП

«Модуль клієнтський» зі складу «Комплексу програмного криптографічного захисту інформації «Крипто Автограф 2.0» (далі – Засіб, Крипто Автограф) призначений для гарантування авторства та захисту цілісності файлів (даних) будь-якого формату шляхом використання електронного підпису (далі – підпис, ЕП) та шифрування.

Документ описує дії користувача, щодо одного модуля Засобу.

Даний документ містить опис послідовності дій користувача щодо встановлення, налаштування та використання «Модуля клієнтського» зі складу «Комплексу програмного криптографічного захисту інформації «Крипто Автограф 2.0».

СКЛАДОВІ КОМПОНЕНТИ ЗАСОБУ

Засіб складається з наступних компонентів:

- ✓ Клієнтська складова;
- ✓ Серверна складова.

МІНІМАЛЬНІ ТЕХНІЧНІ ВИМОГИ

Центральний процесор: Intel® / AMD® 1200 Mhz

Графічний адаптер: в наявності

Оперативна пам'ять: 4096 Mb

Вільне місце на жорсткому диску: 300 Mb

Мережева карта: 100 Мбіт/с

Примітка: Зазначені технічні вимоги є мінімально необхідними для функціонування програмного забезпечення. Розмір вільного місця може збільшуватися в залежності від кількості сертифікатів та списків відкликаних сертифікатів, необхідних для коректного функціонування Засобу.

СУМІСНІСТЬ З ОПЕРАЦІЙНИМИ СИСТЕМАМИ

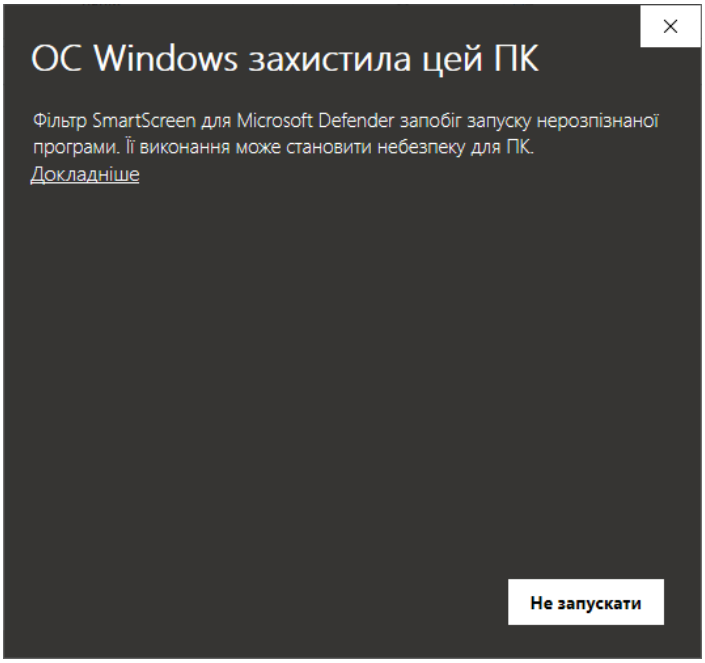
Клієнт:

32- бітні ОС: Microsoft® Windows® 7/8/2008/10/11

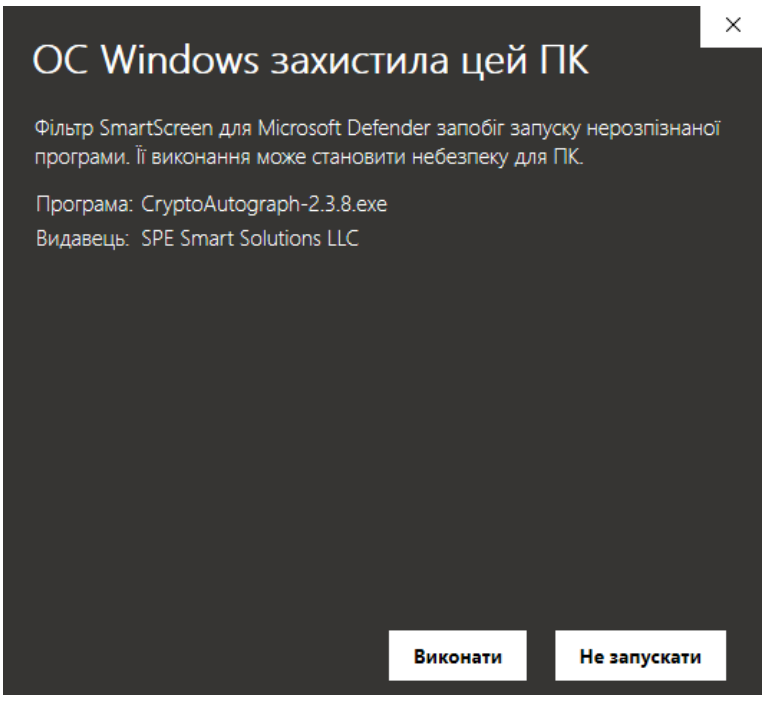
64-бітні ОС: Microsoft® Windows® 7/8/2008 R2/2012/2012 R2/10/11

ВСТАНОВЛЕННЯ КЛІЄНТСЬКОЇ КОМПОНЕТИ ЗАСОБУ

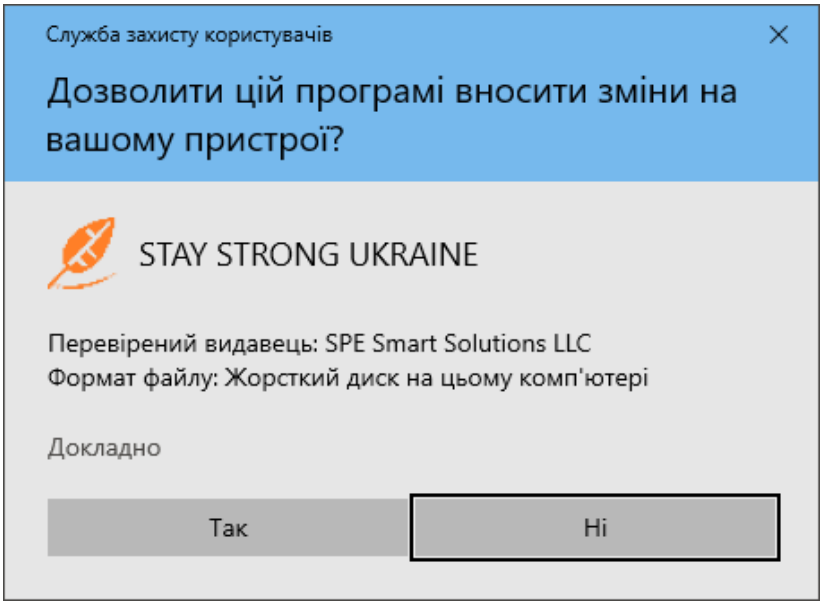
Для встановлення клієнтського модуля необхідно запустити виконуючий файл CryptoAutograph-2.3.8.exe через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої кнопки миші. Після запуску на екрані може з’явитись вікно антивірусу Microsoft Defender, натисніть «Докладніше» для продовження процесу інсталяції.



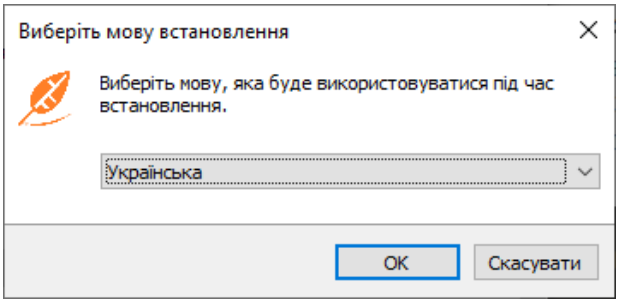
Натисніть «Виконати».



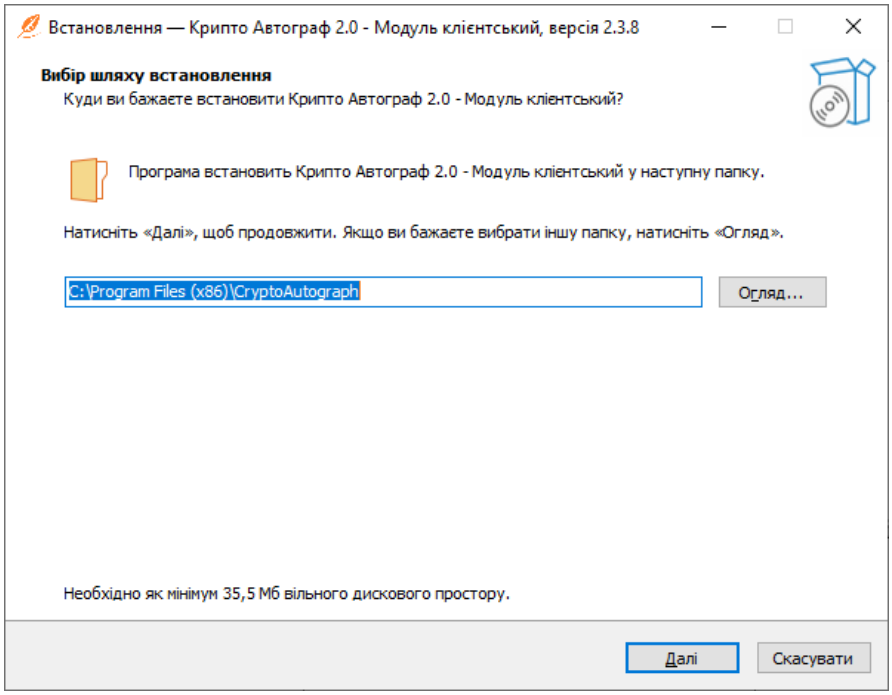
Натисніть «Так» для продовження інсталяції Засобу.



Далі з’явиться вікно вибору мови, яка буде використовуватися під час процесу інсталяції. Оберіть мову та натисніть «ОК».

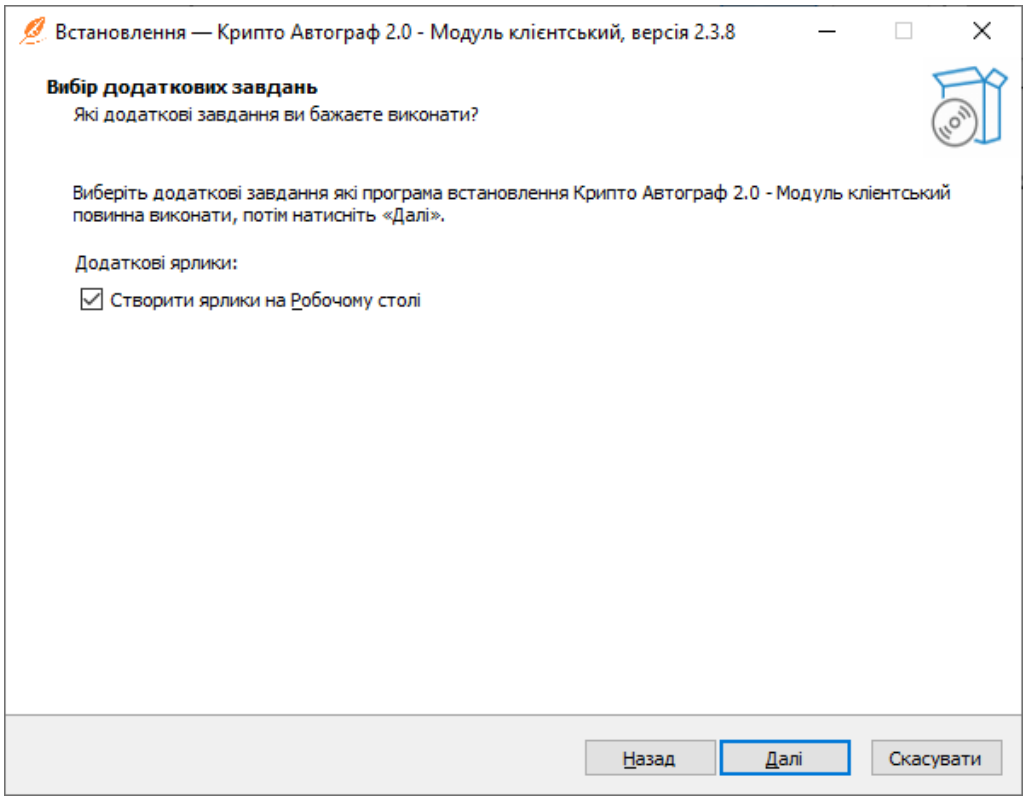


Далі з’явиться вікно встановлення програмного забезпечення, у якому можна обрати каталог для встановлення програмного забезпечення, яке буде мати наступний вигляд:

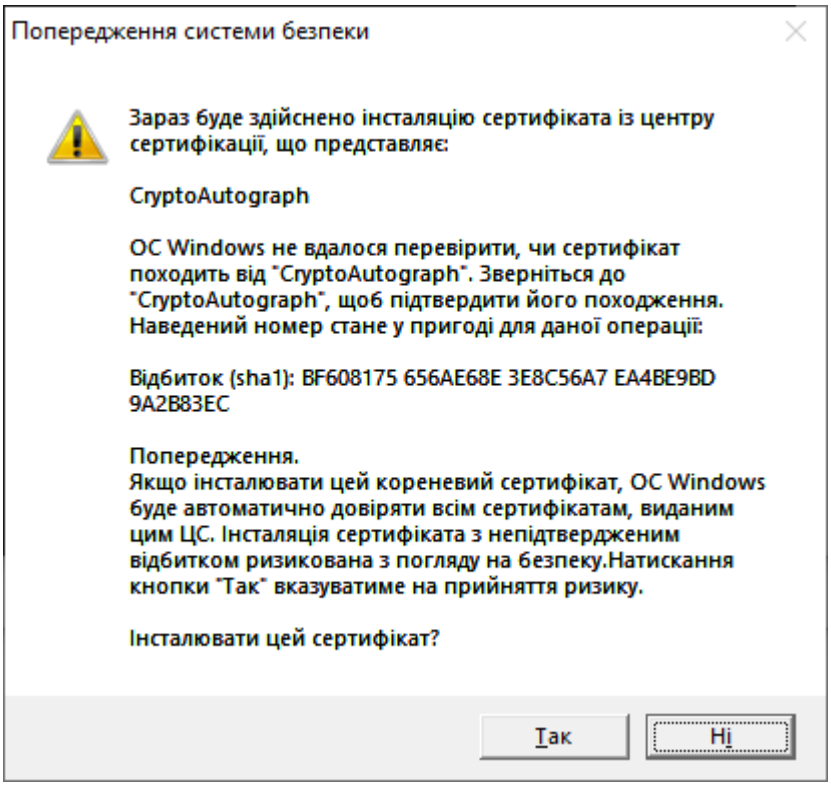


Рекомендуємо залишити налаштування за замовчуванням. Натисніть «Далі» для продовження процесу інсталяції, «Огляд…» - для зміни каталогу для встановлення, «Скасувати» - для припинення процесу інсталяції.

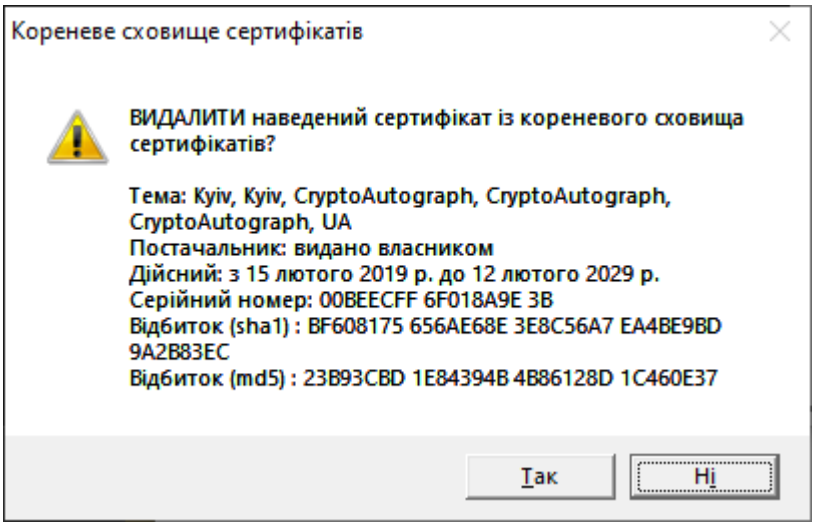
У наступному вікні встановіть позначку, якщо бажаєте створити ярлик на робочому столі Вашої операційної системи. Для продовження процесу інсталяції натисніть «Далі».



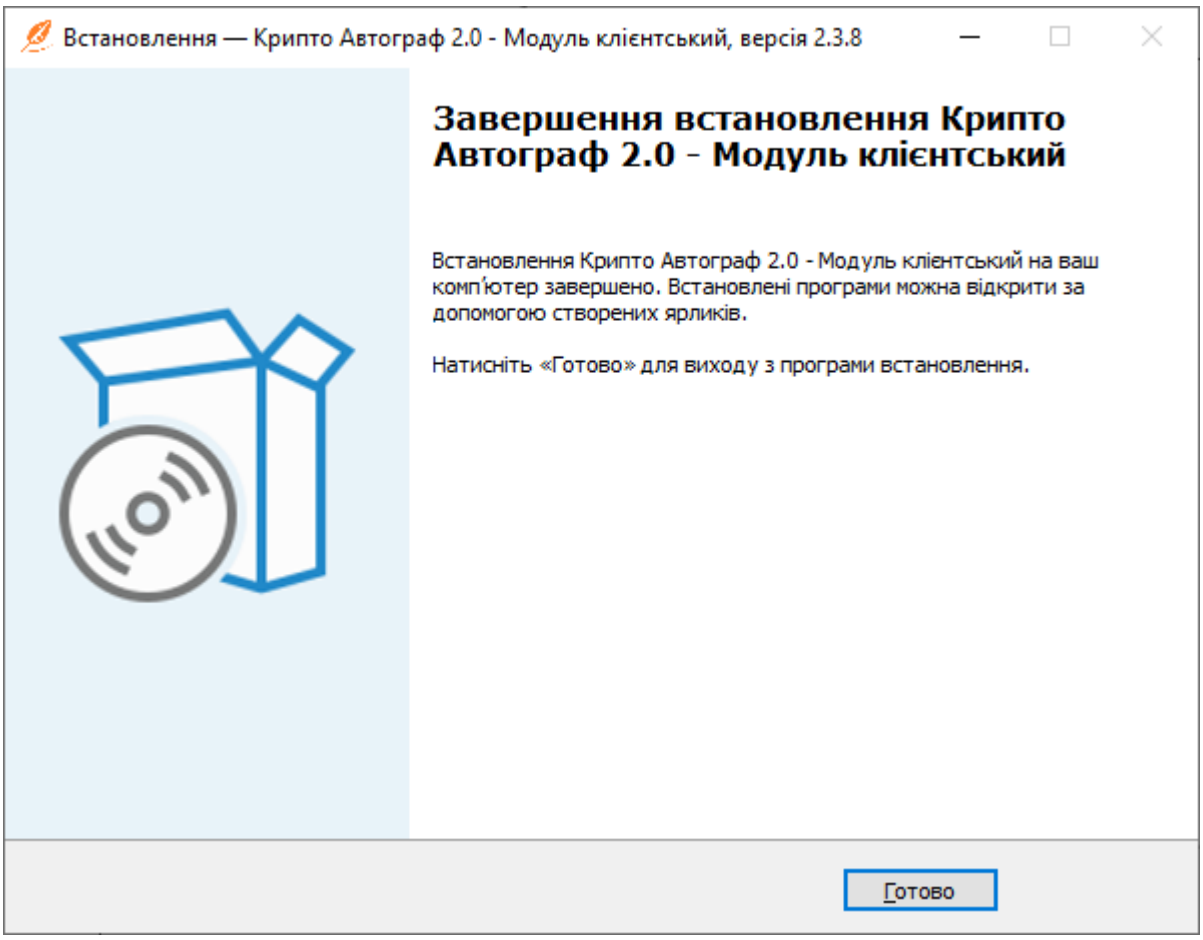
У вікні, що з’явиться в процесі інсталяції, та зображено нижче, натисніть «Так». Це дозволить встановити сертифікат необхідний для роботи веб-модуля Засобу у захищеному режимі.



Якщо на Вашому комп’ютері вже попередньо було встановлено іншу версію Крипто Автографа – це значить, що вказаний сертифікат вже присутній, в такому випадку програма інсталяції запропонує видалити його. Натисніть «Ні».



Дочекайтеся завершення встановлення програмного забезпечення та натисніть кнопку «Готово».



ЛІЦЕНЗУВАННЯ КЛІЄНТСЬКОЇ КОМПОНЕНТИ ЗАСОБУ

Отриманий за договором (на диску або електронною поштою) електронний файл ліцензії license.dat скопіюйте до каталогу в який було встановлено Засіб.

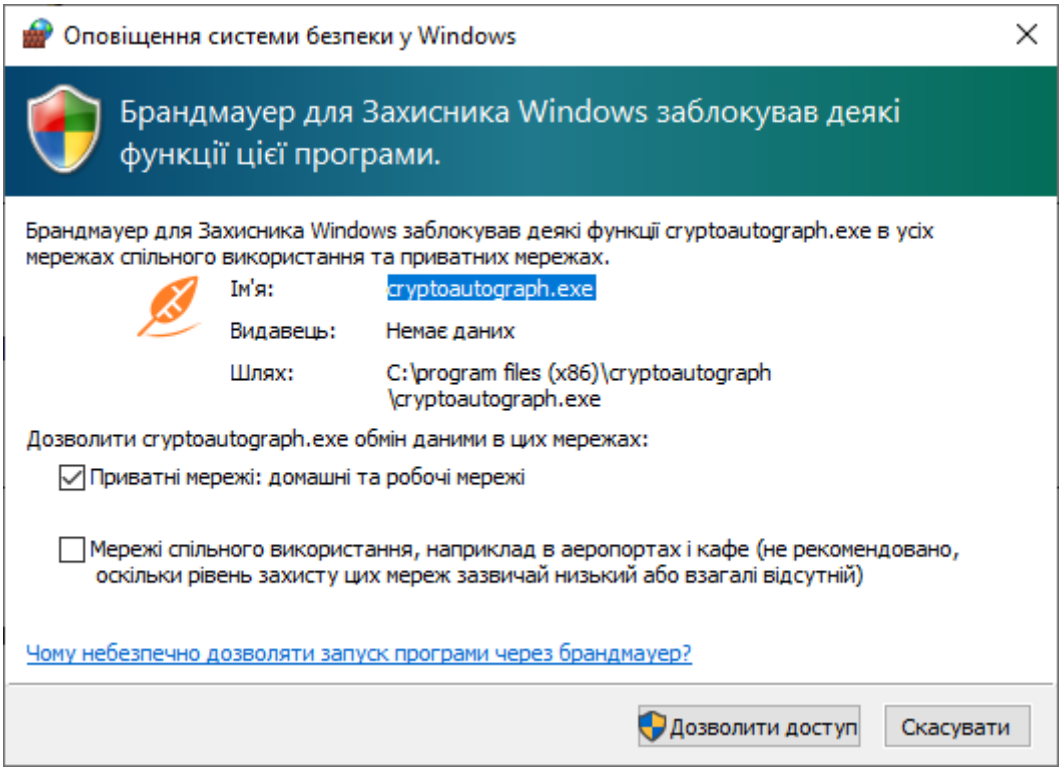
За замовчуванням це каталог:

C:\My Crt

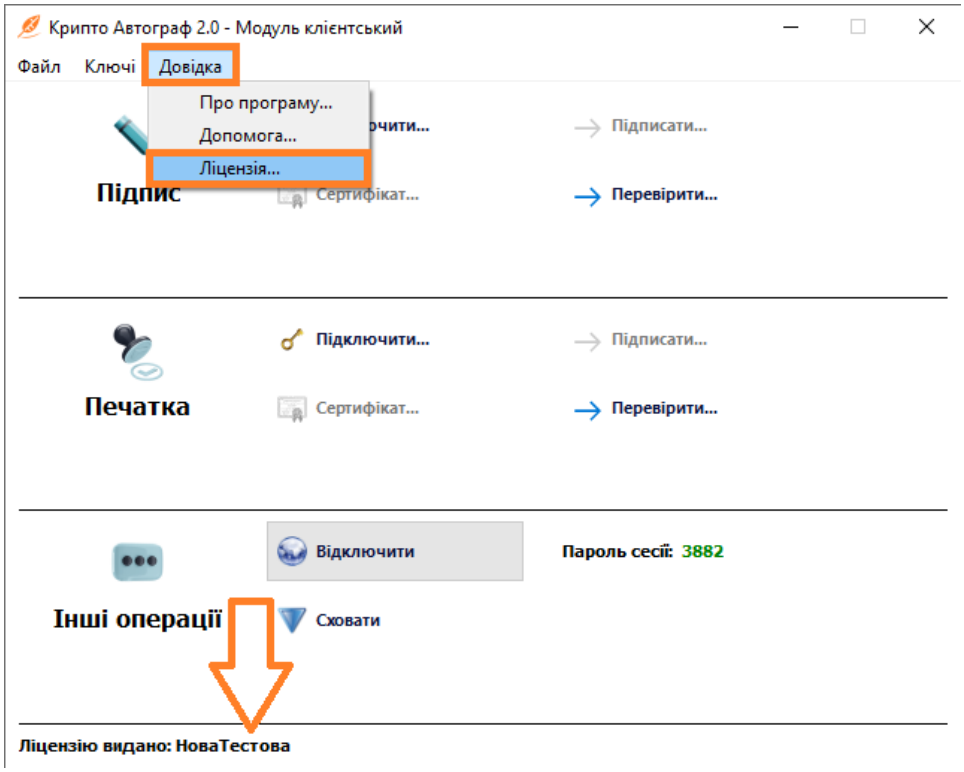
За результатом копіювання електронний файл ліцензії повинен бути розміщений за посиланням:

C:\My Crt\license.dat.

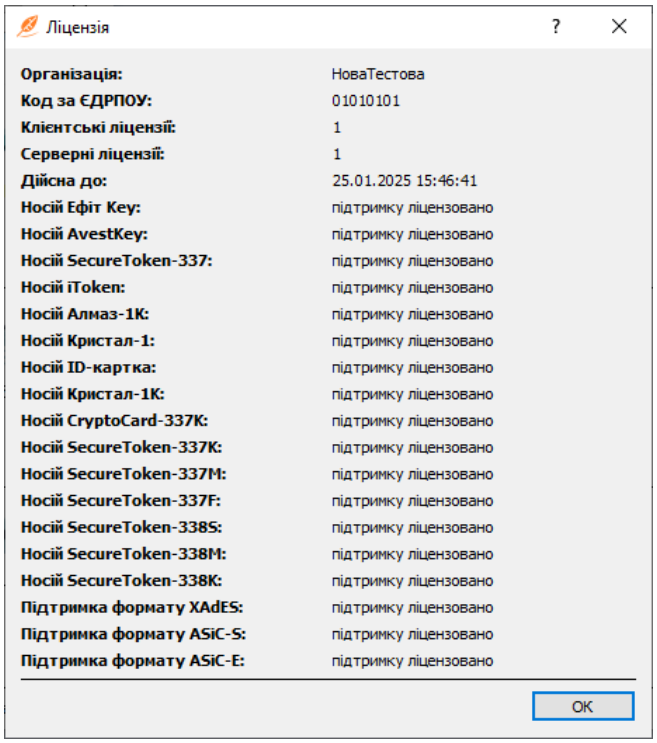
При першому запуску Засобу з’явиться вікно брандмауера операційної системи, що зображено нижче. Натисніть «Дозволити доступ». Це необхідно для створення певних правил для роботи Засобу у мережі Інтернет.



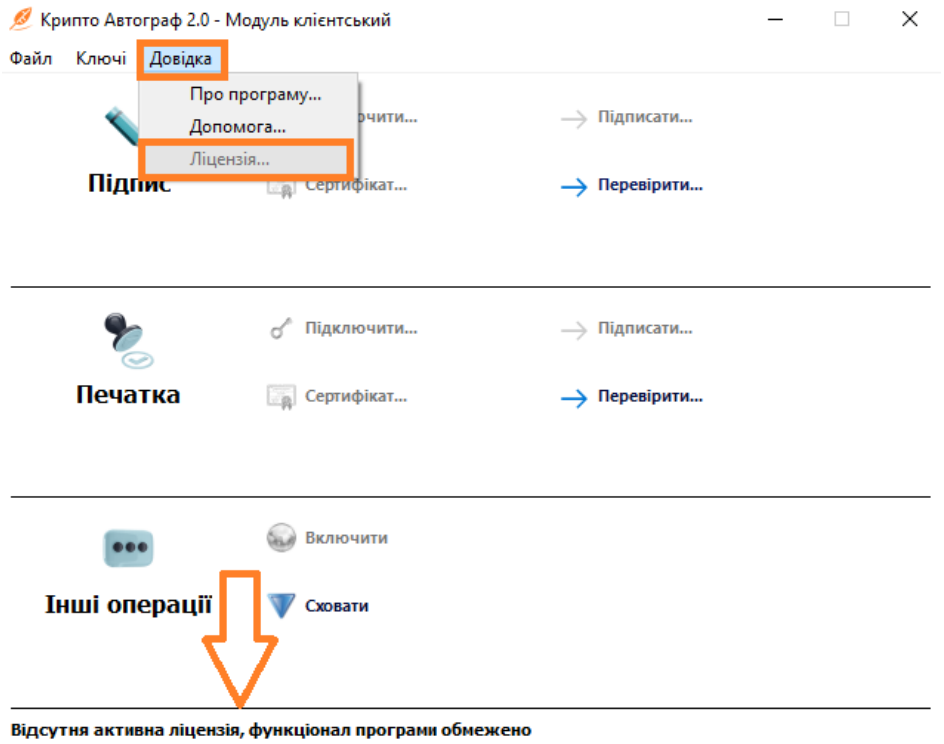
Для перевірки коректності встановлення ліцензії запустіть Засіб через ярлик «Крипто Автограф 2.0 - Модуль клієнтський» на «Робочому столі» або меню «Пуск», в нижній частині вікна зверніть увагу на текст: «Ліцензію видано». Для детального перегляду інформації про видану ліцензію оберіть в графічному інтерфейсі «Довідка» → «Ліцензія…».



Відображення інформації про вміст «електронного файлу ліцензії» свідчить про успішне встановлення Вами ліцензії на Засіб.

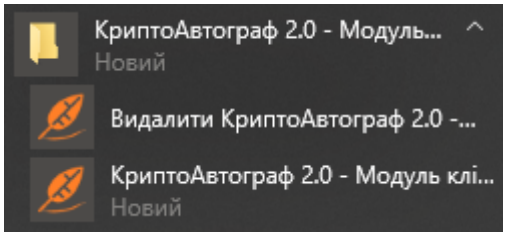


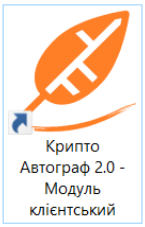
Примітка: У разі відсутності файлу-ліцензії або прострочення терміну її дії вікно програмного забезпечення має наступний вигляд. У такому випадку буде доступним лише функціонал перевірки електронного підпису.



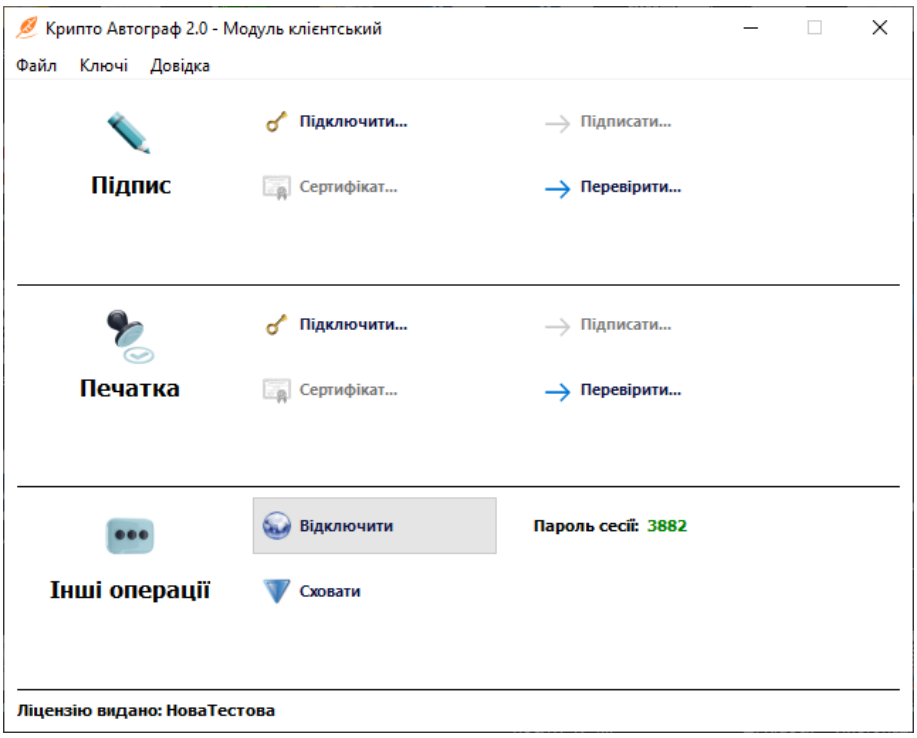
НАЛАШТУВАННЯ КЛІЄНТСЬКОЇ КОМПОНЕНТИ ЗАСОБУ

На «Робочому столі» ОС та в меню «Пуск» доступний ярлик для запуску встановленого програмного забезпечення та здійснення подальшого налаштування Засобу.

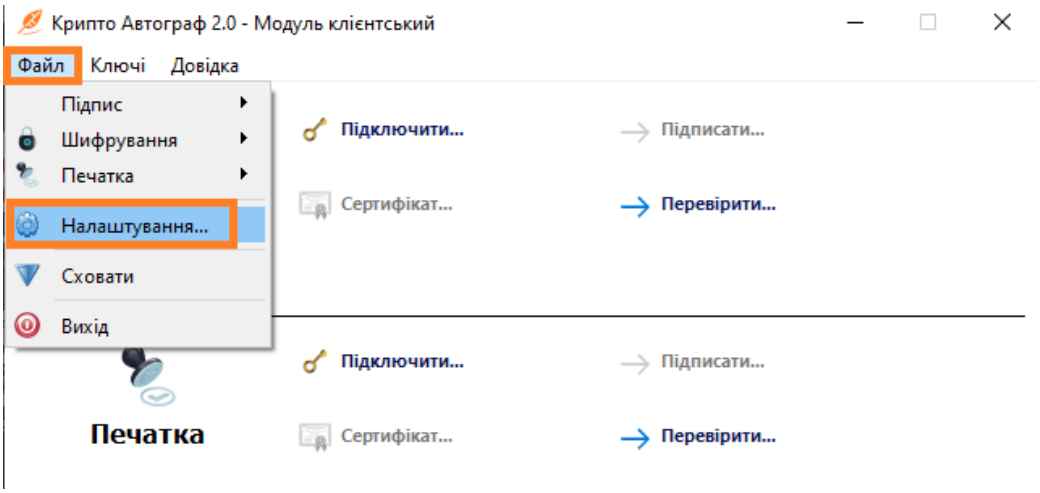


або


Запустивши Засіб відкриється вікно, що наведено нижче.



Для здійснення первинних налаштувань необхідно у горизонтальному меню обрати «Файл» → «Налаштування».



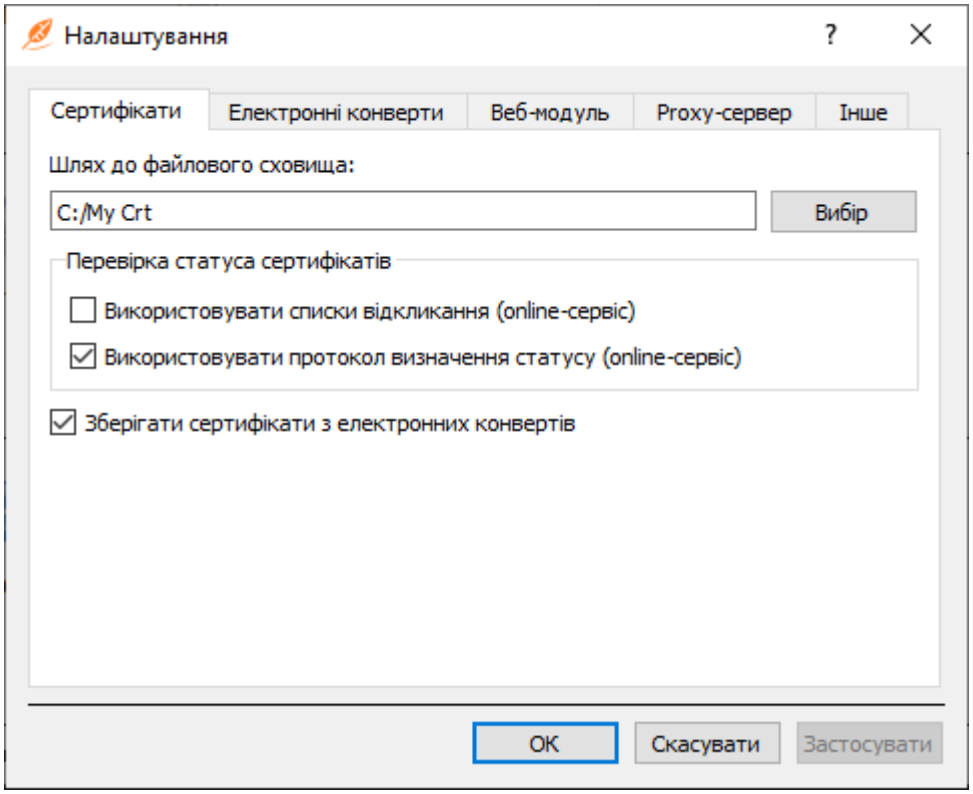
На вкладці налаштувань «Сертифікати» можна обрати каталог, в якому знаходяться сертифікати (користувацькі та кореневі сертифікати КНЕДП) необхідні для роботи Засобу. Рекомендується залишити це налаштування за замовчуванням. Для зміни каталогу натисніть «Вибір» та оберіть новий каталог.

Нижче, у блоці налаштувань «Перевірка статуса сертифікатів», можна обрати вид перевірки статусу сертифіката:

- перевірка у списку відкликаних сертифікатів;
- перевірка за допомогою протоколу визначення статусу сертифіката (OCSP).

Обидва види перевірки потребують підключення до мережі Інтернет.

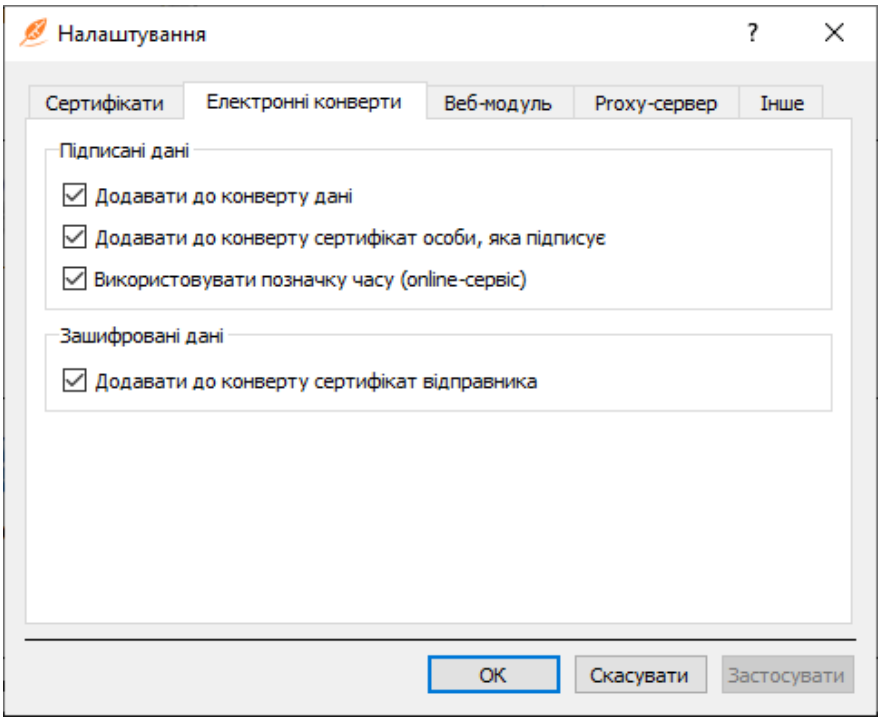
Нижче можна обрати збереження сертифікатів користувачів, які знаходяться в електронних конвертах. Під час перевірки підпису чи розшифруванні електронного конверту, всередині може знаходитися сертифікат підписанта. Для зручності можна зберегти цей сертифікат в каталозі.



На вкладці налаштувань «Електронні конверти» можна налаштувати роботу Засобу під час накладання підпису або шифрування даних. В розділі «Підписані дані» є наступні налаштування:

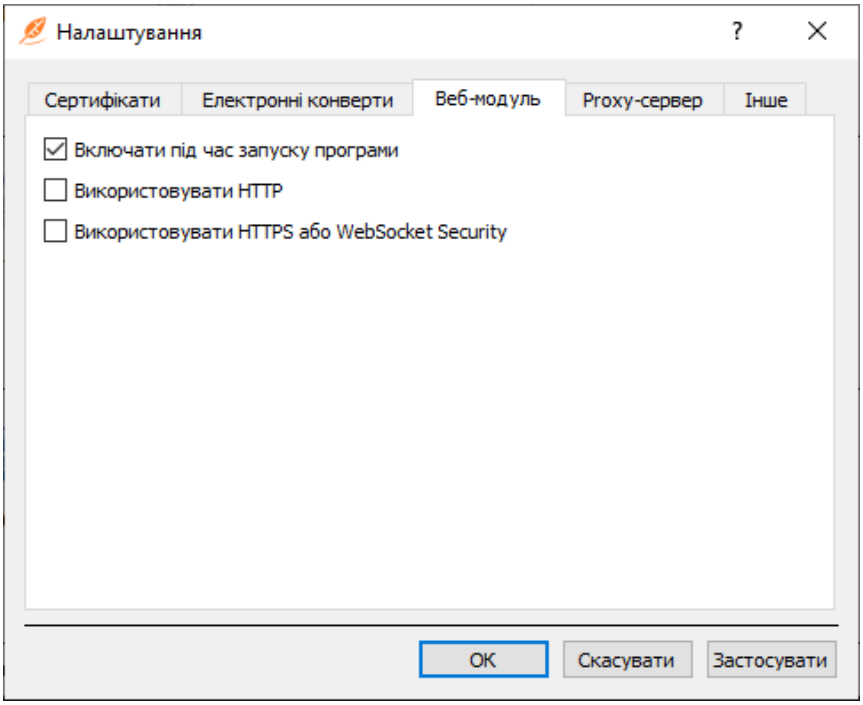
- «Додавати до конверту дані» - файл, що підписується, додається до електронного конверту формату .p7s
- «Додавати до конверту сертифікат особи, яка підписує» - сертифікат користувача, який підписує дані, додається до електронного конверту формату .p7s
- «Використовувати позначку часу» - під час підписання до конверту додається позначка часу, яка в свою чергу отримується від КНЕДП по протоколу TSP (потребує підключення до мережі Інтернет).

В розділі «Зашифровані дані» доступне налаштування «Додавати до конверту сертифікат відправника» - сертифікат користувача, який шифрує дані додається до електронного конверту формату .p7e.

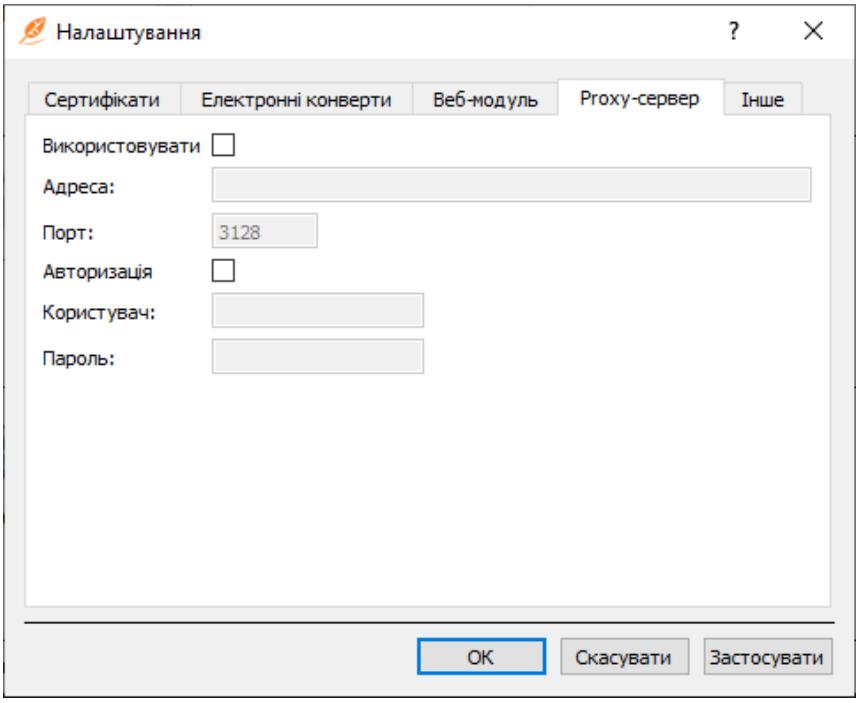


На вкладці налаштувань «Веб-модуль» доступні налаштування:

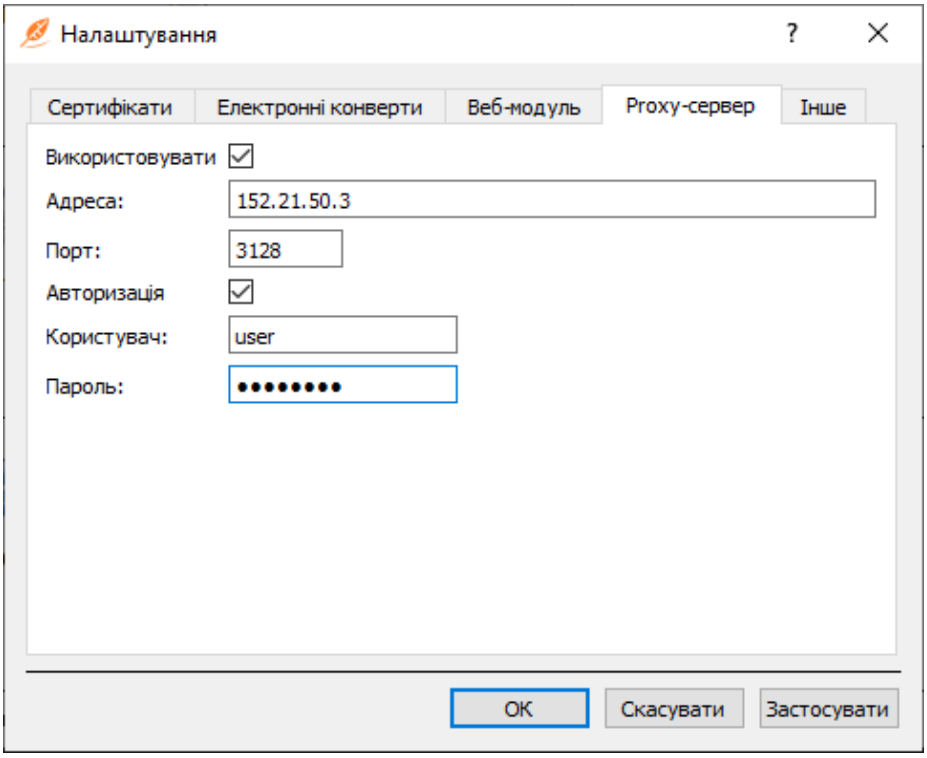
- «Включати під час запуску програми» - веб-модуль буде доступний одразу після запуску програмного забезпечення;
- «Використовувати HTTP» - для підключень по протоколу HTTP;
- «Використовувати HTTPS або WebSocket Security» - для підключень по протоколу HTTPS або WebSocket Security



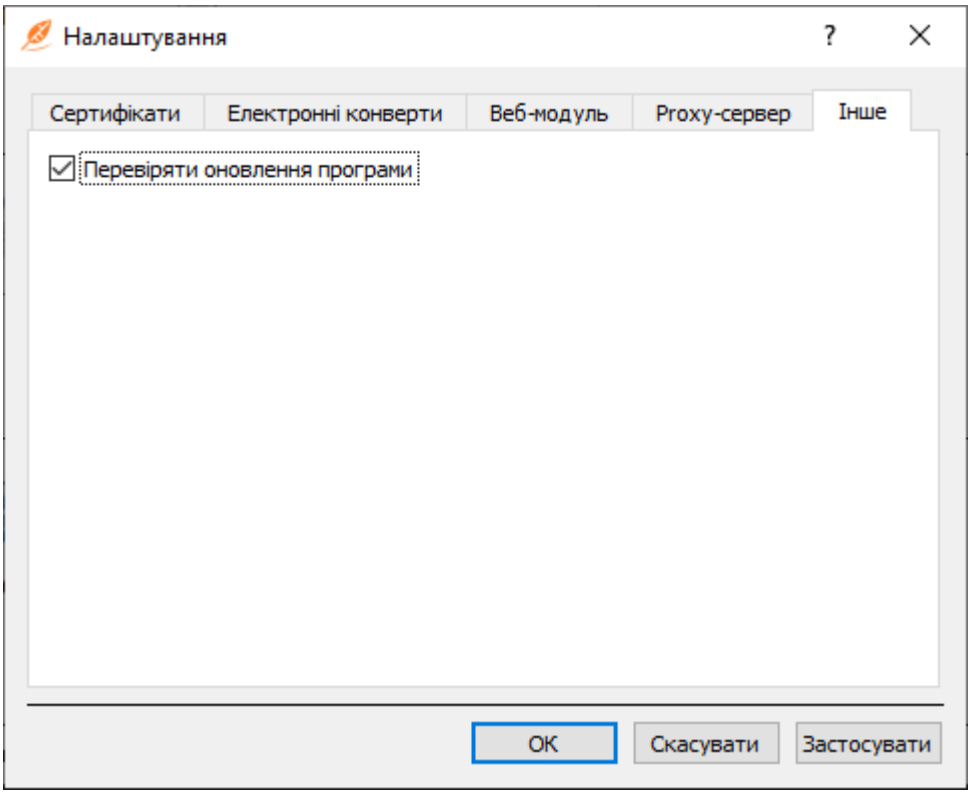
На вкладці налаштувань «Proxy-сервер» доступні налаштування для тих випадків, коли підключення до мережі здійснюється через проміжний проксі-сервер.



Для налаштування підключення через проксі-сервер поставте позначку «Використовувати», нижче в поле «Адреса» введіть IP-адресу проксі-сервера, нижче в поле «Порт» введіть порт на якому працює проксі-сервер (за замовчуванням всі проксі-сервери працюють на порті 3128). Якщо проксі-сервер вимагає авторизації – поставте відповідну позначку, та введіть авторизаційні дані: логін та пароль.



На вкладці налаштувань «Інше» доступне налаштування перевірки наявності оновлень Засобу. Встановіть позначку «Перевіряти оновлення програми» якщо бажаєте здійснювати відповідну перевірку під час запуску Засобу.

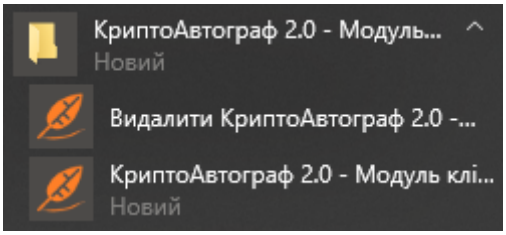


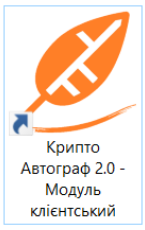
Після здійснення необхідних налаштувань потрібно натиснути кнопку «Застосувати» та кнопку «Ок».

РОБОТА В ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ

На «Робочому столі» операційної системи та в меню «Пуск» доступний ярлик для запуску встановленого програмного забезпечення.

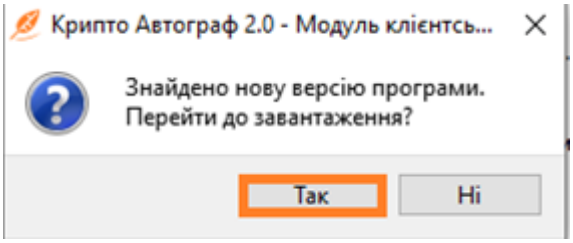
Запустіть програмне забезпечення використовуючи ярлик «Крипто Автограф 2.0 - Модуль клієнтський».



або


Перевірка наявності оновлень

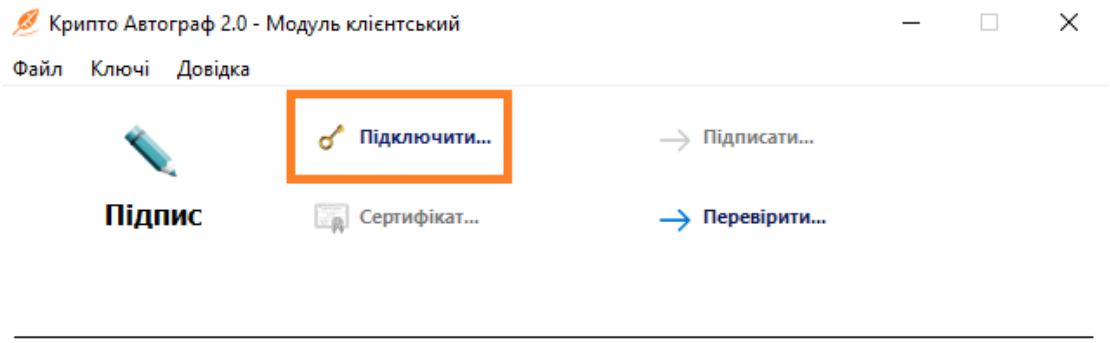
У випадку коли у налаштуваннях було поставлено позначку «Перевіряти оновлення програми», під час запуску Засобу, здійснюється перевірка наявності нової версії на сервері. Якщо під час такої перевірки буде виявлено оновлення Засобу – він запропонує завантажити його.



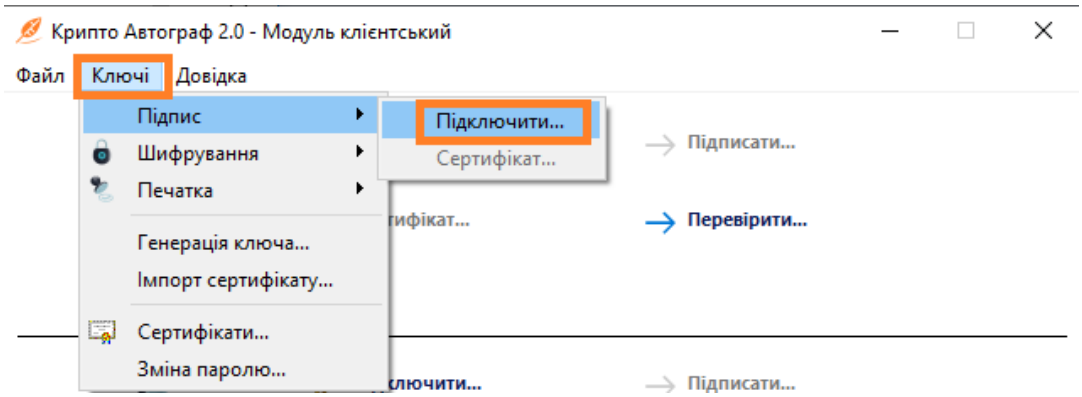
Натисніть «Так» якщо бажаєте завантажити нову версію. Після натискання відкриється вікно Вашого веб-переглядача за замовчуванням та буде здійснено завантаження виконуючого файлу. Зверніть увагу, що для оновлення до нової версії необхідно закрити Засіб, видалити поточну версію (за допомогою інструментів операційної системи або файлу uninstall.exe, що розташований в каталозі C:\Program Files (x86)\CryptoAutograph) та встановити нову версію згідно з даною інструкцією. Якщо Ви не бажаєте здійснювати завантаження нової версії – натисніть «Ні»

Підключення особистого ключа

У графічному інтерфейсі програмного забезпечення натисніть кнопку «Підключити» в розділі «Підпис» (для підключення особистого ключа електронного підпису) або оберіть пункт «Ключі» горизонтального меню, далі «Підпис», потім «Підключити» (зображено на наступній сторінці).

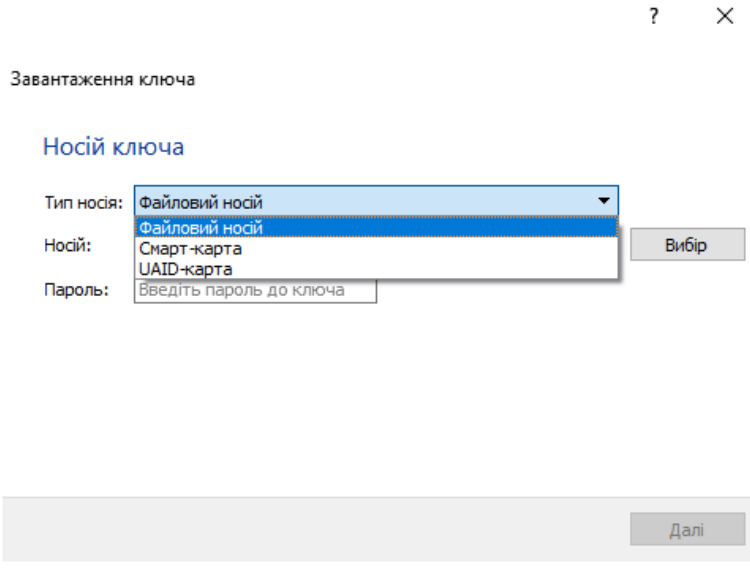


За аналогією можна підключити ключ шифрування і електронну печатку у розділах графічного меню «Шифрування» і «Печатка» відповідно, або в пункті «Ключі» горизонтального меню, далі «Шифрування»- «Підключити» і «Печатка»- «Підключити», відповідно.



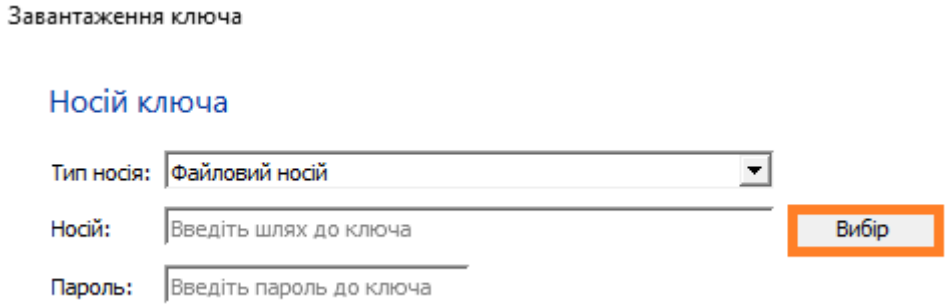
У вікні «Завантаження ключа» оберіть тип носія з випадаючого списку. Доступні варіанти:

- Файловий носій;
- Смарт-карта (USB-токен);
- UAID-карта (паспорт громадянина України).

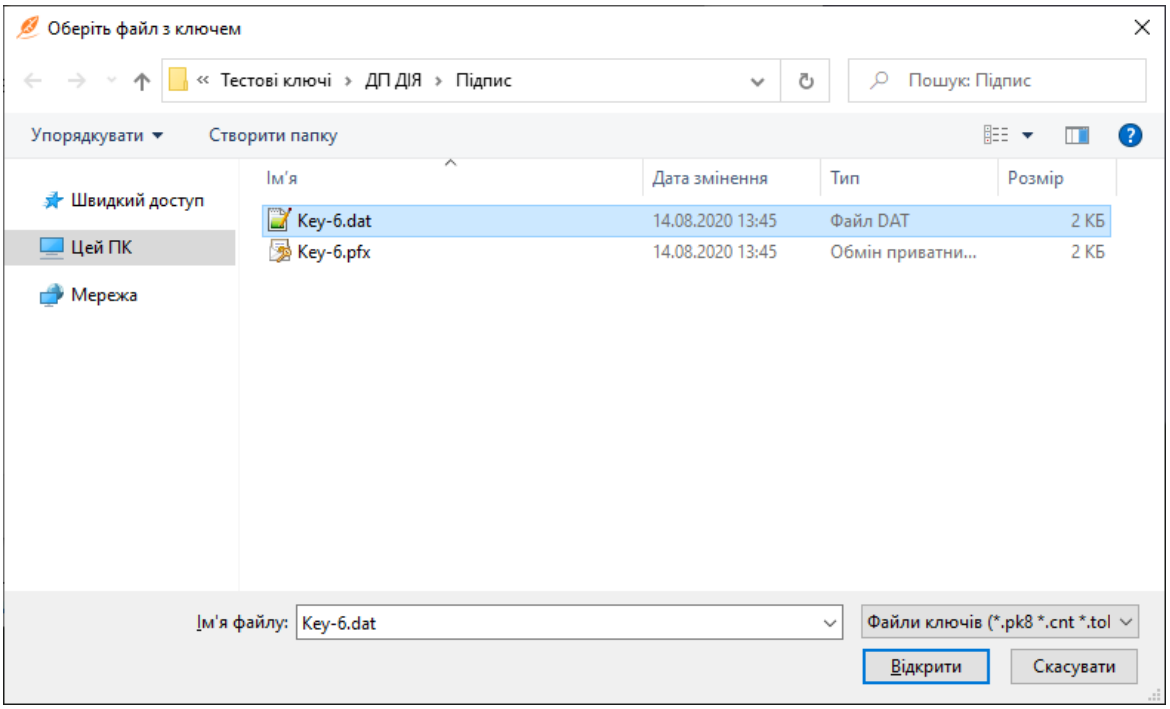


Нижче зображено процедуру підключення ключа УЕП з файлового носія.

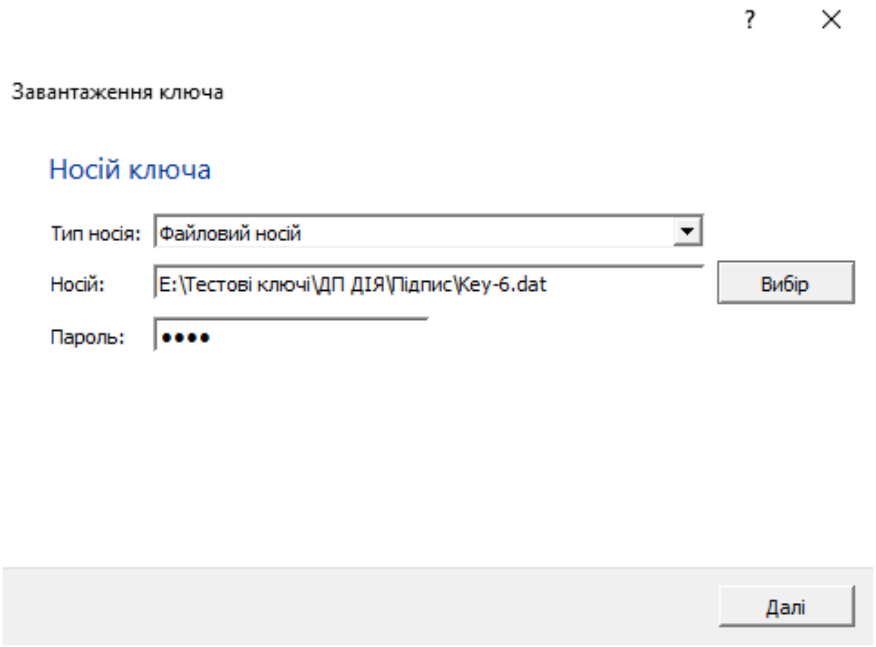
Натисніть кнопку «Вибір» та вкажіть шлях до каталогу в якому знаходиться файл ключа.



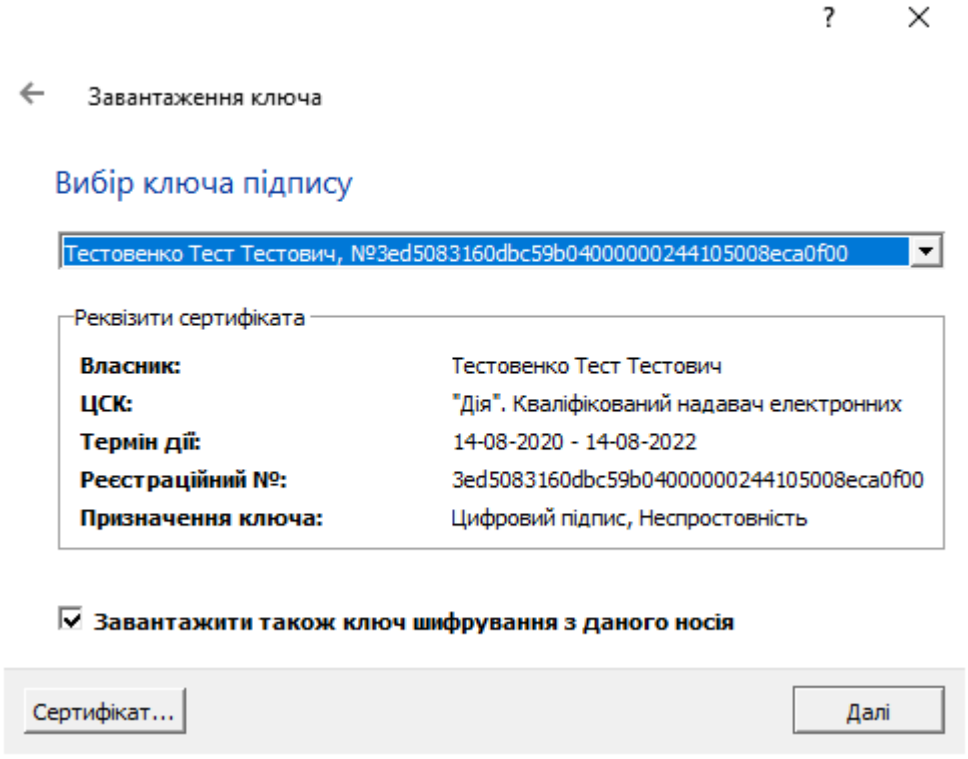
Оберіть Ваш особистий ключ ЕП та натисніть кнопку «Відкрити».

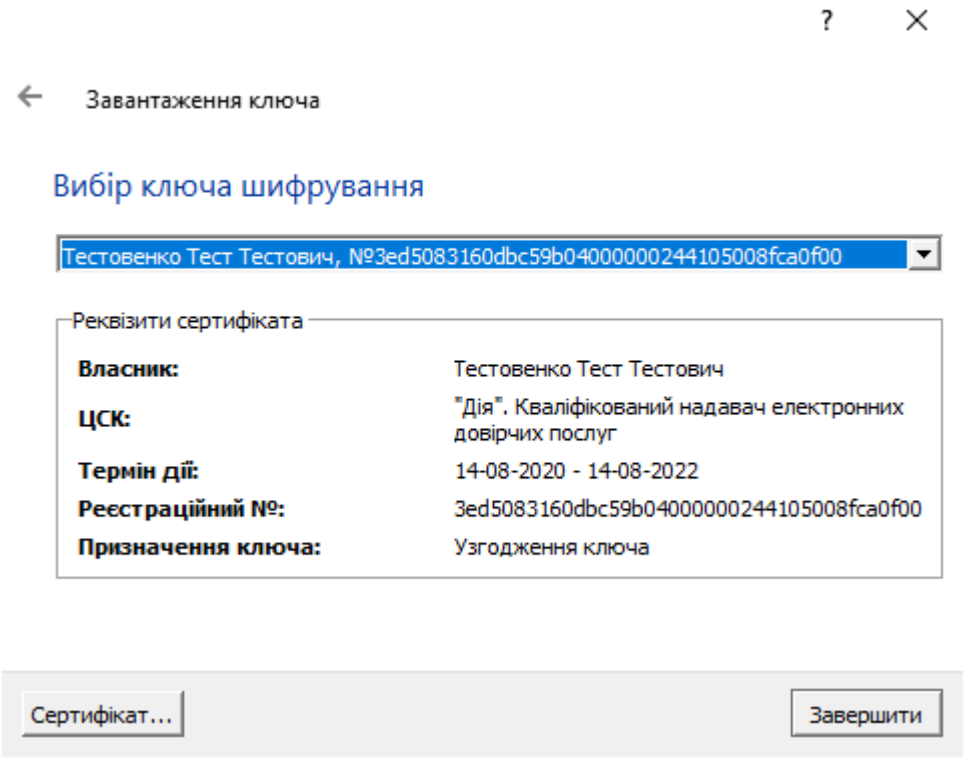


Після обрання файлу, що містить особистий ключ електронного підпису необхідно у полі «Пароль:» зазначити Ваш пароль доступу до особистого ключ ЕП та натиснути кнопку «Далі».

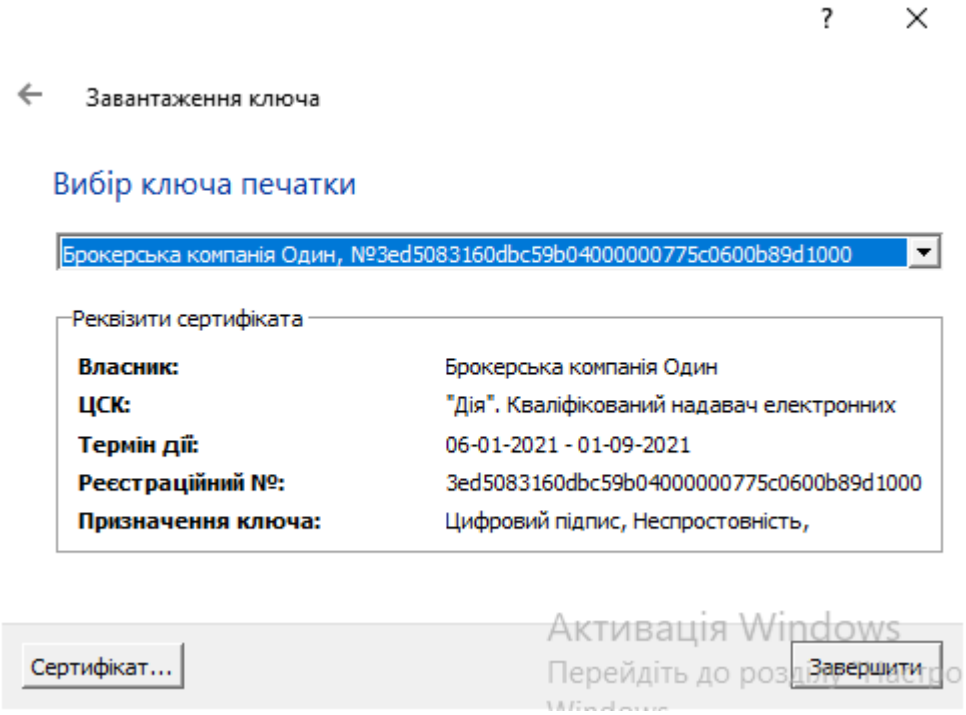


Якщо Ви попередньо генерували окремі ключ для підпису і шифрування, у Вас почергово відкриється два вікна. Перше про ключ підпису, друге про ключ шифрування. (як зображено на наступних двух рисунках)





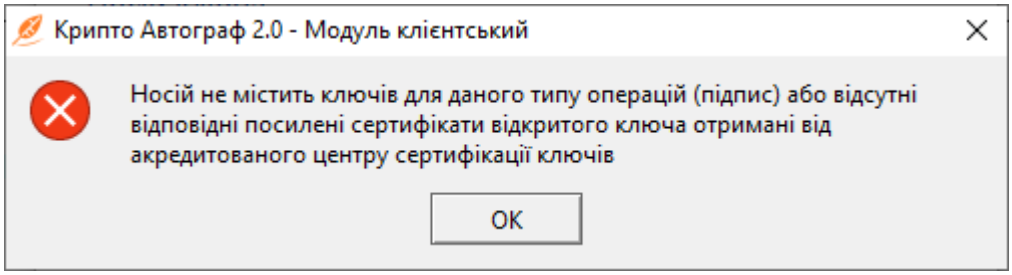
Нижче зображено завантаження ключа електронної печатки.



Якщо в результаті підключення Ви отримали помилку зображену нижче:

- для ключів на файловому носієві (УЕП) – скопіюйте сертифікати користувача та сертифікати КНЕДП до каталогу, вказаного у налаштуваннях, у пункті «Шлях до файлового сховища». За замовчуванням C:/My Crt

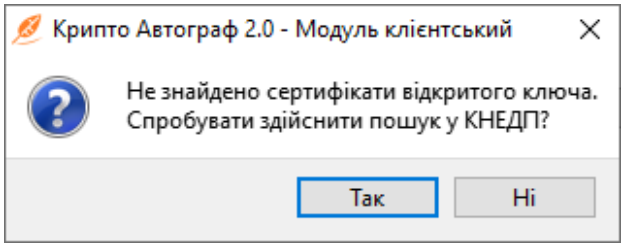
- для ключів на смарт-карті або USB-токені (КЕП) – перейдіть в розділ Імпорт сертифікатів.



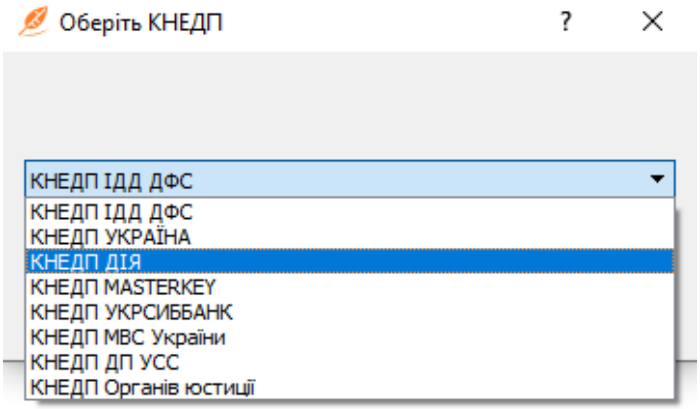
У тому випадку, якщо Ви отримали ключі в одному з КНЕДП з нижченаведеного переліку, є можливість завантажити сертифікати користувача автоматично за допомогою серверу CMP.

- КНЕДП ІДД ДПС;
- КНЕДП ЦСК Україна;
- КНЕДП ДІЯ;
- КНЕДП MASTERKEY;
- КНЕДП УКРСИББАНК;
- КНЕДП МВС України;
- КНЕДП ДП УСС;
- КНЕДП Органів юстиції.

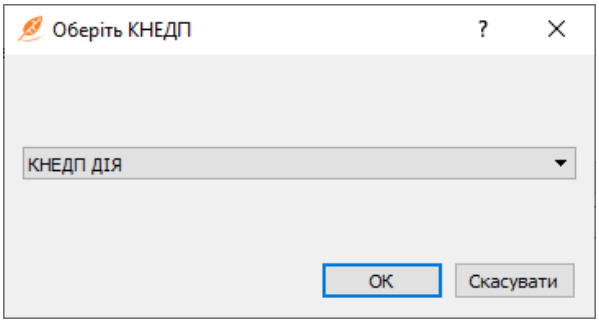
У разі відсутності сертифікатів користувача в каталозі C:/My Crt, після введення паролю до ключа, з’явиться вікно, що зображено нижче.



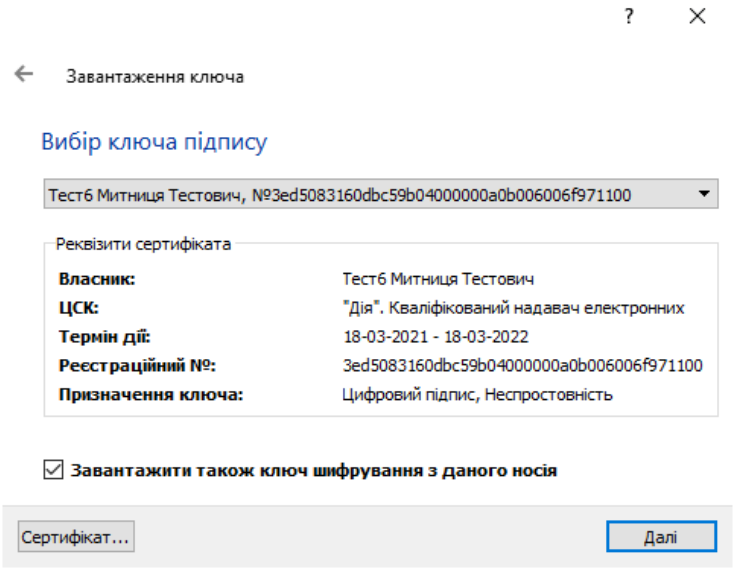
Натисніть «Так» для пошуку Ваших сертифікатів. Далі оберіть з випадаючого списку КНЕДП, в якому Ви отримали сертифікати.



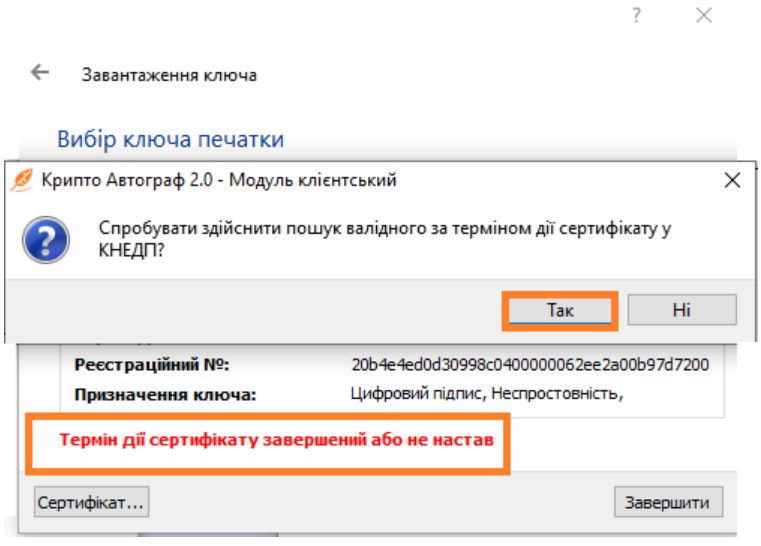
Натисніть «ОК».



Після цього Засіб здійснить пошук сертифікатів на СМР-сервері обраного Вами КНЕДП та завантажить їх до каталогу C:/My Crt. Далі по аналогії з процедурою, описаною вище.



Якщо під час підключення ключа Крипто Автограф виявить, що сертифікати відкритого ключа прострочені – буде здійснено пошук відповідних сертифікатів у каталозі «C:\My Crt». Якщо сертифікат не буде знайдено у каталозі – буде запропоновано здійснити пошук чинного сертифіката в у одному з КНЕДП.



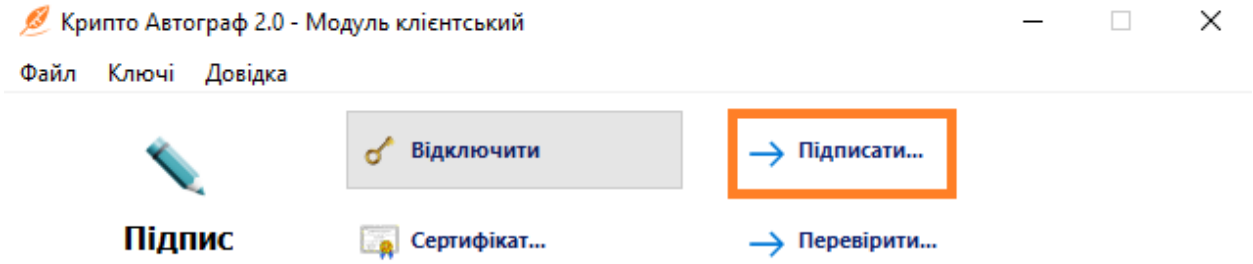
У випадку коли Ви підключаєте ключ КЕП, носієм якого являється ЗНКІ (USB-токен), і сертифікат імпортовано на ЗНКІ (USB-токен), Крипто Автограф виявить, що сертифікати відкритого ключа прострочені – буде здійснено пошук відповідних сертифікатів у каталозі «C:\My Crt». Якщо сертифікат не буде знайдено у каталозі – буде запропоновано здійснити пошук чинного сертифіката в у одному з КНЕДП.

І у випадку підключення файлового ключа, і у випадку ключа на ЗНКІ, в першу чергу після копіювання нового сертифікату до каталогу «C:\My Crt», закрийте і запустіть Засіб повторно для того, щоб він перечитав каталог на предмет наявності Вашого чинного сертифікату. Якщо у Вас немає сертифікатів – дочекайтесь автоматичної взаємодії Засобу з CMP-сервером КНЕДП, як описано вище в даному розділі.

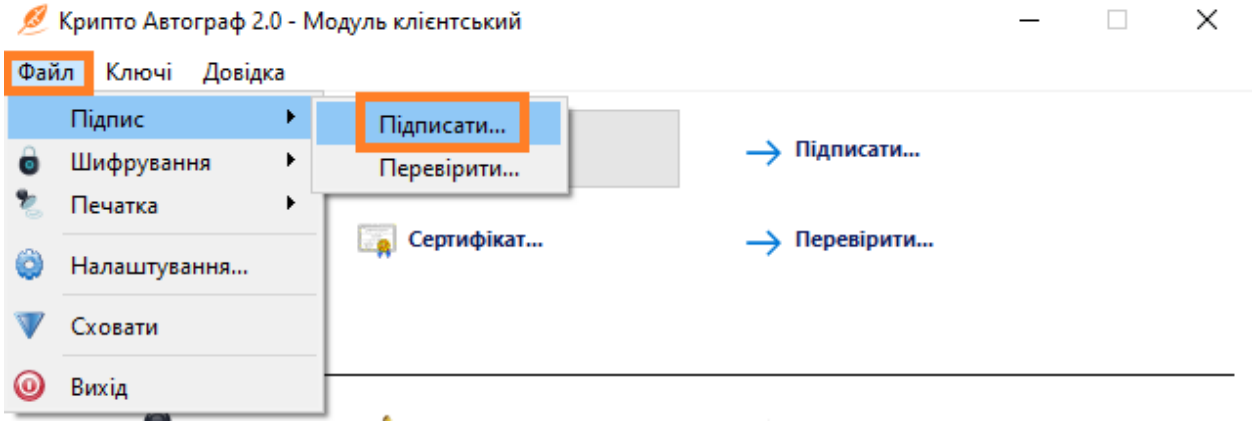
Підписання/ шифрування документів

Підпис

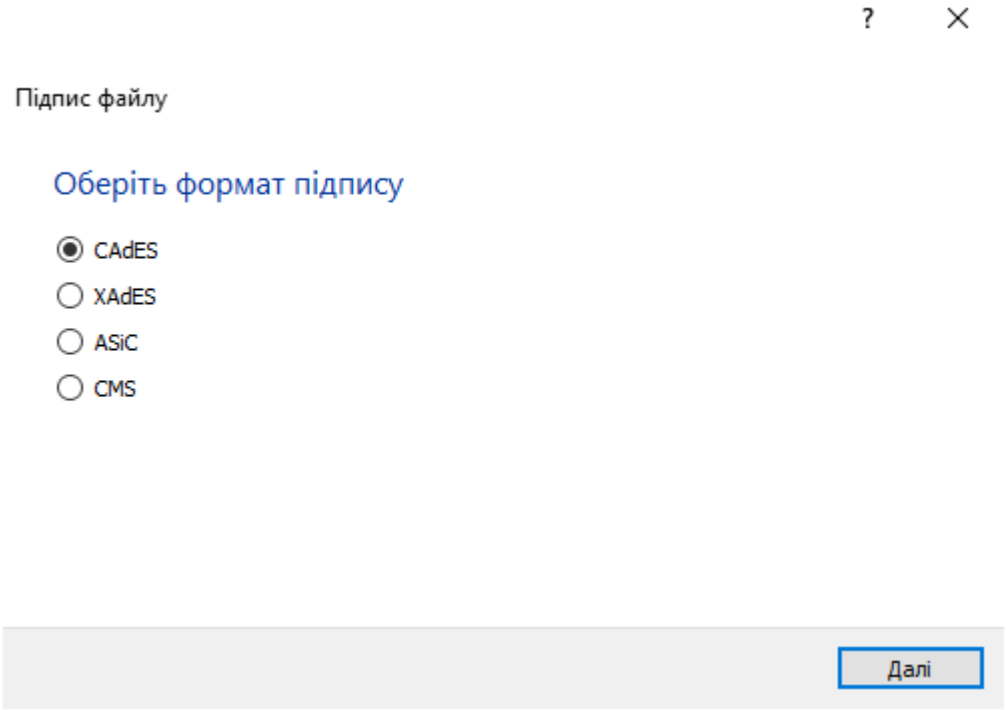
Для накладання ЕП натисніть кнопку «Підписати» в розділі «Підпис» графічного інтерфейсу Засобу.



Або оберіть пункт «Файл» горизонтального меню, далі «Підпис», потім «Підписати».

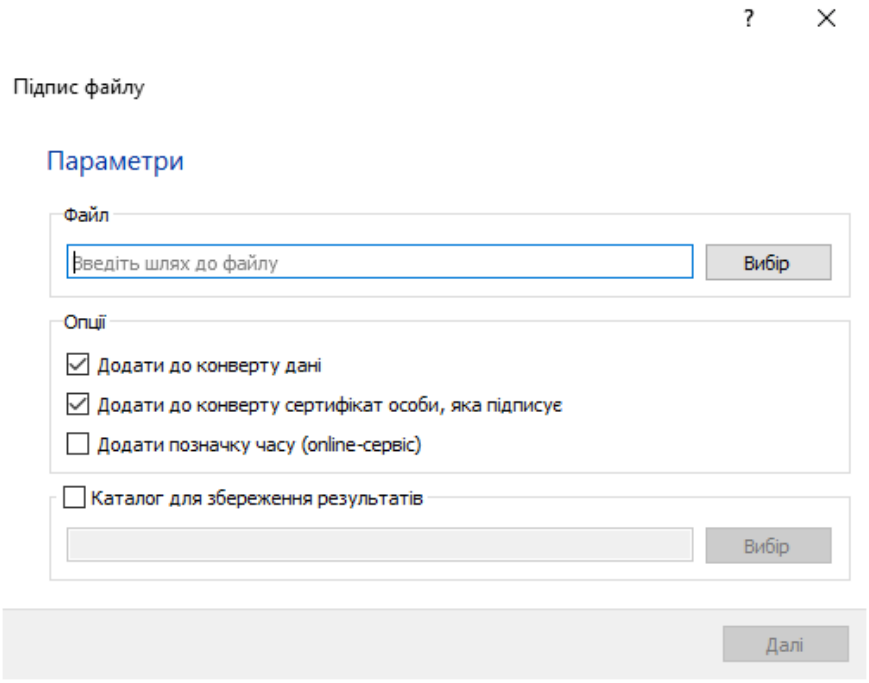


У вікні, що відкрилось, оберіть формат підпису.



Процес підпису в стандартному форматі «CMS»

У вікні, що відкрилось, в розділі «Файл» натисніть кнопку «Вибір» та оберіть в файловому провіднику файл, на який буде накладено ЕП.



У розділі «Опції» є наступні налаштування:

- Додати до конверту дані;
- Додати до конверту сертифікат особи, яка підписує;

- Додати позначку часу.

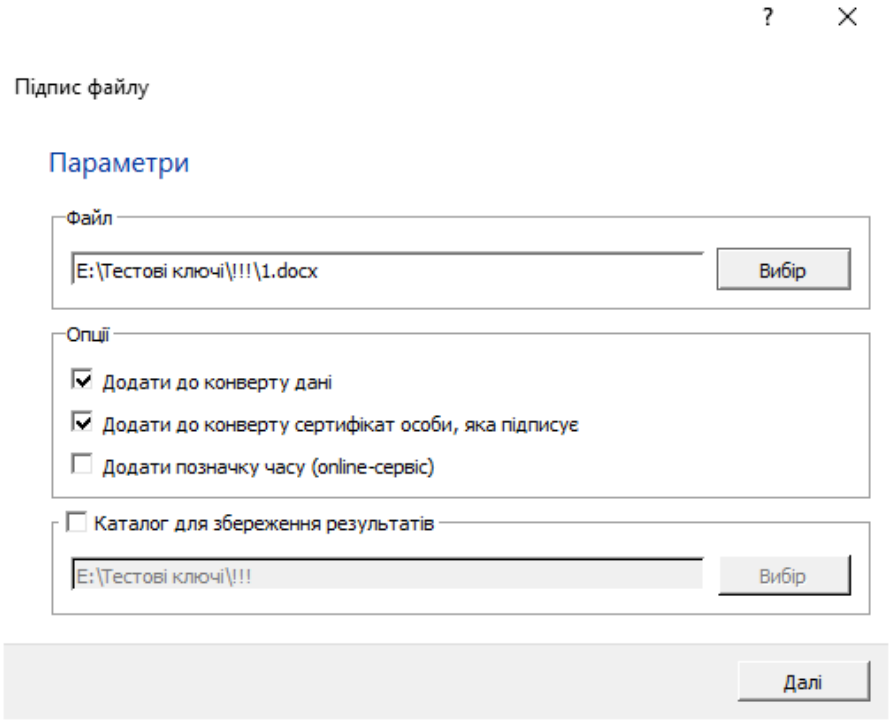
Зніміть позначку в першому пункті якщо Ви бажаєте зберегти окремо файл, що підписується, та ЕП. Залиште позначку в першому пункті якщо бажаєте додати файл до електронного конверту формату .p7s.

Зніміть позначку в другому пункті якщо Ви не бажаєте додавати до електронного конверту власний сертифікат. Залиште позначку в другому пункті якщо бажаєте додати власний сертифікат відкритого ключа до електронного конверту формату .p7s. Для зручності перевірки ЕП другою стороною рекомендується додавати власний сертифікат відкритого ключа до електронного конверту.

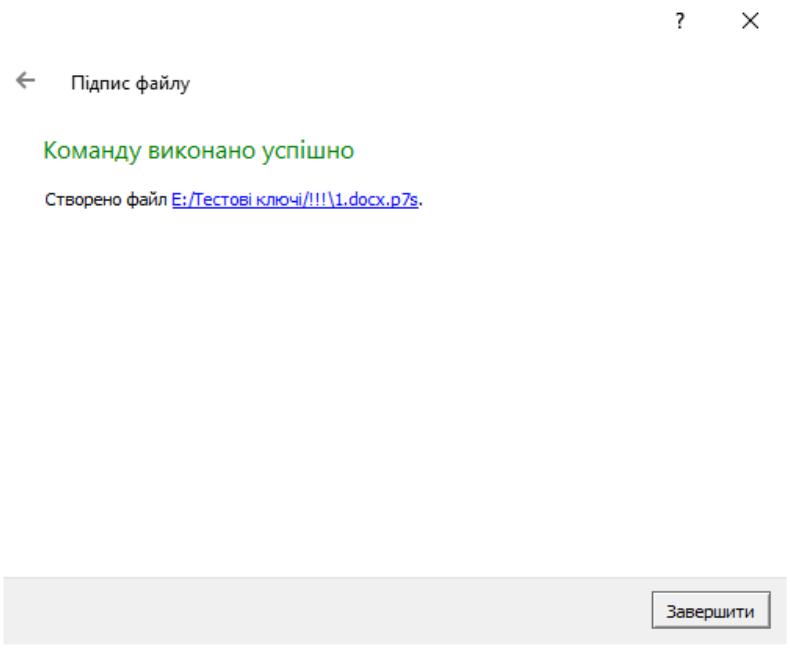
Поставте позначку в третьому пункті якщо бажаєте під час підписання додати до конверту позначку часу, яка, в свою чергу, отримується від КНЕДП по протоколу TSP (потребує підключення до мережі Інтернет).

Поставте позначку напроти пункту «Каталог для збереження файлів» якщо бажаєте змінити каталог, в який буде збережено електронний конверт формату .p7s. За замовчуванням електронний конверт формату .p7s буде збережено в той самий каталог, в якому знаходиться вихідний файл.

Після завершення налаштувань підпису натисніть «Далі».



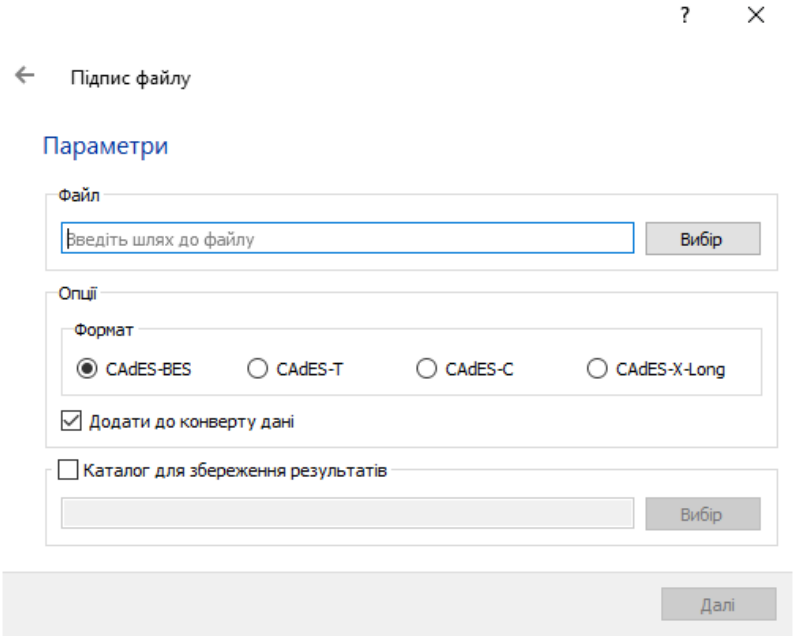
Вікно, що відкриється і зображено нижче, свідчить про успішне створення електронного конверту і відповідно накладання ЕП. Натисніть «Завершити».



Процес підпису в форматі CAdES

При підписанні файлу в форматі CAdES можливі чотири режими:

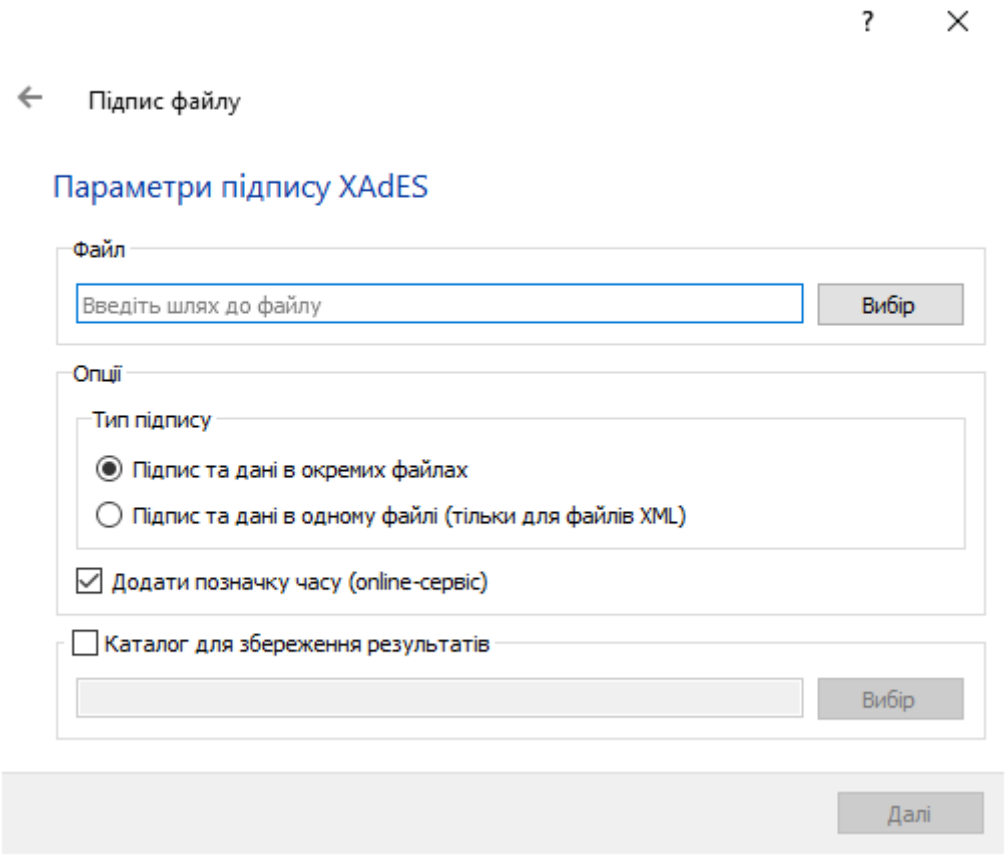
- CAdES-BES (базовий);
- CAdES-T (підпис з довіреним часом);
- CAdES-C (з повним набором перевірочних даних) ;
- CAdES-X-Long (містить в собі повний набір перевірочних даних, як CAdES-C, а також повні дані сертифікатів та списків відкликаних сертифікатів).



Оберіть бажаний режим підпису у категорії «Формат», подальший підпис файлу здійснюється аналогічно з вищеописаним режимом CMS.

Процес підпису в форматі XAdES

XAdES дозволяє зберігати електронний підпис файлу у форматі .xml, окремо від файлу, або ж у спільному конверті.



Оберіть режим підпису у категорії «Формат», подальший підпис файлу здійснюється аналогічно з вищеописаним режимом CMS.

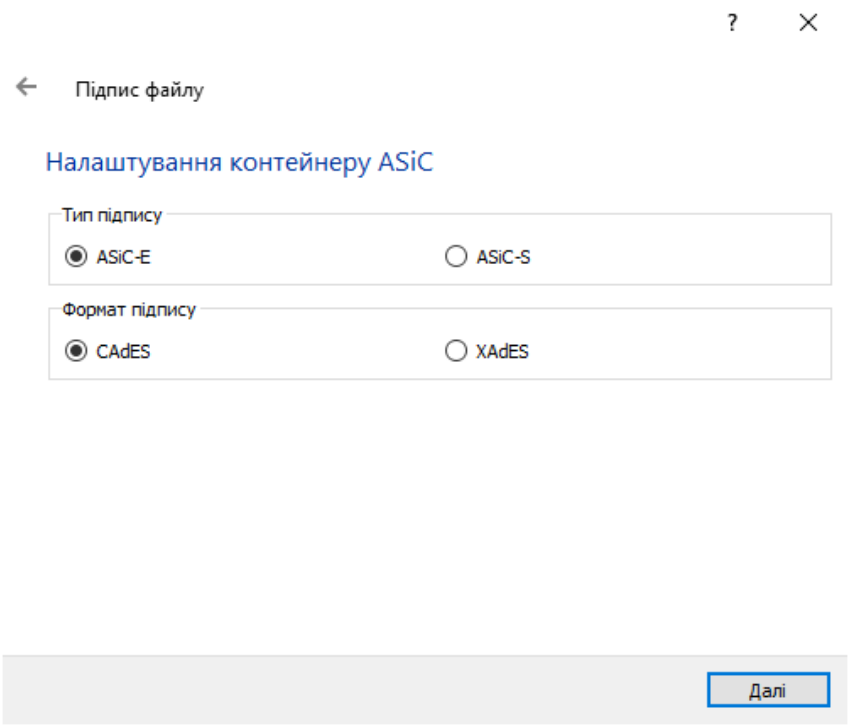
Процес підпису в форматі ASiC

Існує два типи контейнерів електронного підпису типу ASiC: ASiC-S (звичайний) та ASiC-E (розширений). Кожен з двох контейнерів може бути двох форматів: CAdES та XAdES.

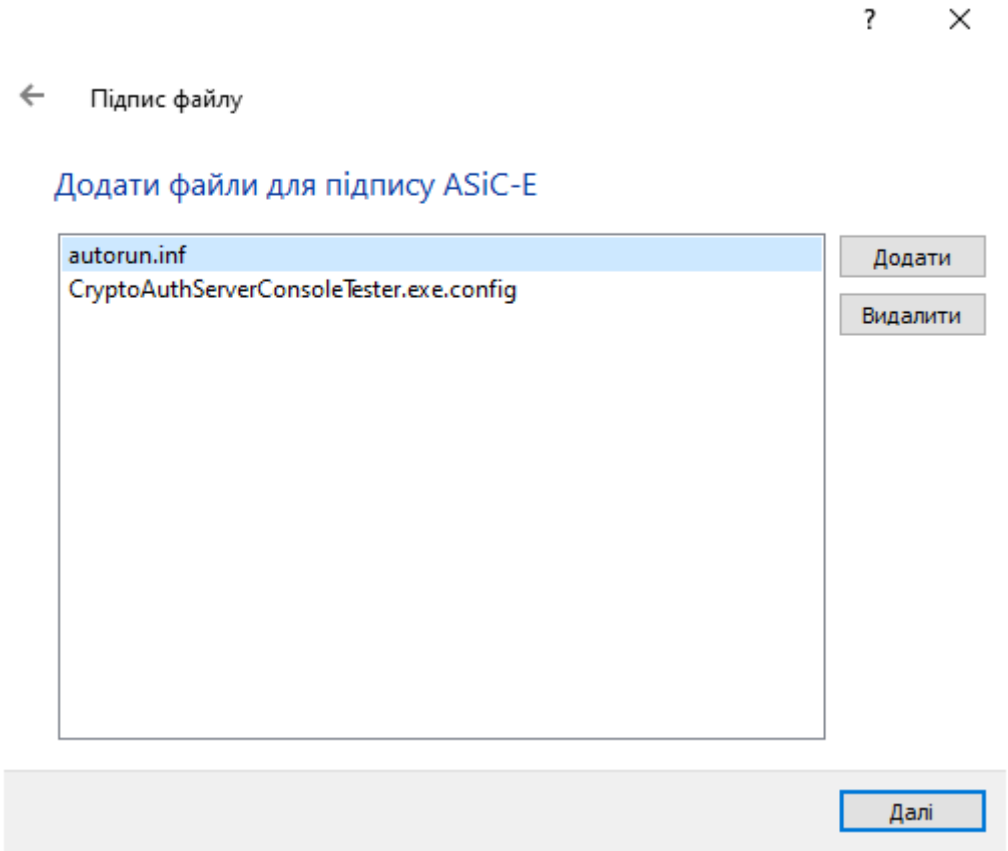
При підписанні файлів в режимі ASiC можливо чотири варіанти:

- ASiC-S + CAdES;
- ASiC-S + XAdES;
- ASiC-E + CAdES;
- ASiC-E + XAdES.

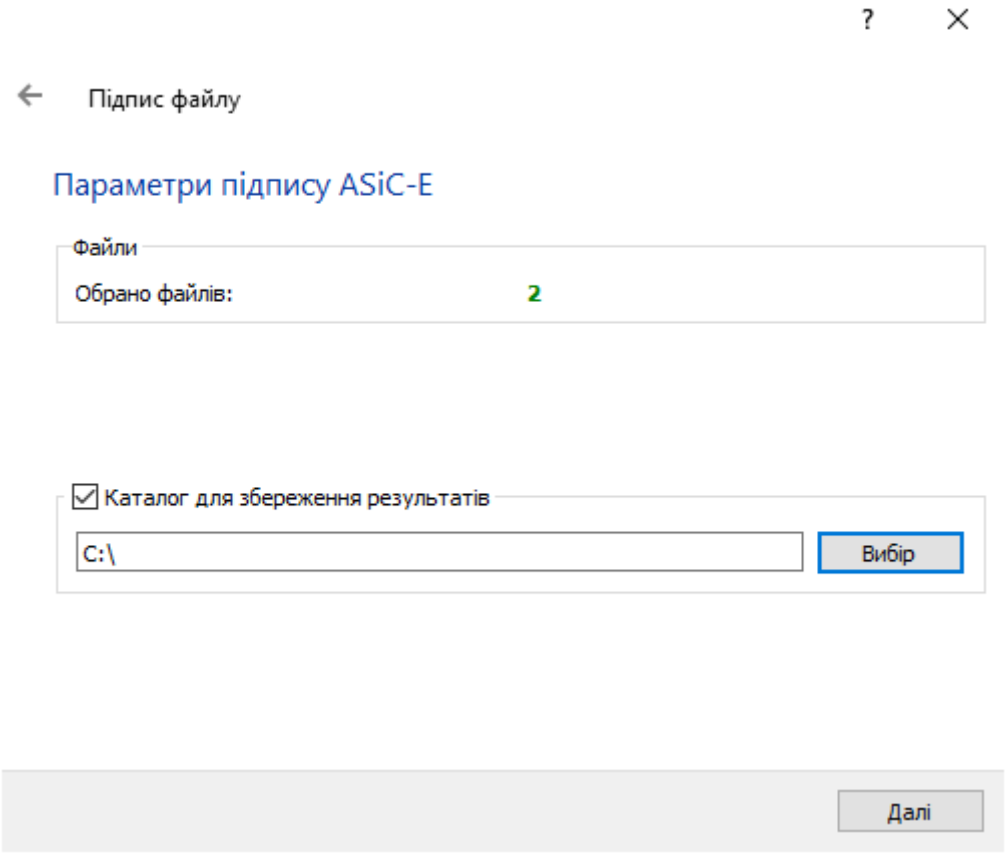
Оберіть по одному варіанту у розділах «Тип підпису» та «Формат підпису» та натисніть «Далі».

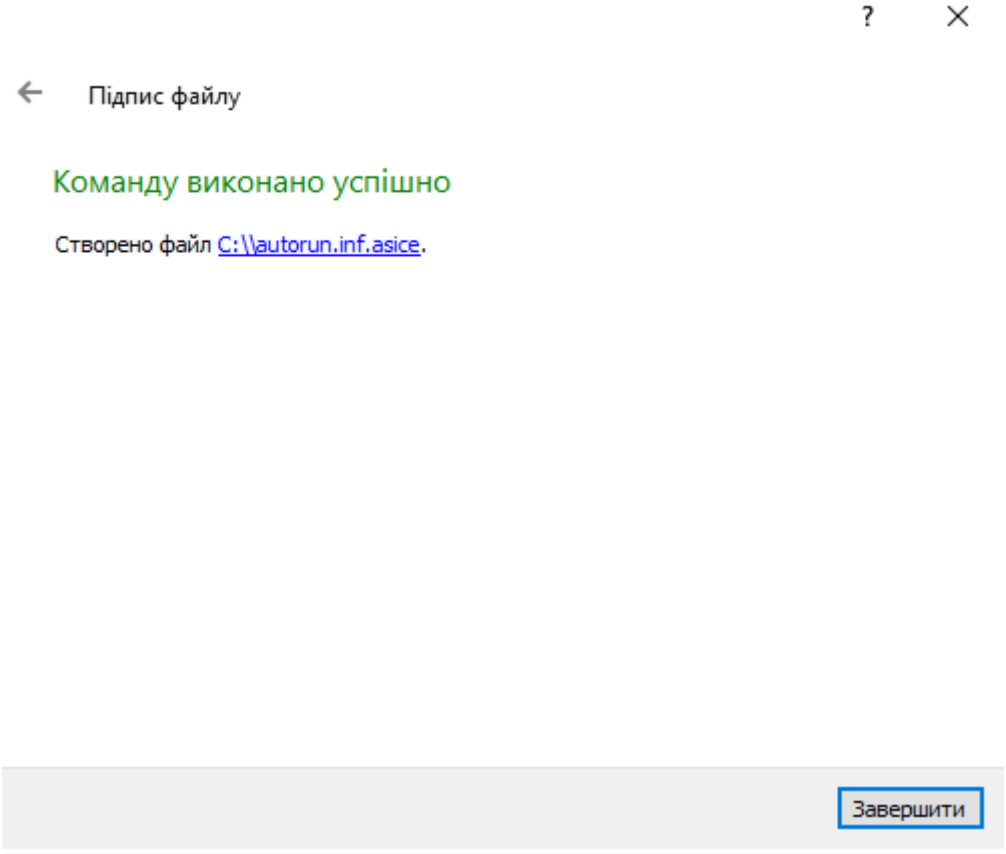


У вікні, що відкрилось і зображено нижче, натисніть «Додати» та через файловий провідник операційної системи оберіть один або декілька файлів, які Ви бажаєте підписати. Після обрання натисніть «Далі» для продовження.



У вікні, що відкрилось і зображено нижче, відображено кількість обраних файлів, та шлях до каталогу в який буде збережено підпис. Натисніть «Далі»



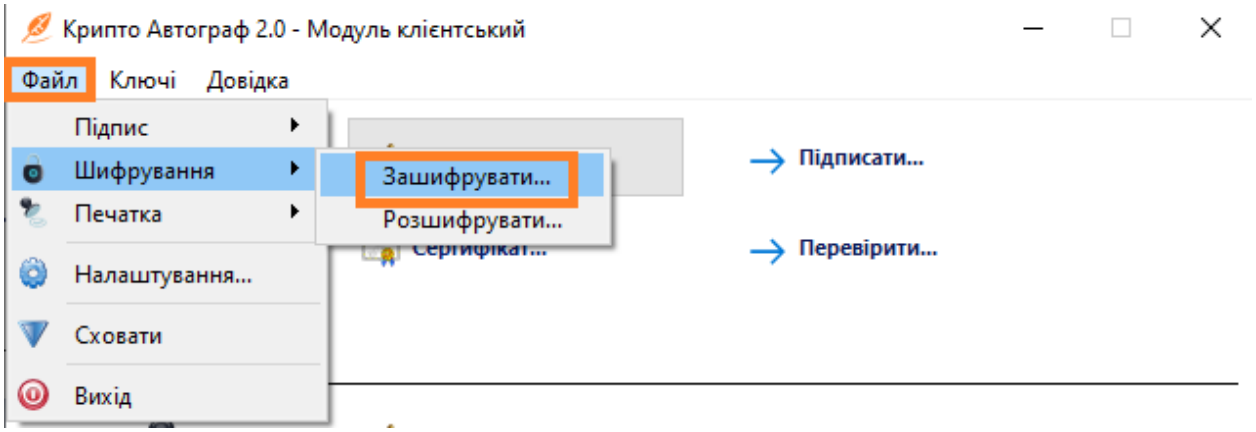


Шифрування

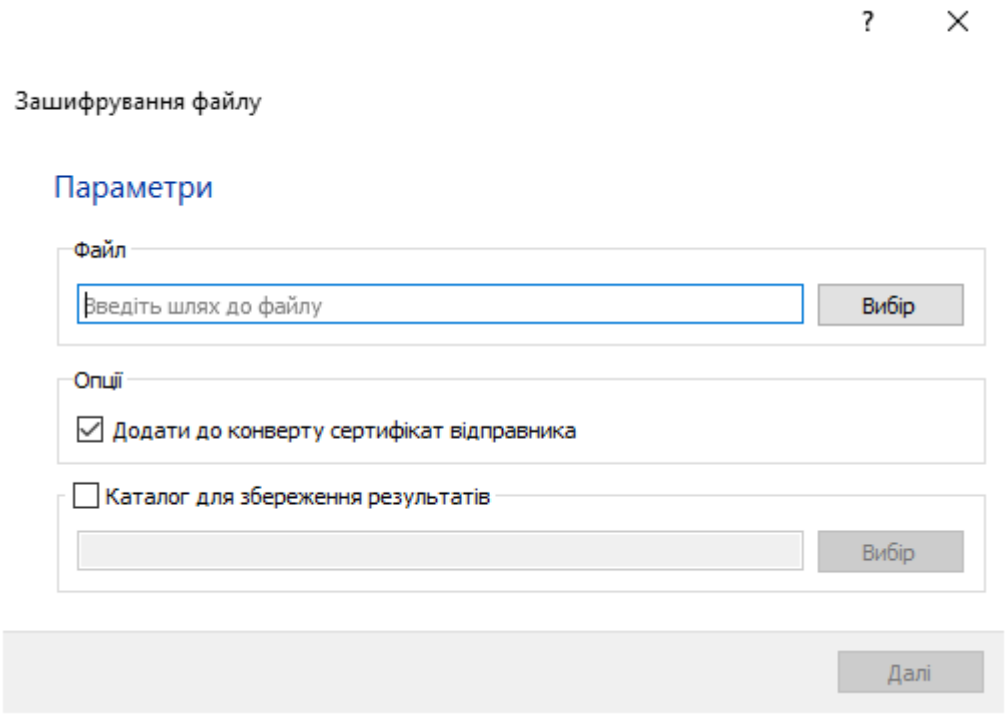
Для шифрування оберіть пункт «Файл» горизонтального меню, далі «Шифрування», потім «Зашифрувати».

Або натисніть кнопку «Зашифрувати» в розділі «Шифрування» графічного інтерфейсу Засобу.

Зверніть увагу, що за замовчуванням розділ «Шифрування» не відображається в графічному інтерфейсі користувача. Для того щоб його увімкнути перейдіть в розділ КОНФІГУРАЦІЯ ЗАСОБУ, параметр «useencryption».



У вікні, що відкрилось, в розділі «Файл» натисніть кнопку «Вибір» та оберіть в файловому провіднику файл, який буде зашифровано.

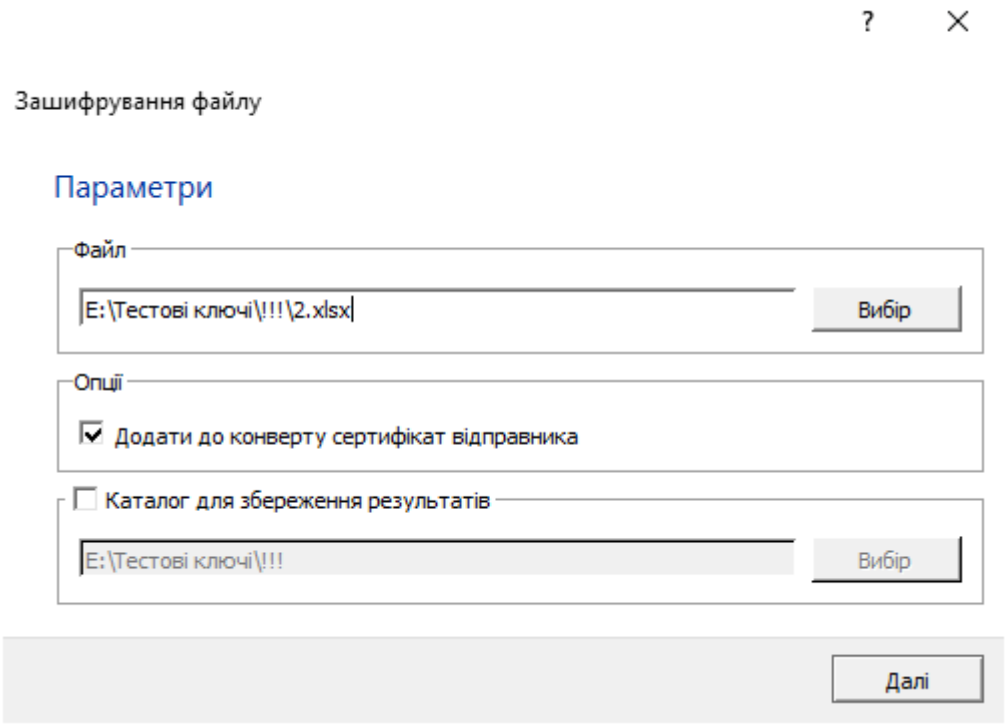


Обравши файл для шифрування, перейдіть до розділу «Опції». Зніміть позначку в пункті «Додати до конверту сертифікат відправника» якщо Ви не

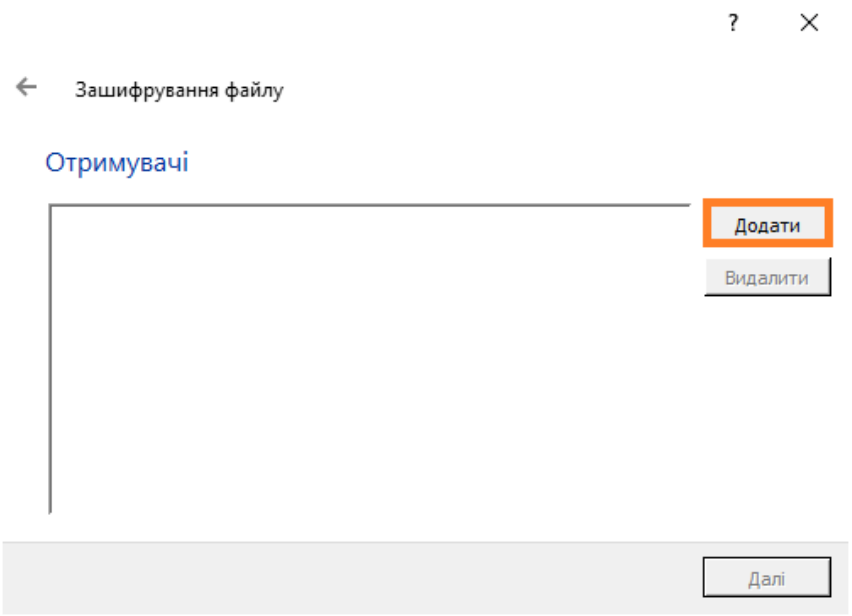
бажаєте додавати до електронного конверту сертифікат особи. Залиште позначку якщо бажаєте додати сертифікат відкритого ключа до електронного конверту формату .p7e. Для зручності розшифрування файлу другою стороною рекомендується додавати сертифікат відкритого ключа до електронного конверту.

Поставте позначку напроти пункту «Каталог для збереження файлів» якщо бажаєте змінити каталог, в який буде збережено електронний конверт формату .p7e. За замовчуванням електронний конверт формату .p7e буде збережено в той самий каталог, в якому знаходиться вихідний файл.

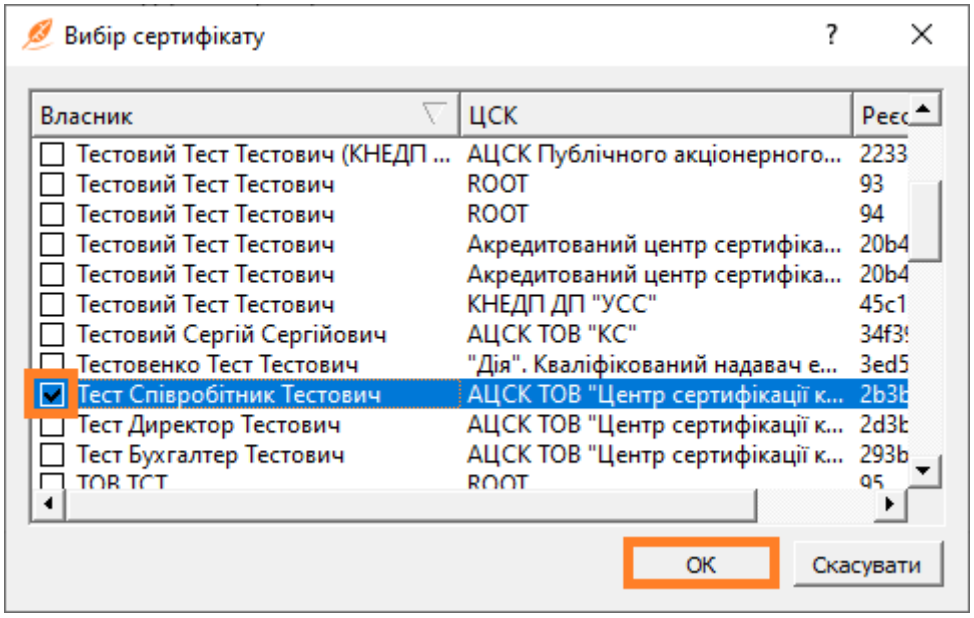
Після завершення налаштувань шифрування натисніть «Далі».



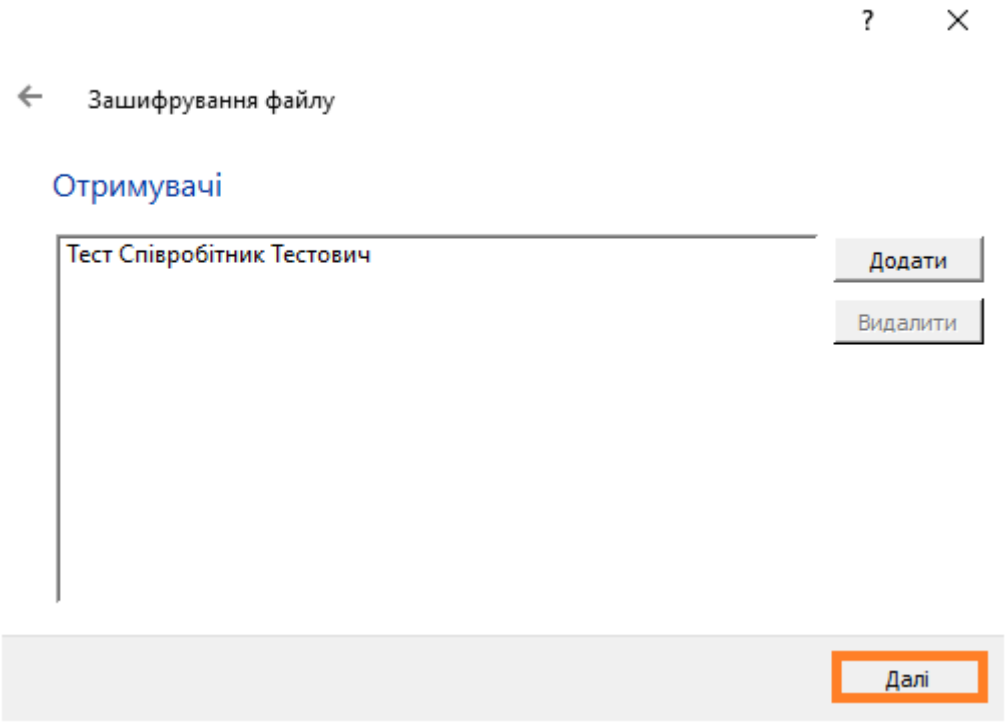
У вікні, що відкрилось і зображено нижче, необхідно вказати отримувачів зашифрованого файлу. Для цього натисніть кнопку «Додати» в правій частині вікна.



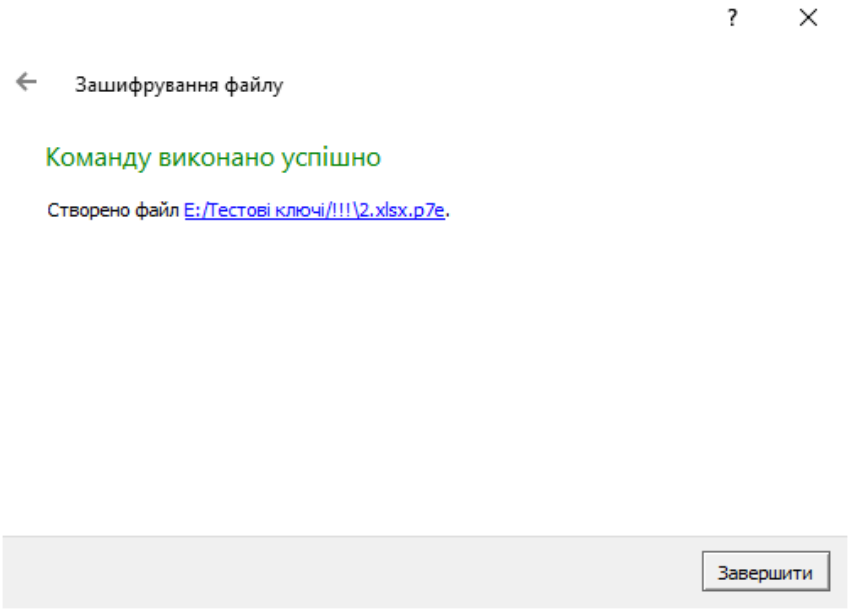
У вікні, що відкрилось і зображено нижче, оберіть отримувачів і поставте відмітки напроти обраних, та натисніть «ОК». Перелік отримувачів формується на підставі наявності сертифікатів відкритого ключа в каталозі C:\My Crt. Якщо потрібного отримувача немає в переліку – це свідчить про відсутність сертифікату відкритого ключа в каталозі C:\My Crt.



Підтвердьте обраних отримувачів натисканням кнопки «Далі».

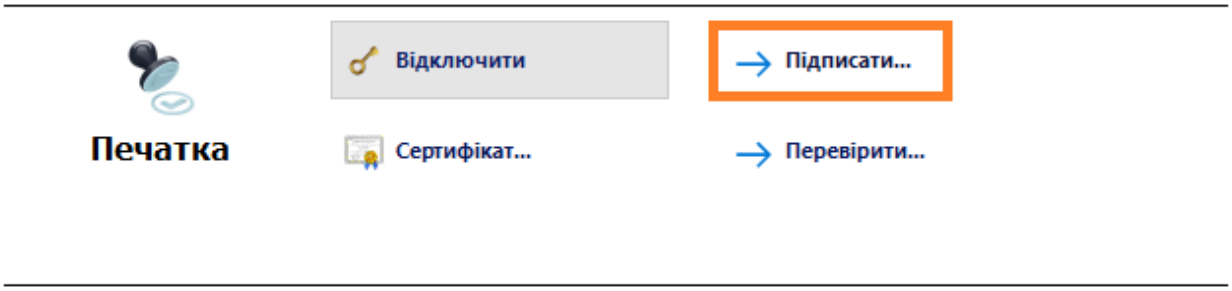


Вікно, що відкриється і зображено нижче, свідчить про успішне створення електронного конверту і відповідно шифрування файлу.

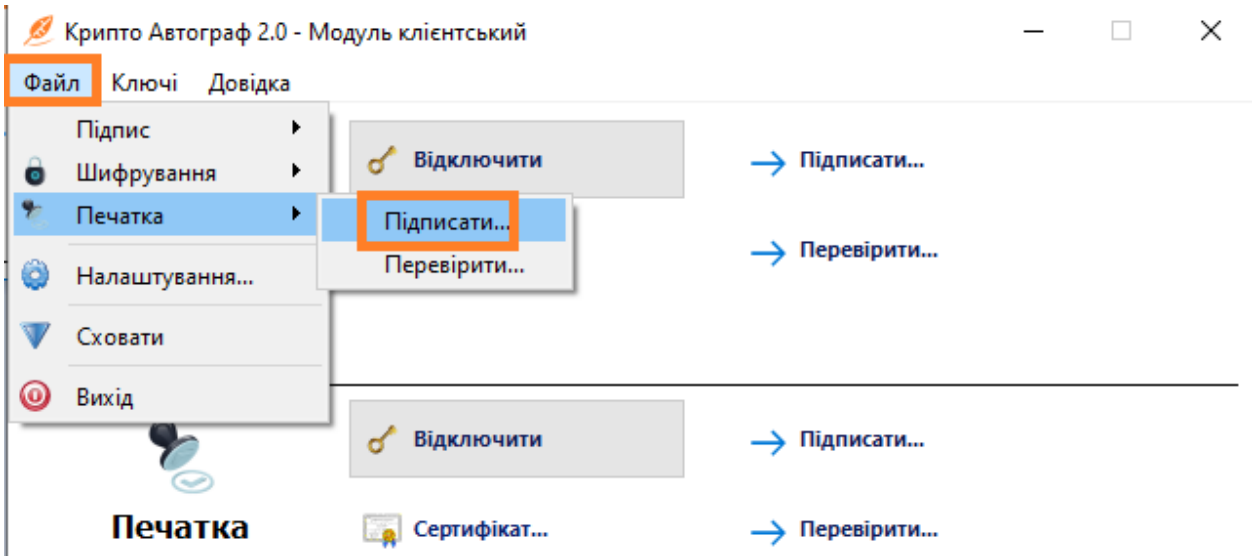


Печатка

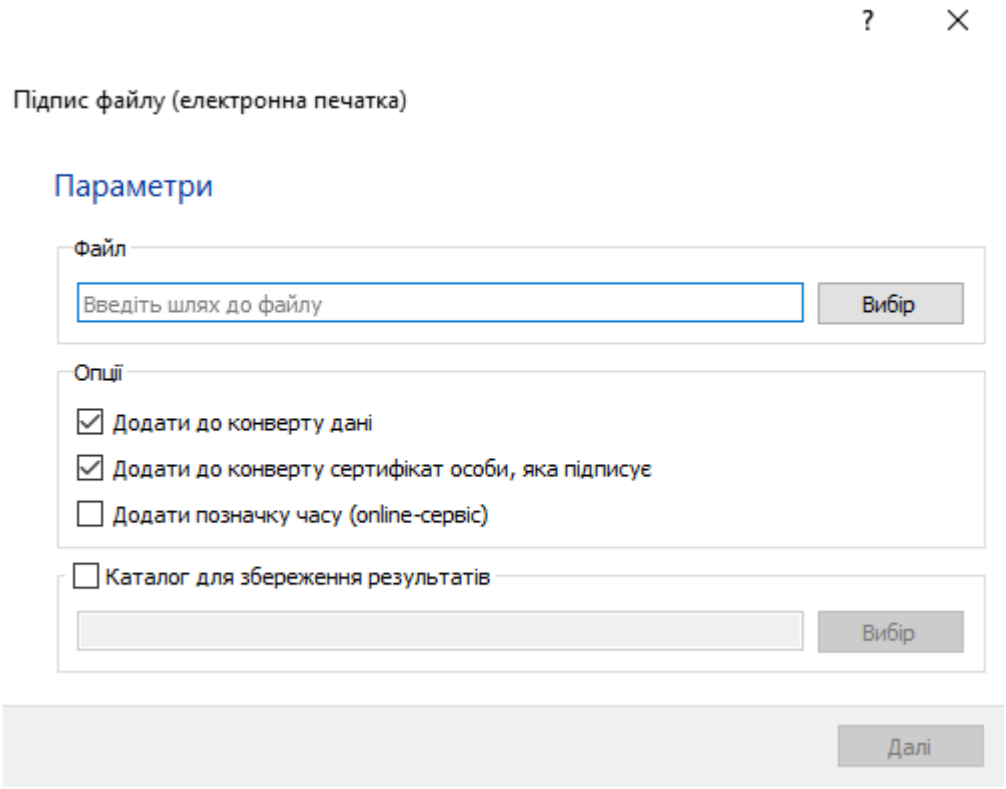
Для накладання електронної печатки натисніть кнопку «Підписати» в розділі «Печатка» графічного інтерфейсу Засобу.



Або оберіть пункт «Файл» горизонтального меню, далі «Печатка», потім «Підписати».



У вікні, що відкрилось, в розділі «Файл» натисніть кнопку «Вибір» та оберіть в файловому провіднику файл, на який буде накладено ЕП.



У розділі «Опції» є наступні налаштування:

- Додати до конверту дані;
- Додати до конверту сертифікат особи, яка підписує;
- Додати позначку часу.

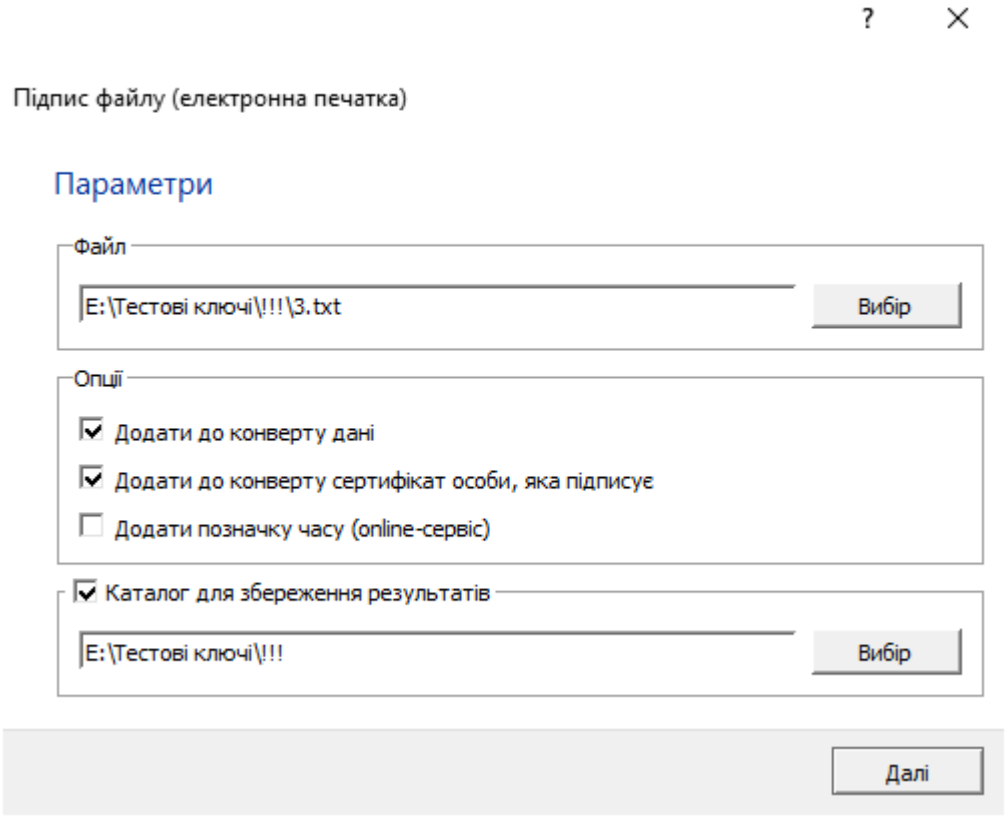
Зніміть позначку в першому пункті якщо Ви бажаєте зберегти окремо файл, що підписується, та електронну печатку. Залиште позначку в першому пункті якщо бажаєте додати файл до електронного конверту формату .p7s.

Зніміть позначку в другому пункті якщо Ви не бажаєте додавати до електронного конверту сертифікат особи. Залиште позначку в другому пункті якщо бажаєте додати сертифікат відкритого ключа до електронного конверту формату .p7s. Для зручності перевірки електронної печатки другою стороною рекомендується додавати сертифікат відкритого ключа до електронного конверту.

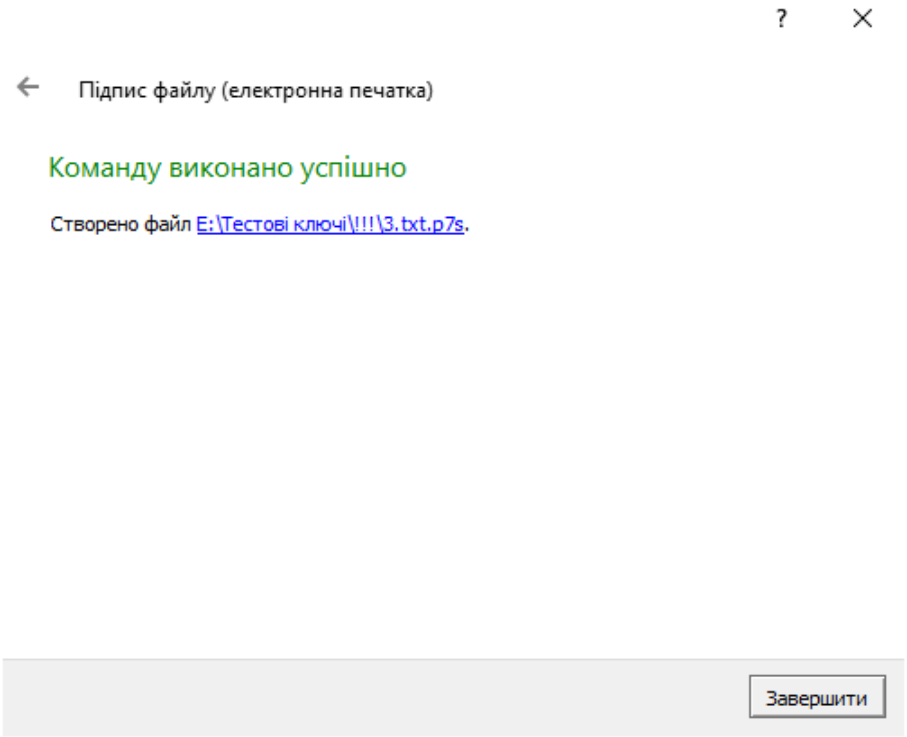
Поставте позначку в третьому пункті якщо бажаєте під час підписання додати до конверту позначку часу, яка, в свою чергу, отримується від КНЕДП по протоколу TSP (потребує підключення до мережі Інтернет).

Поставте позначку напроти пункту «Каталог для збереження файлів» якщо бажаєте змінити каталог, в який буде збережено електронний конверт формату .p7s. За замовчуванням електронний конверт формату .p7s буде збережено в той самий каталог, в якому знаходиться вихідний файл.

Після завершення налаштувань підпису натисніть «Далі».

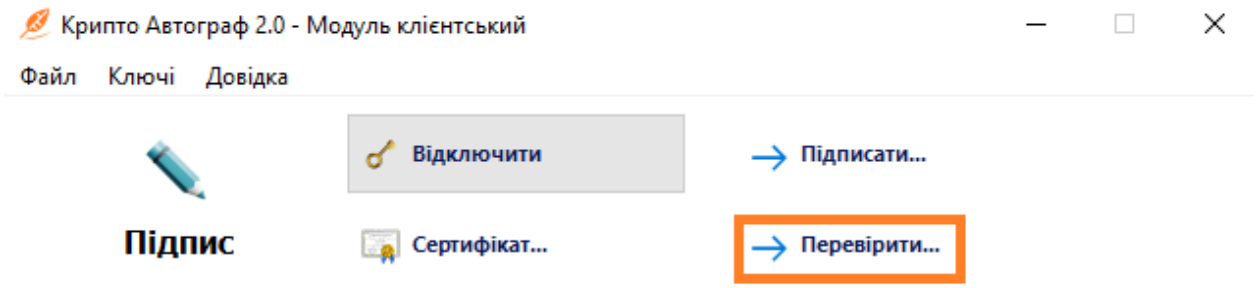


Вікно, що відкриється і зображено нижче, свідчить про успішне створення електронного конверту і відповідно накладання ЕП.

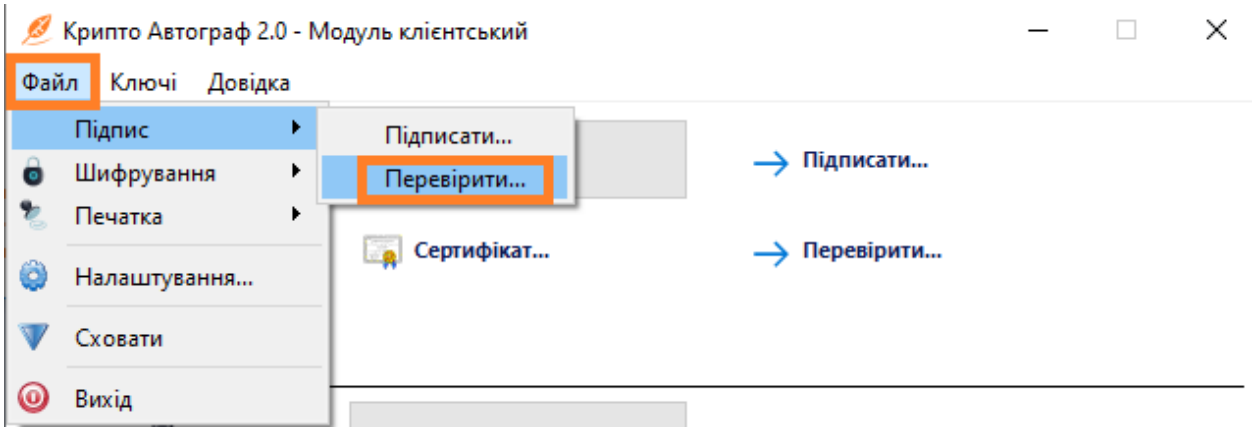


Перевірка ЕП/ розшифрування
Перевірка підпису

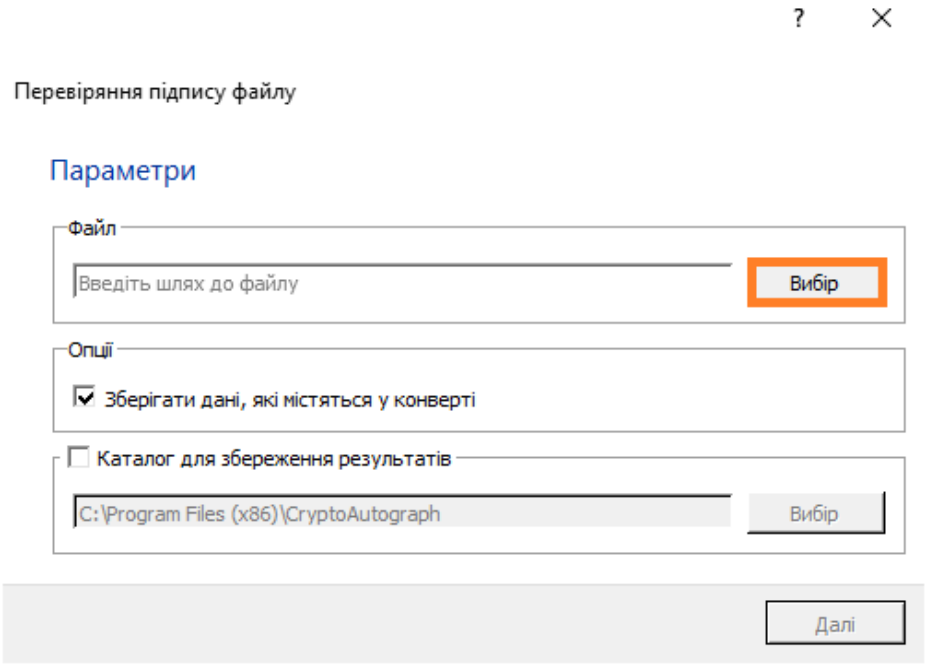
Для перевірки ЕП натисніть кнопку «Перевірити» в графічному інтерфейсі Засобу. Варто зазначити, що для перевірки підпису не обов’язково підключати особистий ключ.



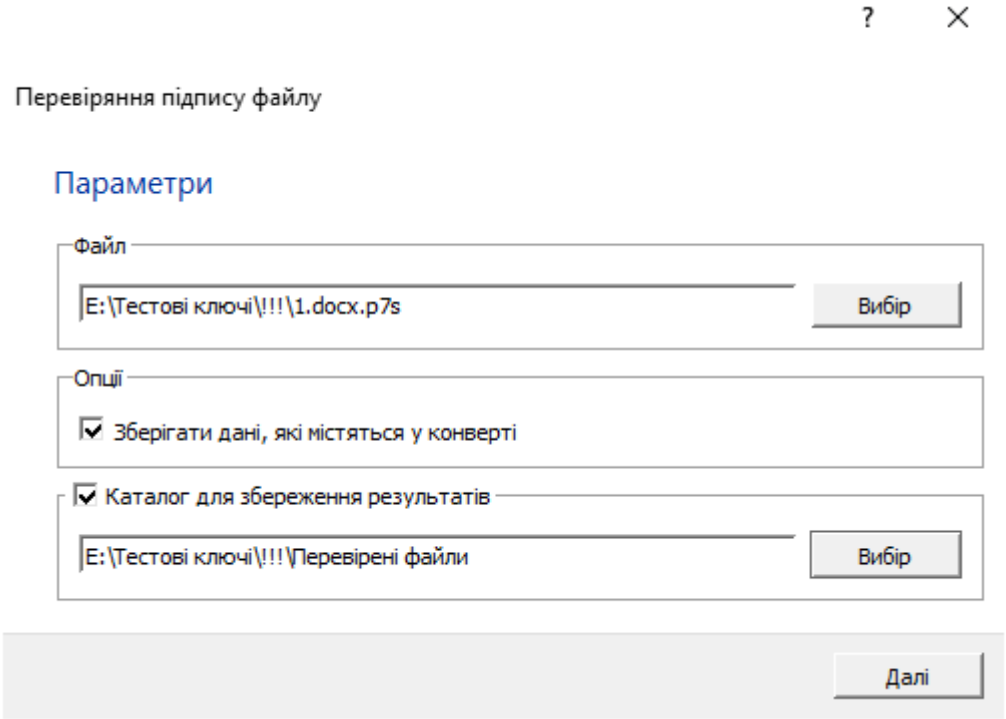
Або в горизонтальному меню натисніть пункт «Файл», потім «Підпис» і оберіть пункт меню «Перевірити».



У вікні, що відкрилось і зображено нижче, натисніть «Вибір» для обрання підписаного файлу формату .p7s.

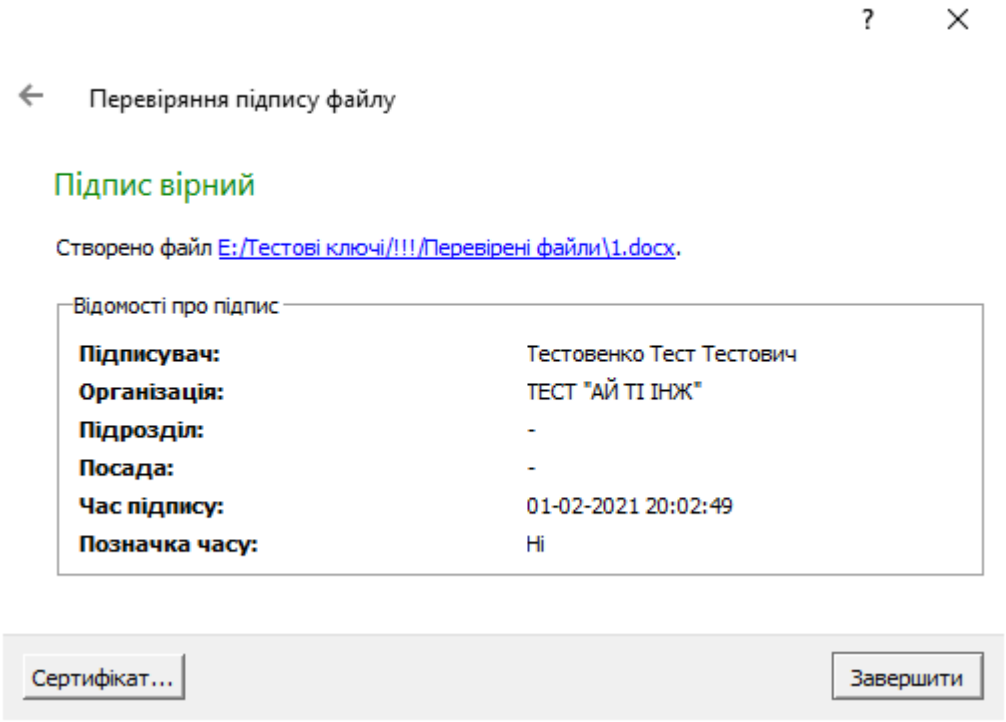


Після обрання файлу Ви можете зняти позначку в розділі «Опції» напроти пункту «Зберігати дані, які містяться у конверті». В такому випадку файл, що підписано, не буде збережено. Буде лише перевірений ЕП. Також можна поставити позначку «Каталог для збереження результатів» для зміни каталогу. За замовчування результати будуть збережені в каталог, де міститься вихідний файл. Після здійснення налаштувань натисніть «Далі».



У вікні, що відкрилось і зображено нижче, бачимо підтвердження підпису, посилання на файл, натиснувши на яке можна перейти до каталогу з файлом, а також відомості про підпис. Натиснувши на кнопку «Сертифікат» в

лівому нижньому куті, можна переглянути відомості про сертифікат підписувача. Натисніть «Завершити» для закінчення процедури перевірки.

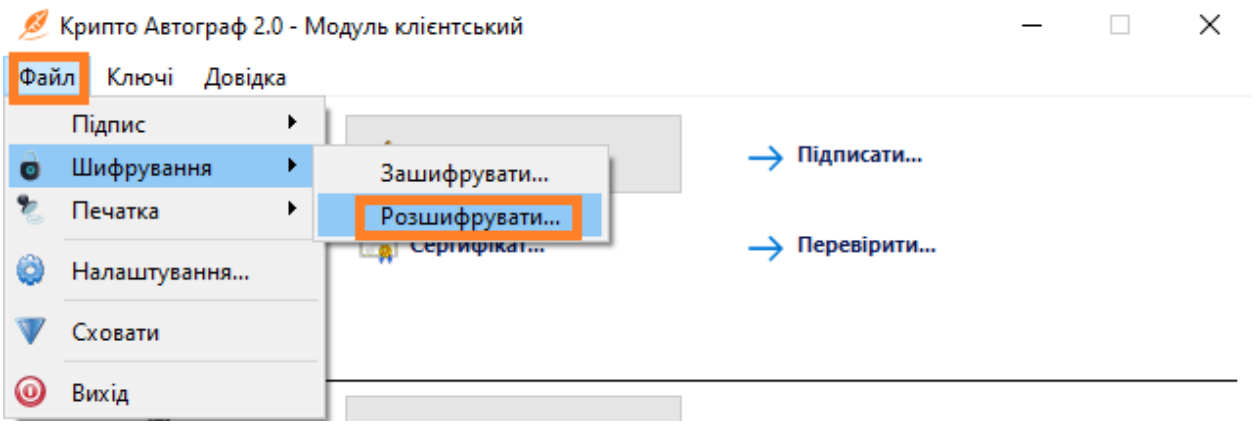


Розшифрування файлу

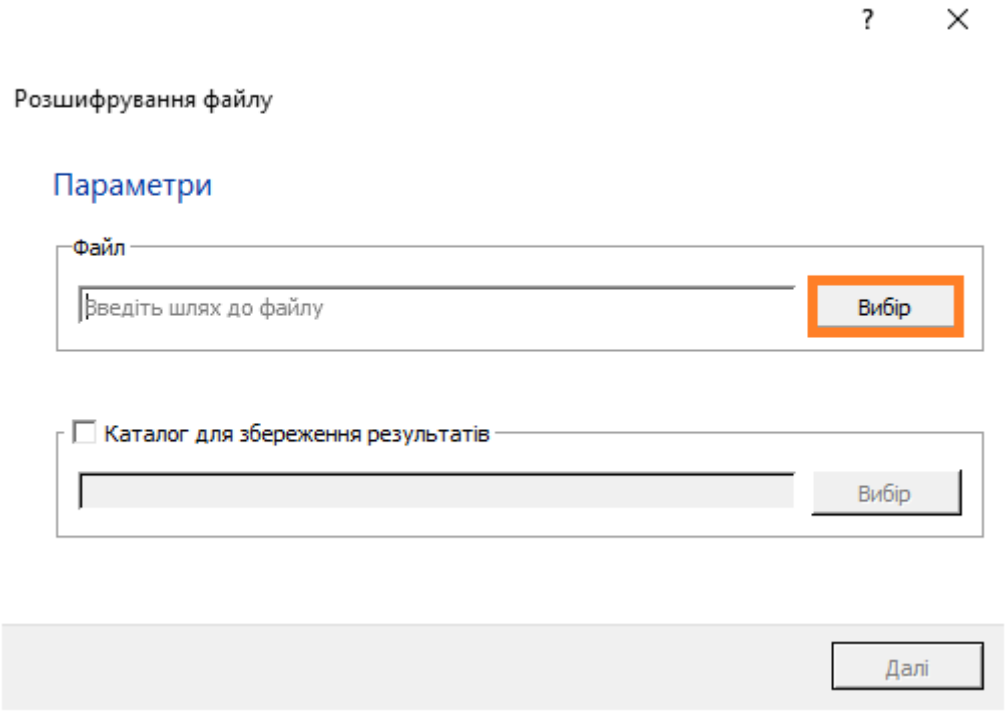
На відміну від перевірки підпису, для процедури розшифрування файлу необхідно підключити особистий ключ користувача, який був вказаний як отримувач зашифрованого файлу. Після підключення особистого ключа, або у разі якщо ключ вже підключено, оберіть в горизонтальному меню пункт «Файл», далі «Шифрування», потім «Розшифрувати».

Або натисніть кнопку «Розшифрувати» в розділі «Шифрування» графічного інтерфейсу.

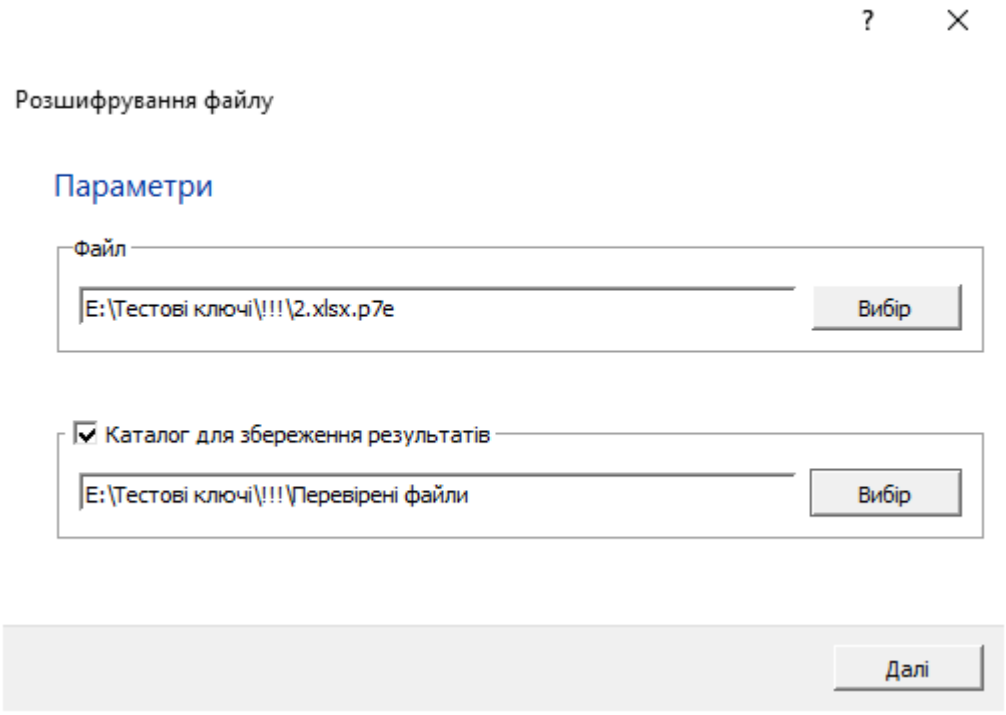
Зверніть увагу, що за замовчуванням розділ «Шифрування» не відображається в графічному інтерфейсі користувача. Для того щоб його увімкнути перейдіть в розділ КОНФІГУРАЦІЯ ЗАСОБУ, параметр «useencryption».



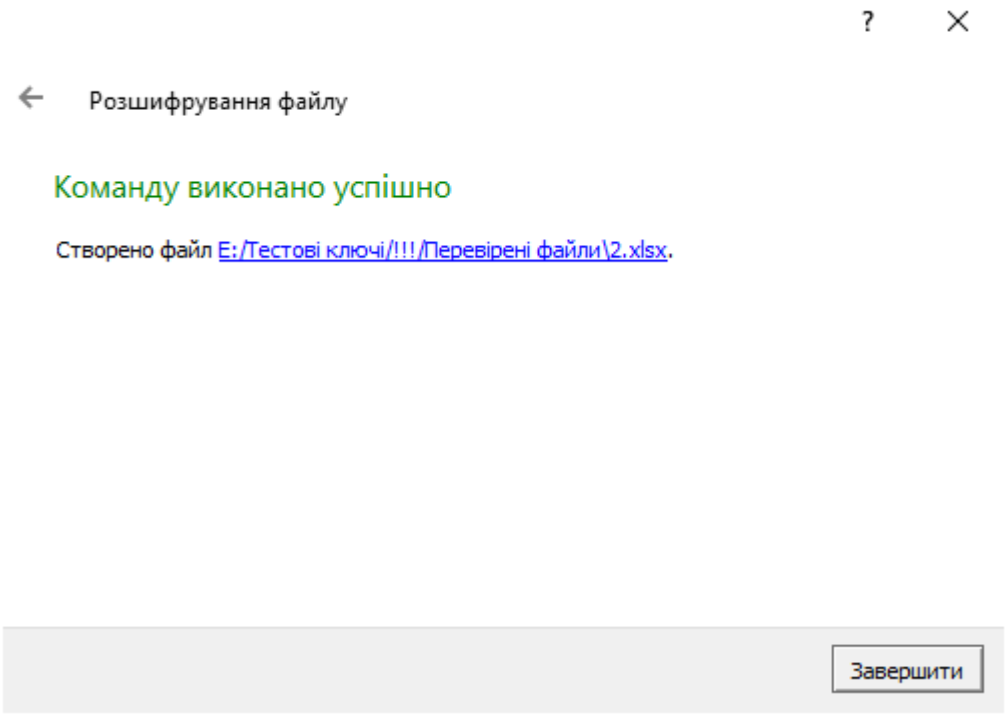
У вікні, що відкрилось і зображено нижче натисніть «Вибір» для обрання зашифрованого файлу формату .p7e.



Після обрання файлу Ви можете поставити позначку «Каталог для збереження результатів» для зміни каталогу. За замовчування результати будуть збережені в каталог, де міститься вихідний файл. Після здійснення налаштувань натисніть «Далі».

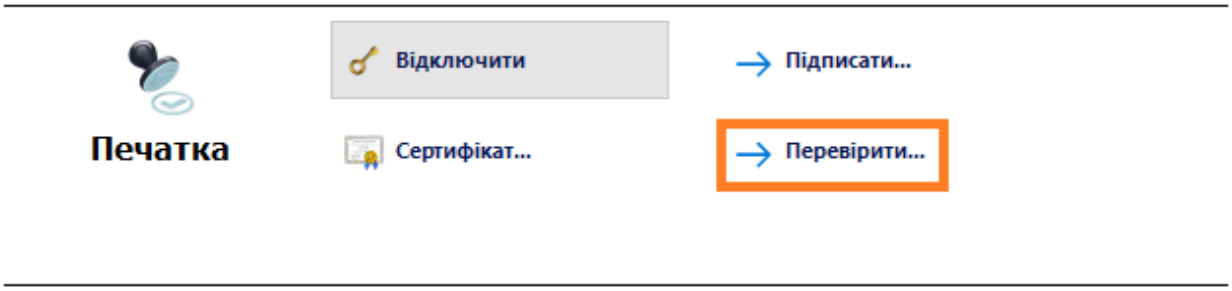


У вікні, що відкрилось і зображено нижче, бачимо підтвердження розшифрування, посилання на файл, натиснувши на яке можна перейти до каталогу з файлом, а також відомості про сертифікат відправника. Натиснувши на кнопку «Сертифікат» в лівому нижньому куті, можна переглянути детальні відомості про сертифікат відправника. Натисніть «Завершити» для закінчення процедури розшифрування.

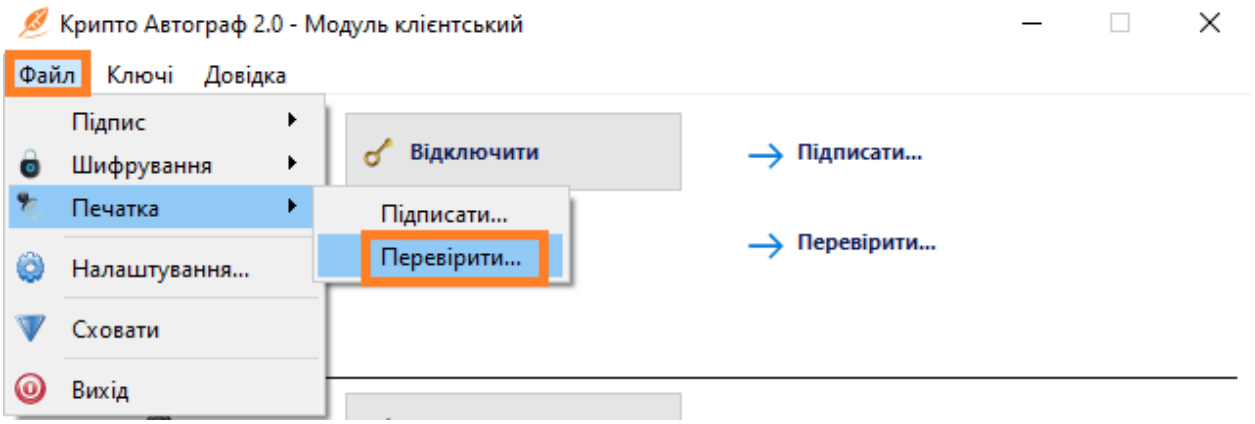


Перевірка електронної печатки

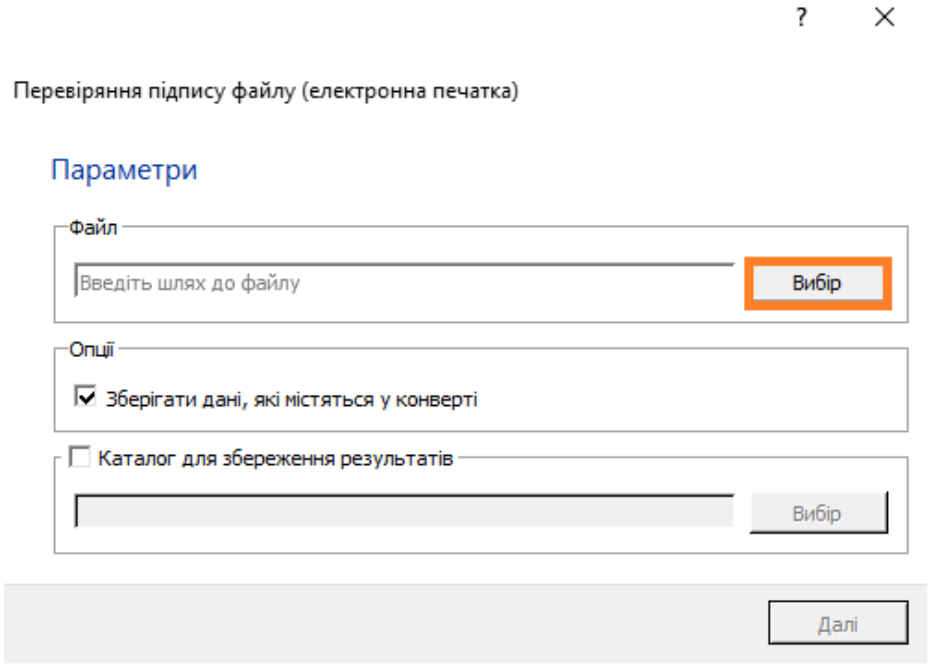
Для перевірки електронної печатки натисніть кнопку «Перевірити» в графічному інтерфейсі Засобу. Варто зазначити, що для перевірки електронної печатки не обов’язково підключати особистий ключ.



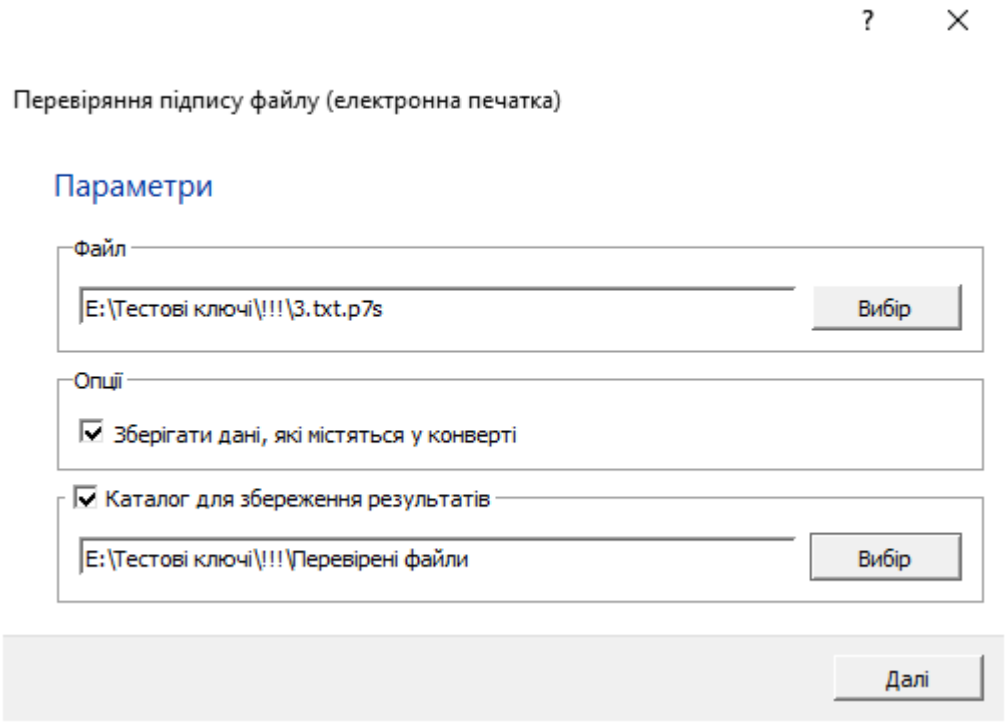
Або в горизонтальному меню натисніть пункт «Файл», потім «Печатка» і оберіть пункт меню «Перевірити».



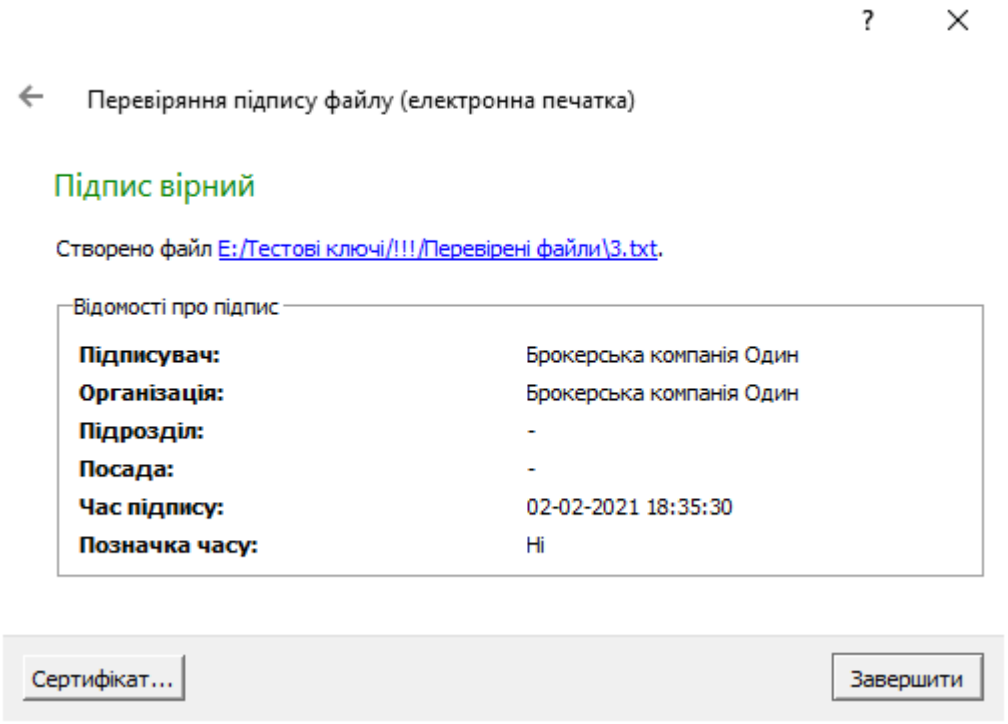
У вікні, що відкрилось і зображено нижче, натисніть «Вибір» для обрання підписаного файлу формату .p7s.



Після обрання файлу Ви можете зняти позначку в розділі «Опції» напроти пункту «Зберігати дані, які містяться у конверті». В такому випадку файл, що підписано, не буде збережено. Буде лише перевірена електронна печатка. Також можна поставити позначку «Каталог для збереження результатів» для зміни каталогу. За замовчування результати будуть збережені в каталог, де міститься вихідний файл. Після здійснення налаштувань натисніть «Далі».



У вікні, що відкрилось і зображено нижче, бачимо підтвердження електронної печатки, посилання на файл, натиснувши на яке можна перейти до каталогу з файлом, а також відомості про підпис. Натиснувши на кнопку «Сертифікат» в лівому нижньому куті, можна переглянути відомості про сертифікат підписувача. Натисніть «Завершити» для закінчення процедури перевірки.



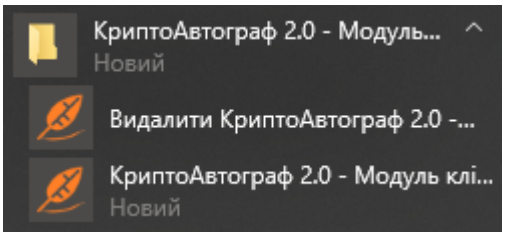
ФОРМУВАННЯ КРИПТОГРАФІЧНИХ КЛЮЧІВ

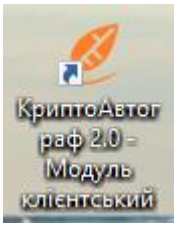
Формування запиту на сертифікат на смарт-карту (USB-токен, ЗНКІ)

Формування запиту на сертифікат юридичної особи - підписувача

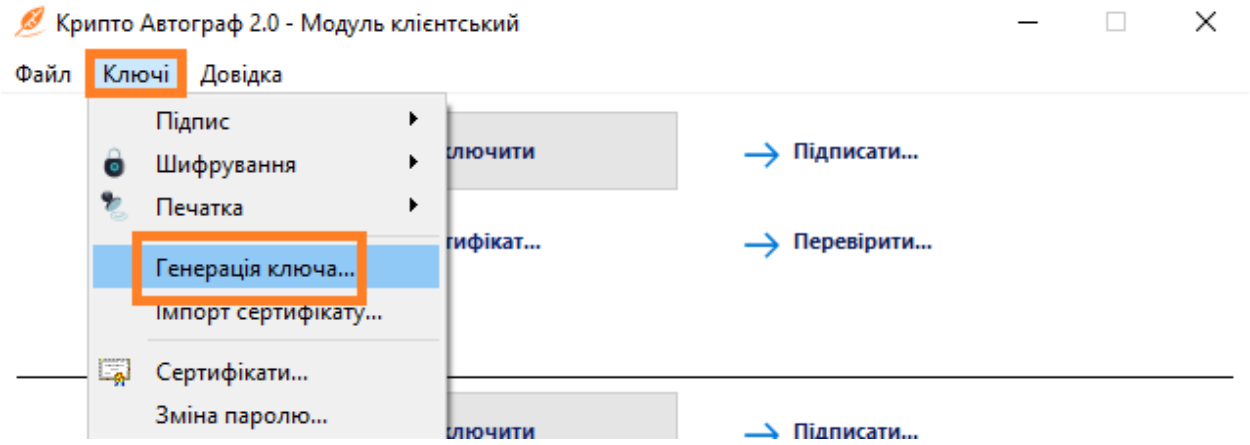
На «Робочому столі» ОС та в меню «Пуск» доступний ярлик для запуску встановленої клієнтської складової Засобу.

Запустіть програмне забезпечення використовуючи ярлик «Крипто Автограф 2.0 - Модуль клієнтський».



або


Запустивши програмне забезпечення використовуючи ярлик «Крипто Автограф 2.0 - Модуль клієнтський» відкриється вікно де необхідно обрати «Ключі» → «Генерація ключа».

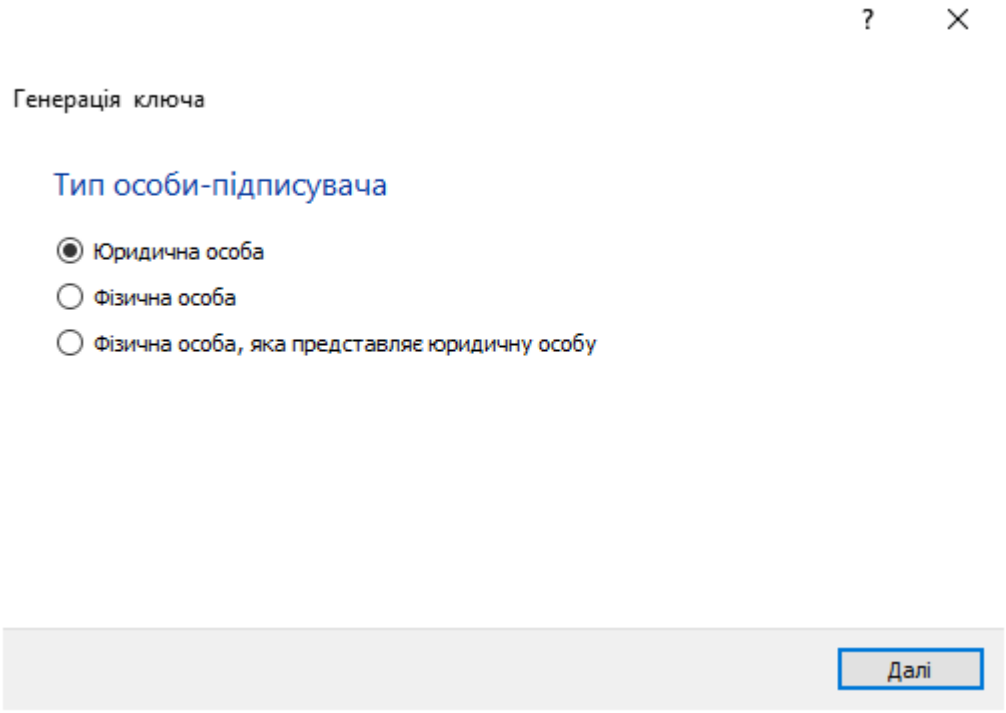


У вікні, яке відкрилося, необхідно обрати:

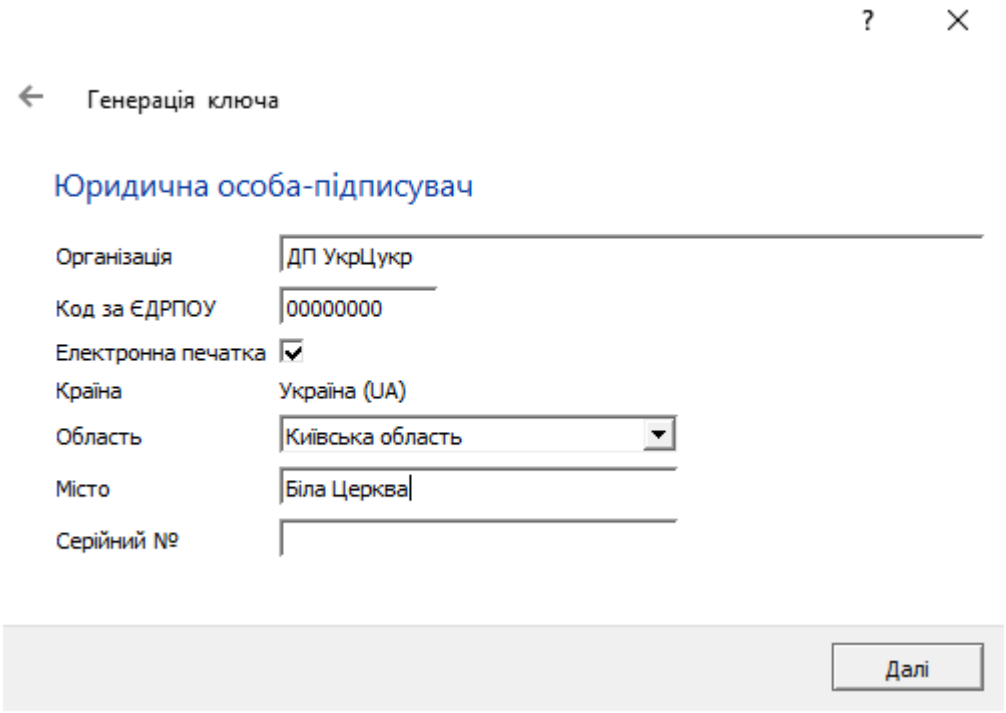
Юридична особа	Для формування сертифіката відкритого ключа електронного підпису (печатки) юридичної особи
Фізична особа	Для формування сертифіката відкритого ключа електронного підпису фізичної особи
Фізична особа, яка представляє юридичну особу	Для формування сертифіката відкритого ключа електронного

	підпису фізичної особи, що є працівником юридичної особи

Обираємо «Юридична особа» для формування криптографічних ключів та запиту на сертифікацію відкритого ключа в акредитованому центрі сертифікації ключів з метою отримання сертифіката відкритого ключа електронного підпису (печатки) або шифрування юридичної особи.



У вікні, що відкрилося необхідно вказати інформацію про юридичну особу.

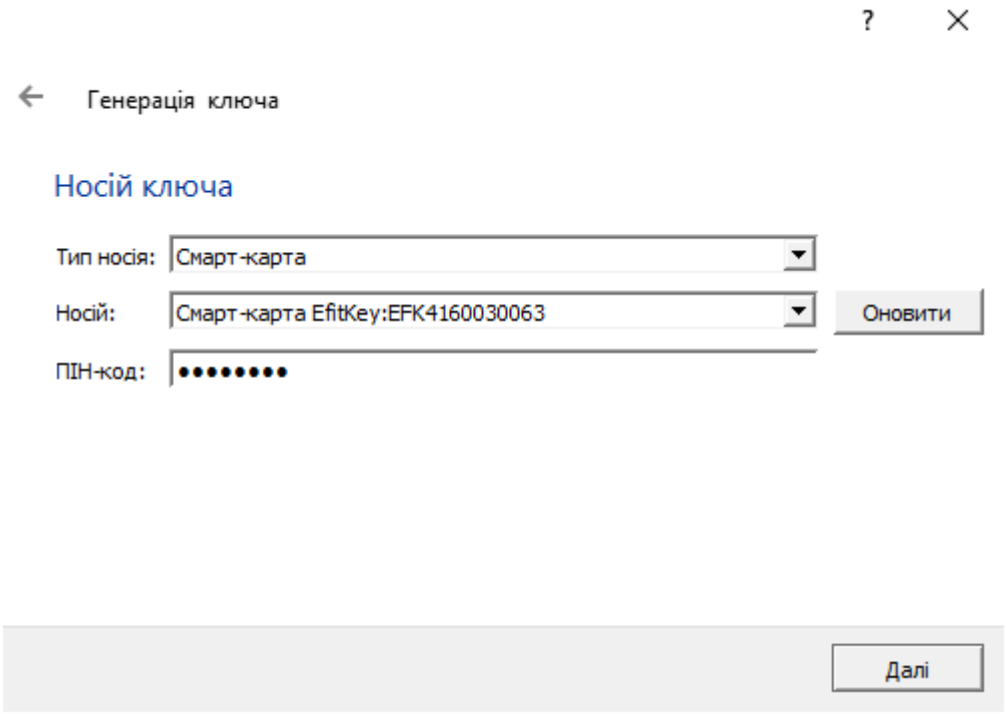


Важливо заповнювати інформацію відповідно до правил зазначених нижче:

ЗАГАЛЬНА ІНФОРМАЦІЯ	
ПОЛЕ	ЗНАЧЕННЯ ПОЛЯ
Організація	Повне (або офіційне скорочене) найменування організації - юридичної особи, за установчими документами (Статут) або відомостями про державну реєстрацію.
Код за ЄДРПОУ	Унікальний ідентифікаційний номер юридичної особи в Єдиному державному реєстрі підприємств та організацій України
Електронна печатка	Зробіть позначку в цьому полі, якщо бажаєте згенерувати електронну печатку

Область	Область, у якій зареєстрована організація - юридична особа. Примітка: Для міста Києва та Севастополя область не зазначається.
Місто	Місто, в якому зареєстрована організація - юридична особа.
Серійний №	Залиште поле незаповненим

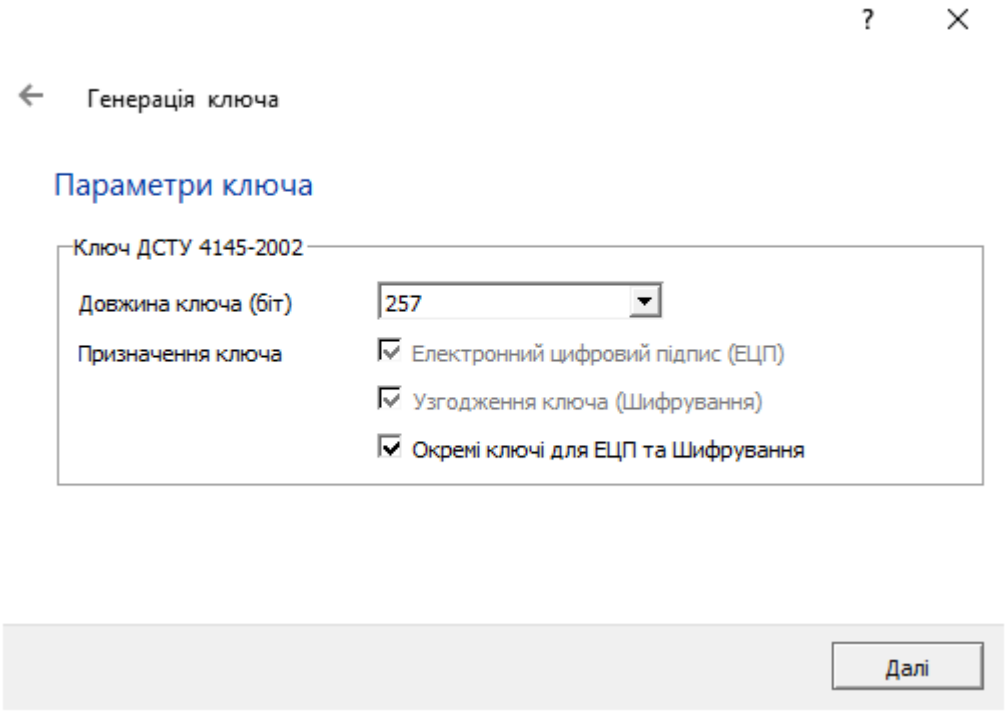
Заповнивши інформацію натисніть «Далі» та в наступному вікні оберіть тип носія для генерації ключа. В нашому випадку буде розглянуто генерацію на смарт-карту Efit Key (для цього оберіть смарт-карту у полі «Тип носія»). Після обрання типу носія, введіть ПІН-код смарт-карти та натисніть «Далі».



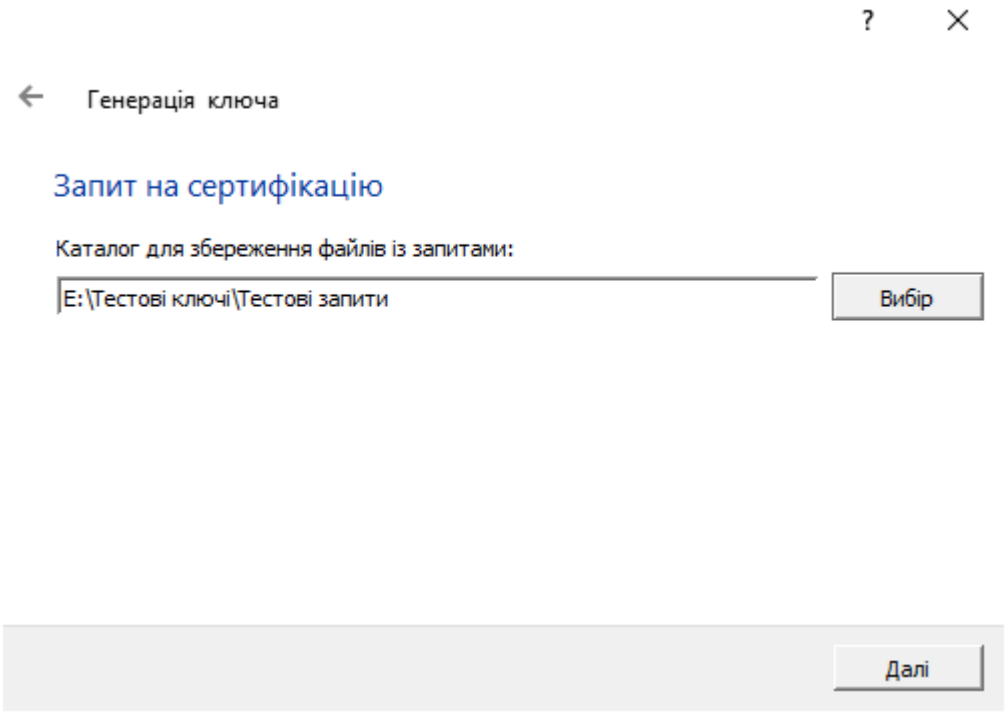
У вікні, що відкрилось оберіть довжину ключа та його призначення. Довжину рекомендуємо залишити за замовчуванням (257 біт). У розділі «Призначення ключа» оберіть необхідне для Вас призначення згідно з таблицею.

Призначення відкритого ключа:

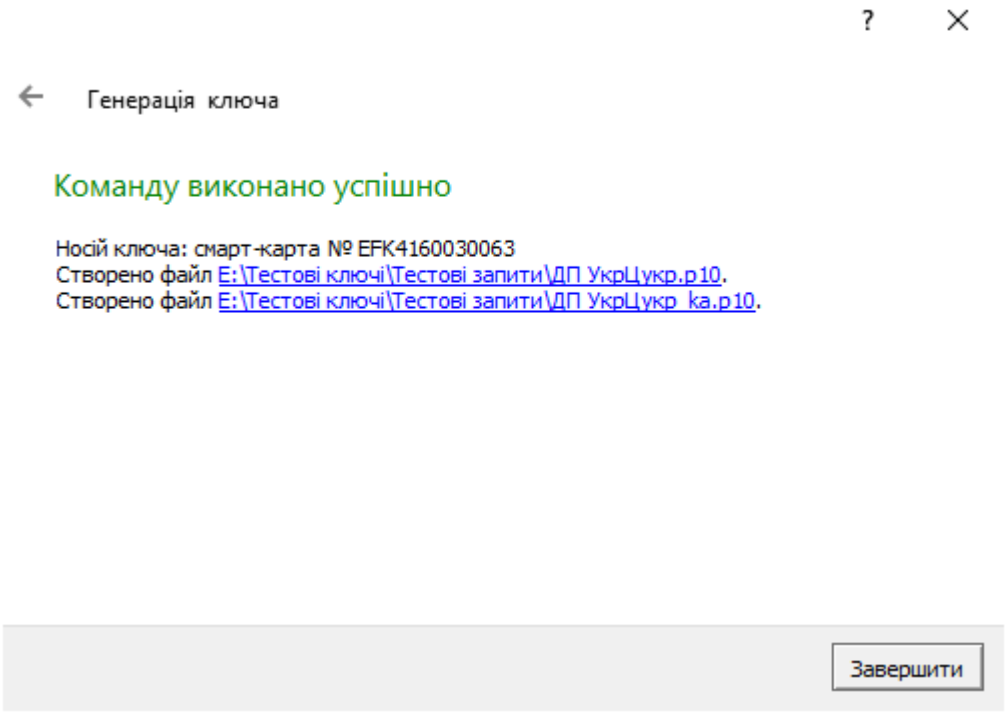
Електронний підпис	Електронний підпис або печатка. (генерується один ключ та один запит на сертифікат)
Узгодження ключа	Шифрування. (генерується один ключ та один запит на сертифікат)
Окремі ключі для ЕП та узгодження ключа	Окремі ключі для шифрування та ЕП (електронної печатки). (генерується два ключі та два запити на сертифікат)



В наступному вікні вкажіть шлях до каталогу, в який буде збережено файли запитів, натиснувши «Вибір». Після обрання каталогу натисніть «Далі».

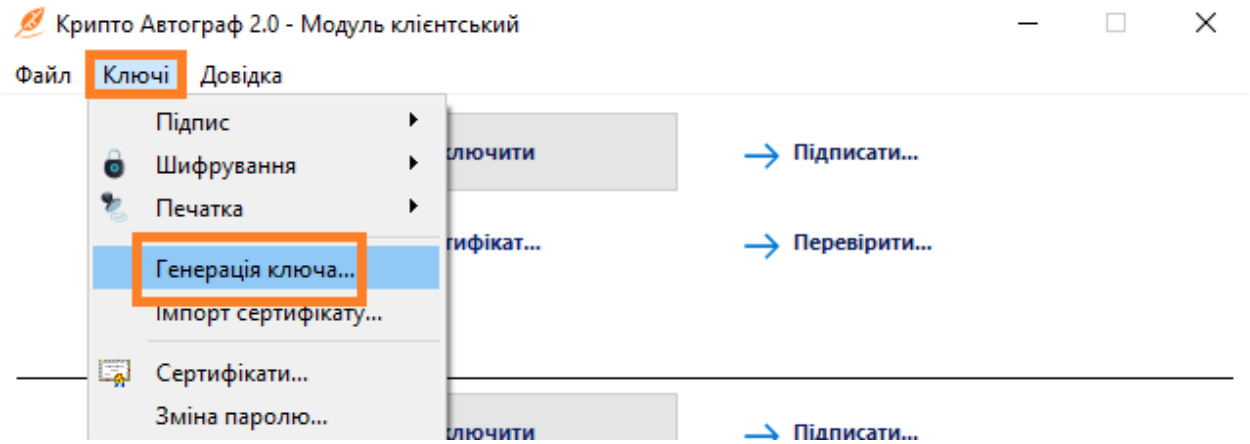


У вікні, що відкриється, зображено інформацію про завершення генерації ключа (ключів) та створення запиту (запитів) на сертифікат (сертифікати). Для продовження натисніть «Завершити».

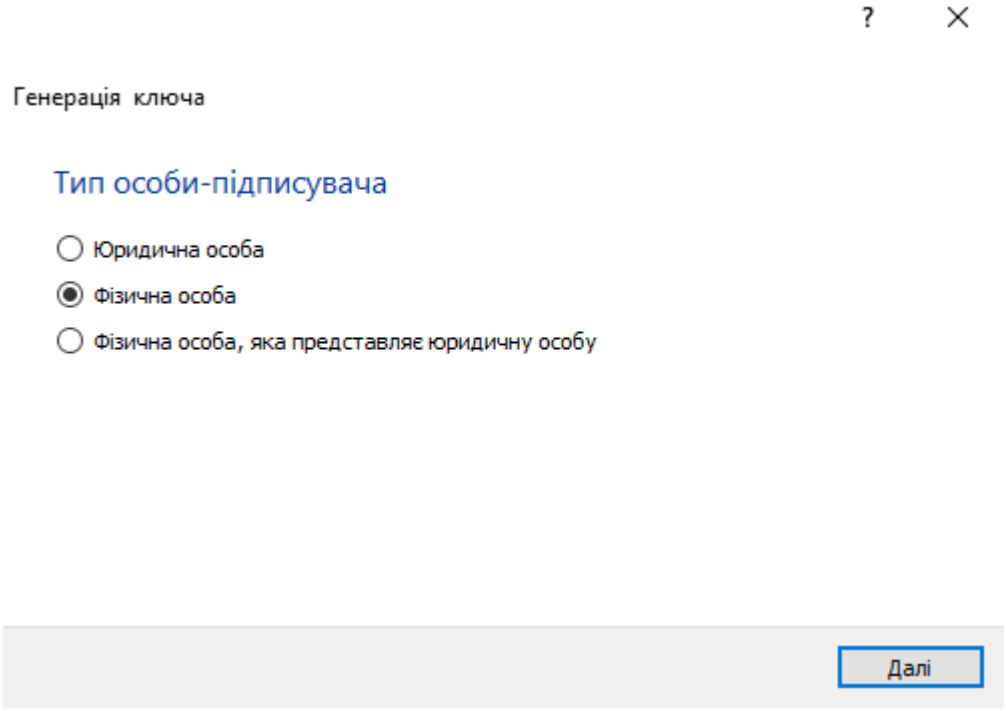


Формування запиту на сертифікат фізичної особи - підписувача

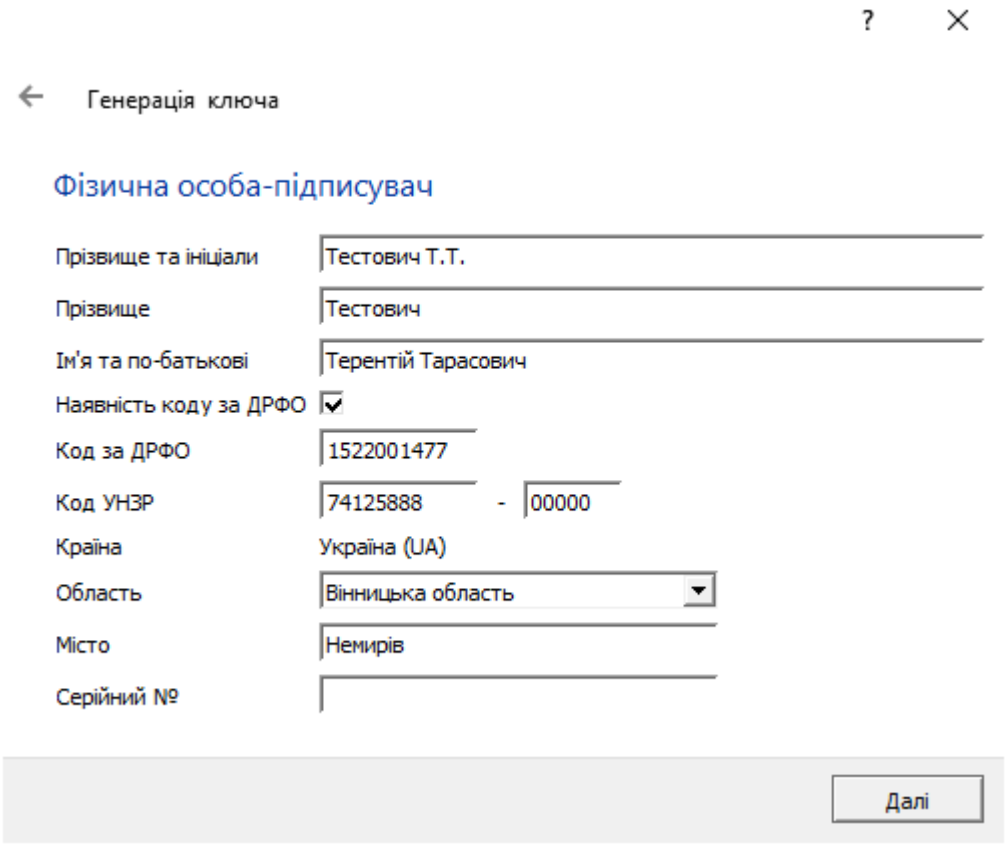
Запустивши програмне забезпечення використовуючи ярлик «Крипто Автограф 2.0 - Модуль клієнтський» відкриється вікно де необхідно обрати «Ключі» → «Генерація ключа».



Обираємо «Фізична особа» для формування криптографічних ключів та запиту на сертифікацію відкритого ключа в акредитованому центрі сертифікації ключів з метою отримання сертифіката відкритого ключа електронного підпису або шифрування фізичної особи.



У вікні, що відкрилося необхідно зазначити інформацію про фізичну особу.

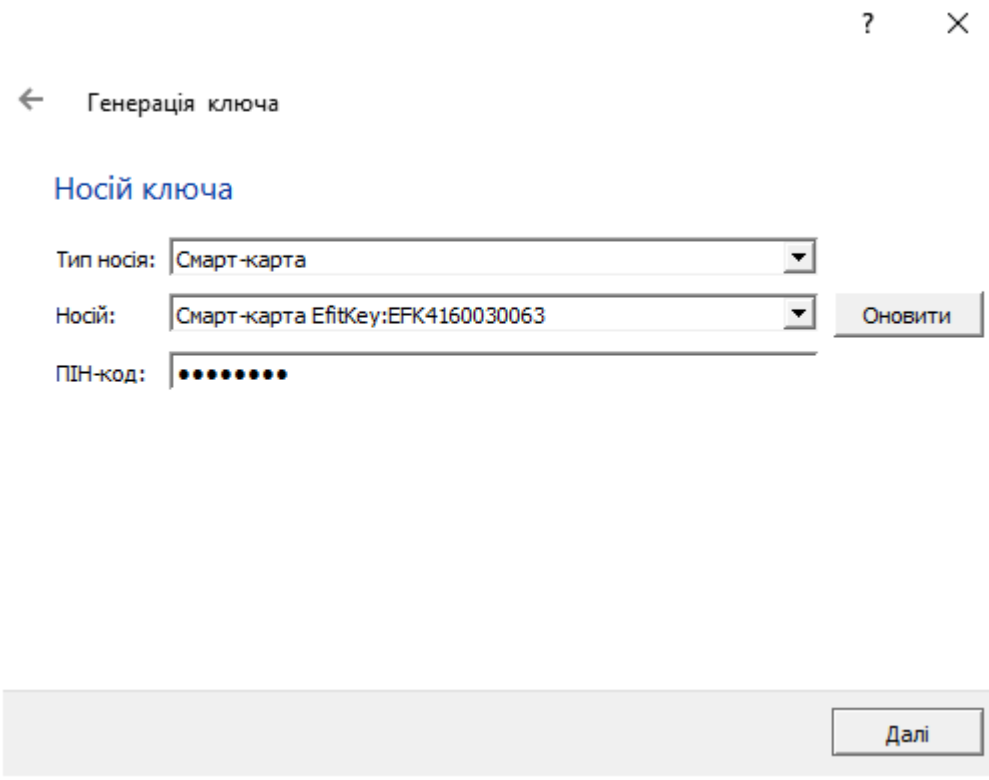


Важливо заповнювати інформацію відповідно до правил зазначених нижче:

ЗАГАЛЬНА ІНФОРМАЦІЯ	
ПОЛЕ	ЗНАЧЕННЯ ПОЛЯ
Прізвище та ініціали	Прізвище та ініціали фізичної особи – підписувача.
Прізвище	Прізвище підписувача за паспортними даними.
Ім’я та по батькові	Ім’я та по батькові підписувача за паспортними даними.
Наявність коду за ДРФО	Поставте позначку у разі наявності коду за ДРФО (РНОКПП)
Код за ДРФО	Код за ДРФО підписувача (реєстраційний номер облікової картки платника податків)

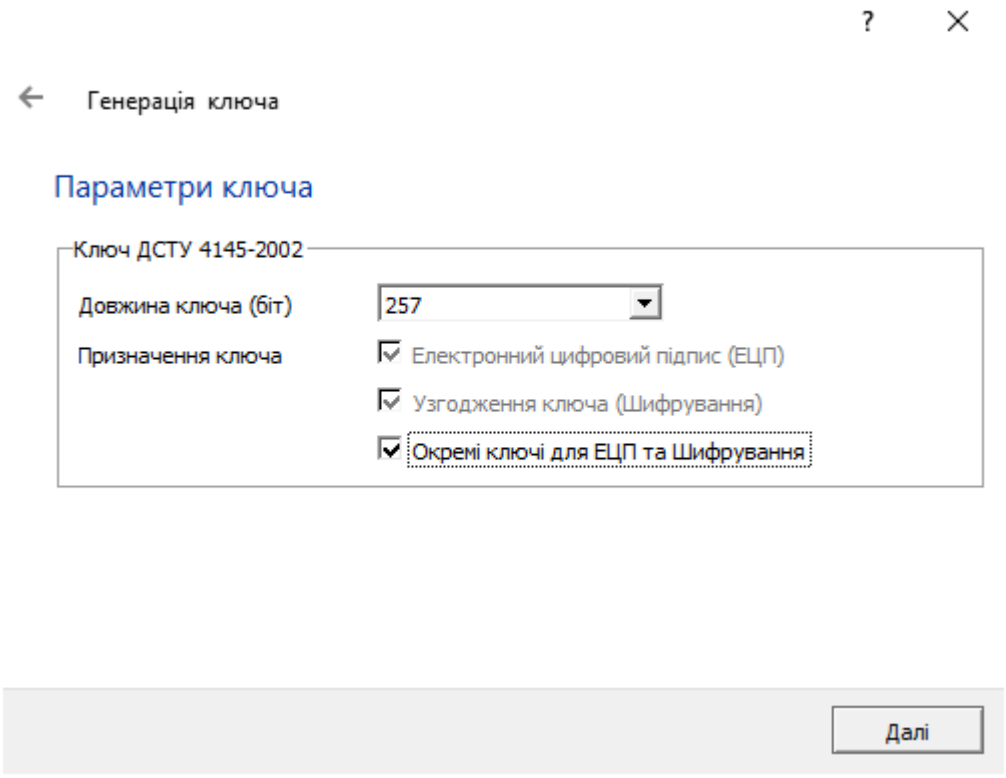
Код УНЗР	Унікальний номер запису в Єдиному державному демографічному реєстрі
Область:	Область, у якій зареєстрована фізична особа – підписувач. Примітка: Для міста Києва та Севастополя область не зазначається.
Місто:	Місто, в якому зареєстрована фізична особа – підписувач.
Серійний №	Залиште поле незаповненим

Заповнивши інформацію натисніть «Далі» та в наступному вікні оберіть тип носія для генерації ключа. В нашому випадку буде розглянуто генерацію на смарт-карту Efit Key. Після обрання типу носія, введіть ПІН-код смарт-карти та натисніть «Далі».

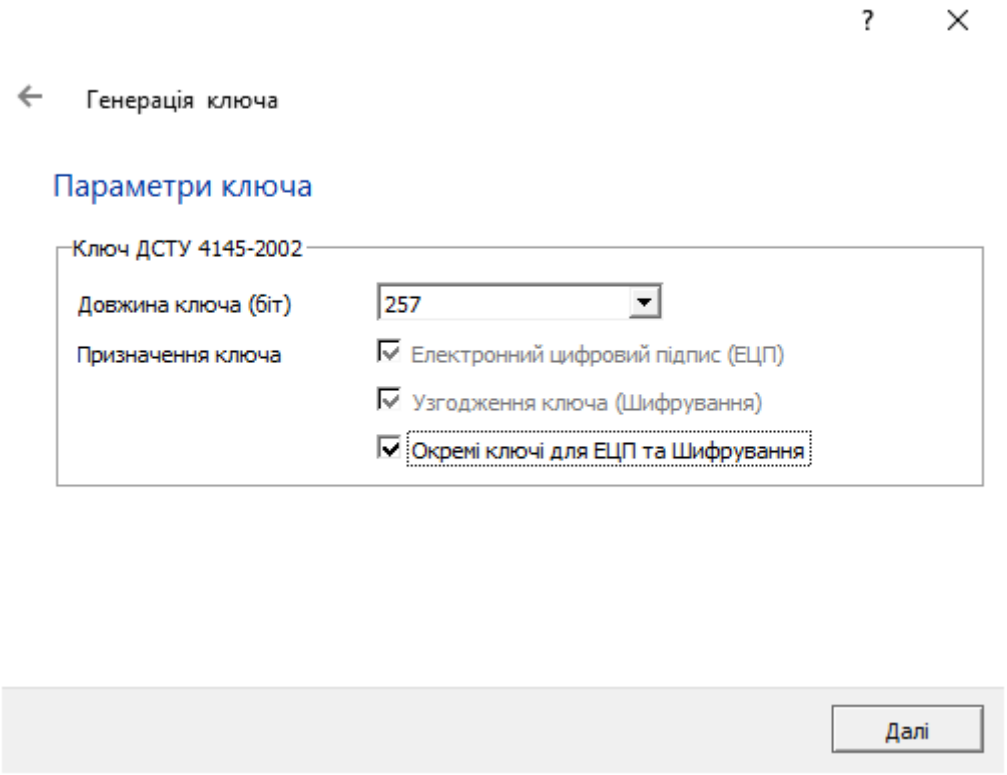


У вікні, що відкрилось оберіть довжину ключа та його призначення. Довжину рекомендуємо залишити за замовчуванням (257 біт). У розділі «Призначення ключа» оберіть необхідне для Вас призначення згідно з таблицею.

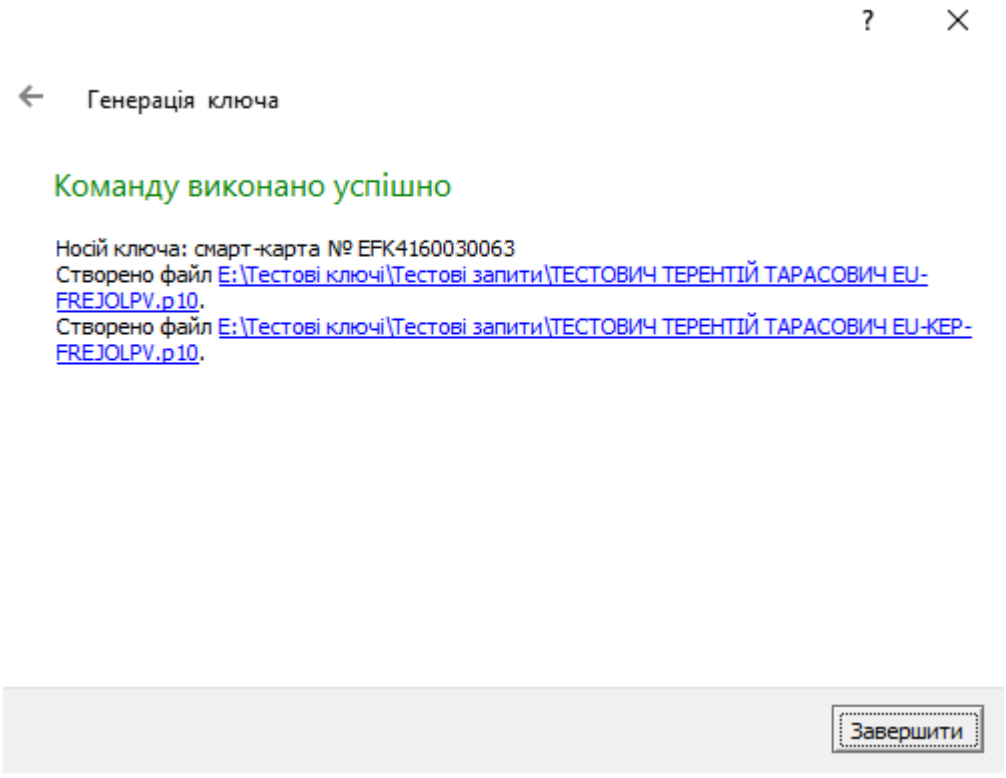
Призначення відкритого ключа:	
Електронний підпис	Електронний підпис або печатка. (генерується один ключ та один запит на сертифікат)
Узгодження ключа	Шифрування. (генерується один ключ та один запит на сертифікат)
Окремі ключі для ЕП та узгодження ключа	Окремі ключі для шифрування та ЕП (електронної печатки). (генерується два ключі та два запити на сертифікат)



В наступному вікні вкажіть шлях до каталогу, в який буде збережено файли запитів, натиснувши «Вибір». Після обрання каталогу натисніть «Далі».

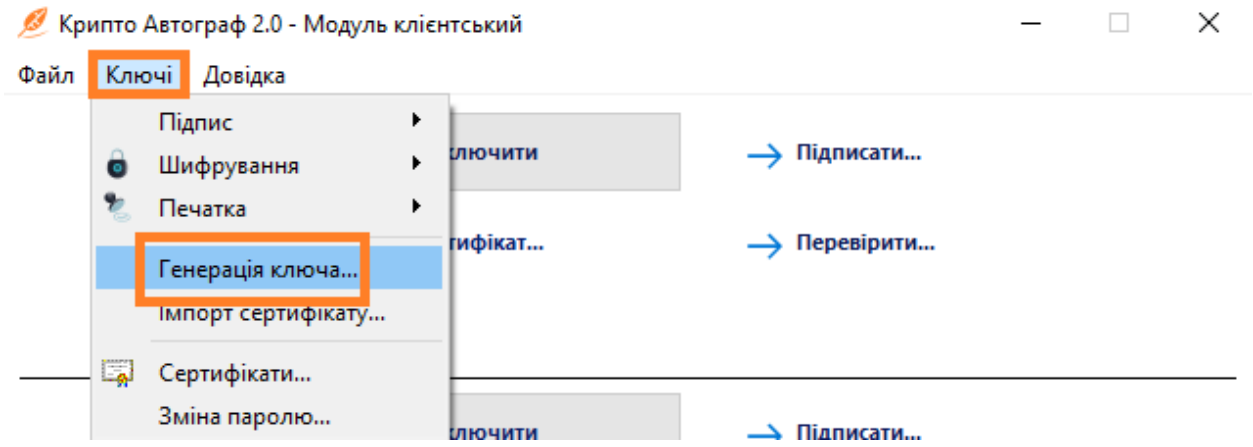


У вікні, що відкриється, зображено інформацію про завершення генерації ключа (ключів) та створення запиту (запитів) на сертифікат (сертифікати). Для продовження натисніть «Завершити».



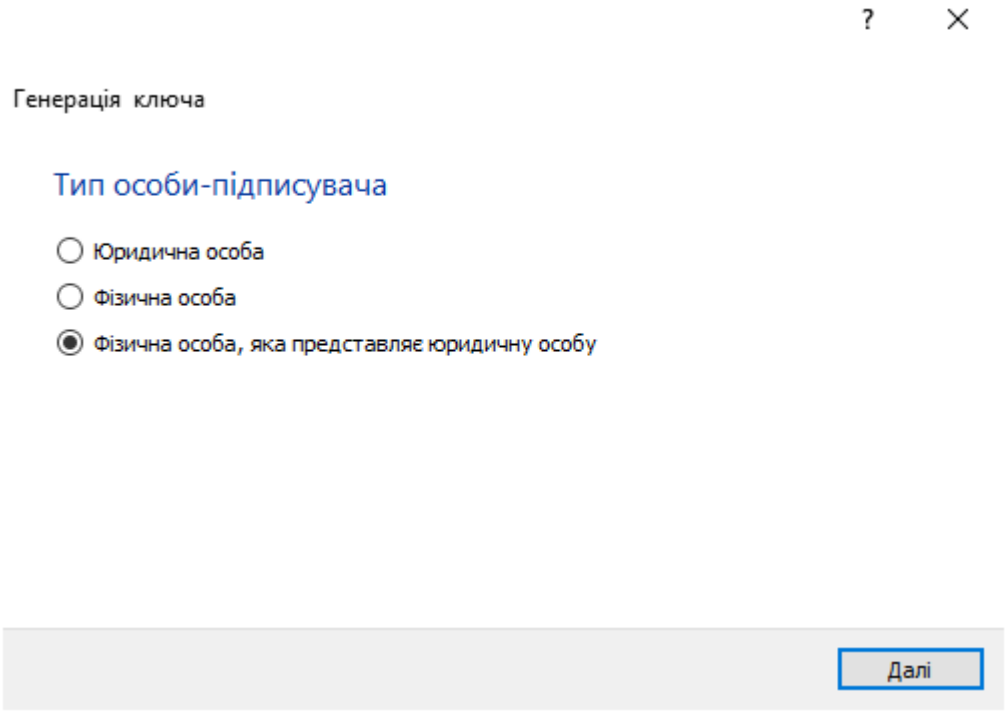
Формування запиту на сертифікат фізичної особи-підписувача, що є співробітником юридичної особи, або суб'єктом підприємницької діяльності

Запустивши програмне забезпечення використовуючи ярлик «Крипто Автограф 2.0 - Модуль клієнтський» відкриється вікно де необхідно обрати «Ключі» → «Генерація ключа».

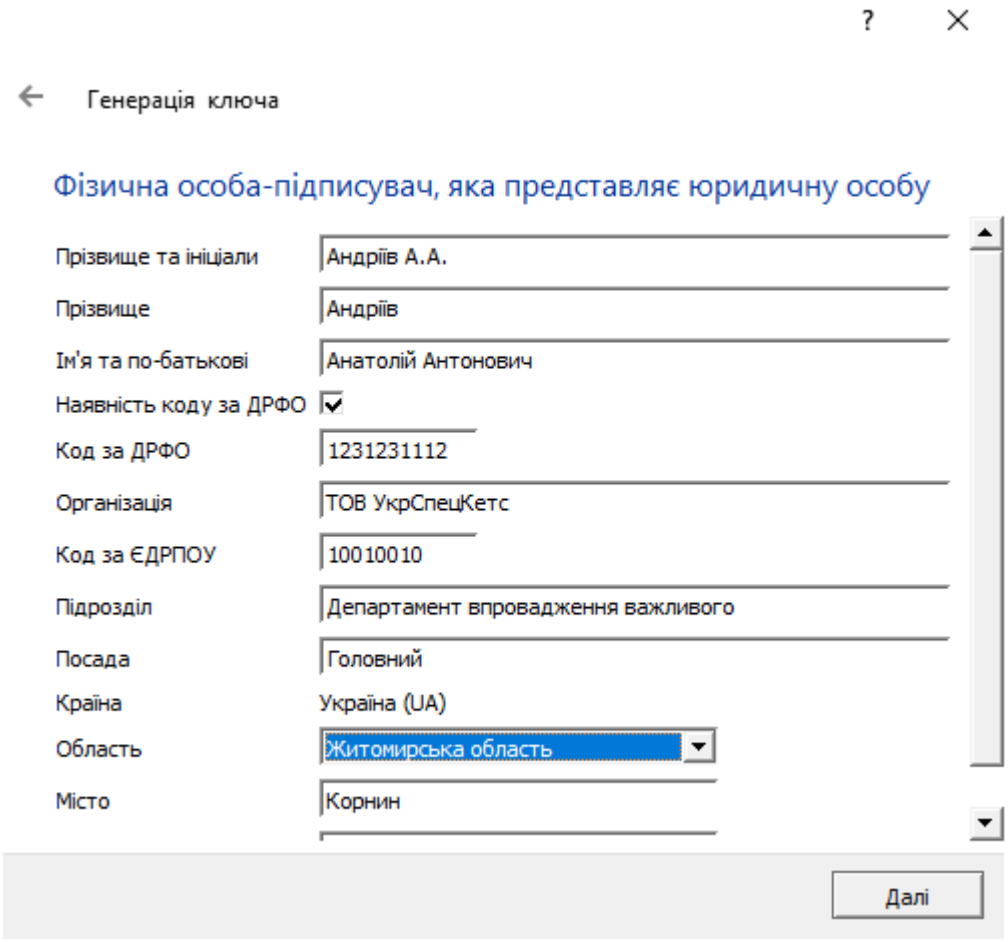


Обираємо «Фізична особа, яка представляє юридичну особу» для формування криптографічних ключів та запитів на сертифікацію відкритого ключа в акредитованому центрі сертифікації ключів з метою отримання сертифіката відкритого ключа електронного підпису або шифрування фізичної

особи, що є співробітником організації - юридичної особи, або фізичної особи, яка є суб’єктом підприємницької діяльності.



У вікні, що відкрилося необхідно зазначити інформацію про фізичну особу, що є співробітником організації - юридичної особи, або фізичної особи, яка є суб’єктом підприємницької діяльності.

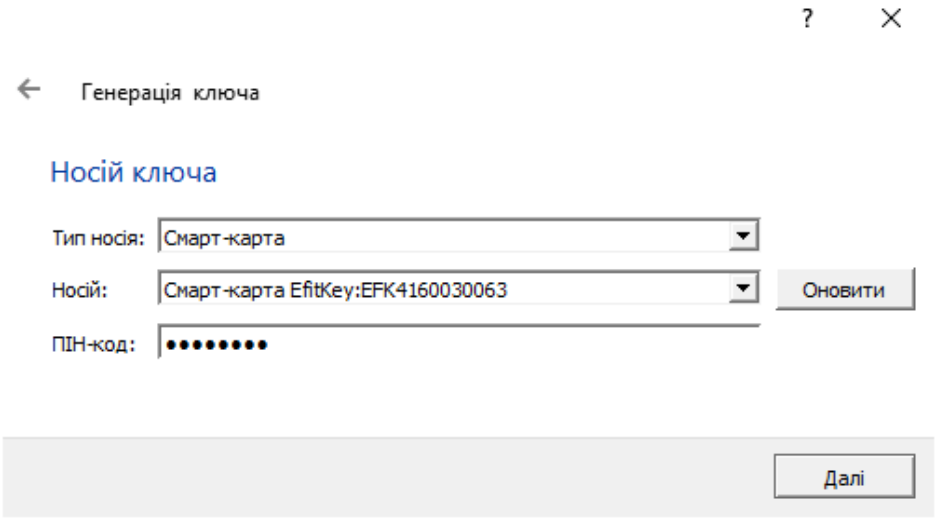


Важливо заповнювати інформацію відповідно до правил зазначених нижче:

ЗАГАЛЬНА ІНФОРМАЦІЯ	
ПОЛЕ	ЗНАЧЕННЯ ПОЛЯ
Прізвище та ініціали:	Прізвище та ініціали фізичної особи – підписувача.
Прізвище:	Прізвище підписувача за паспортними даними.
Ім’я та по батькові:	Ім’я та по батькові підписувача за паспортними даними.
Наявність коду за ДРФО	Поставте позначку у разі наявності коду за ДРФО (РНОКПП)

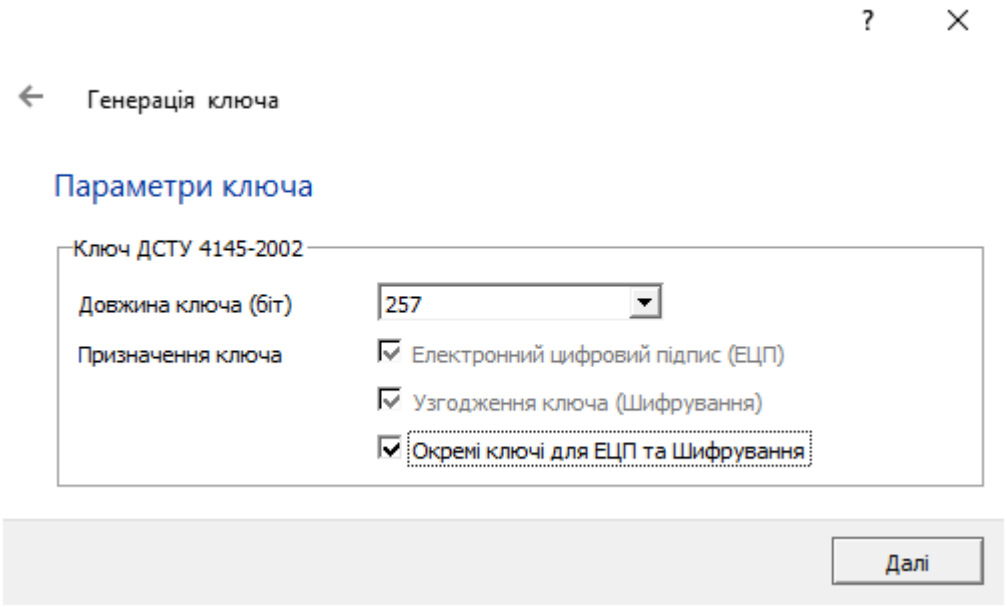
Код за ДРФО	Код за ДРФО підписувача (реєстраційний номер облікової картки платника податків)
Організація	Повне (або офіційне скорочене) найменування організації - юридичної особи, за установчими документами (Статут) або відомостями про державну реєстрацію.
Код за ЄДРПОУ	Унікальний ідентифікаційний номер юридичної особи в Єдиному державному реєстрі підприємств та організацій України
Підрозділ	Підрозділ організації, згідно установчих документів, в якому працює фізична особа, що представляє юридичну особу
Посада	Посада в підрозділі, яку займає фізична особа, що представляє юридичну особу
Область:	Область, у якій зареєстрована організація, яка пов’язана з фізичною особою –підписувачем. Примітка: Для міста Києва та Севастополя область не зазначається.
Місто:	Місто, в якому зареєстрована організація, яка пов’язана з фізичною особою- підписувачем.
Серійний №	Залиште поле незаповненим

Заповнивши інформацію натисніть «Далі» та в наступному вікні оберіть тип носія для генерації ключа. В нашому випадку буде розглянуто генерацію на смарт-карту Efit Key. Після обрання типу носія, введіть ПІН-код смарт-карти та натисніть «Далі».

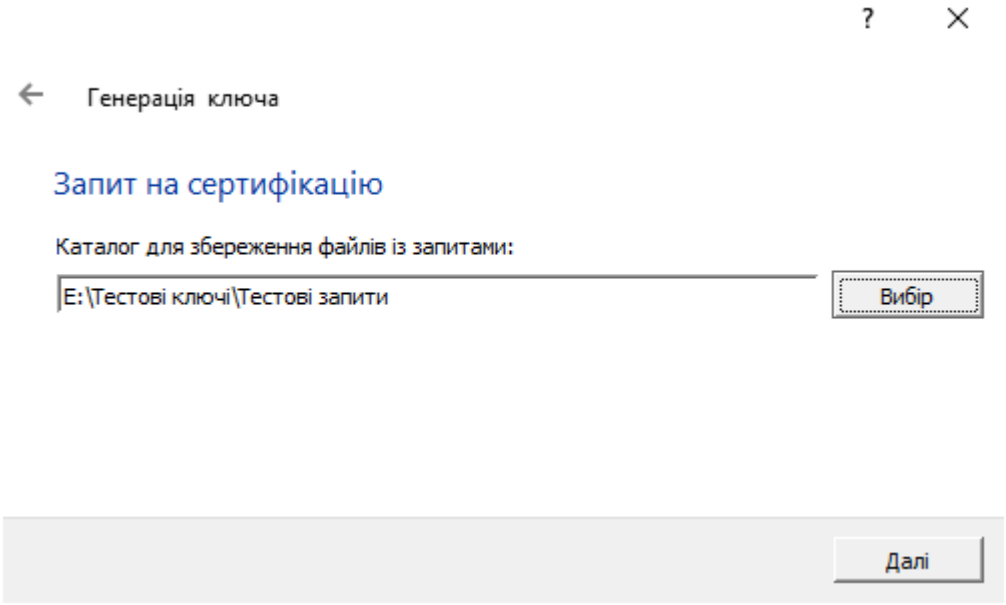


У вікні, що відкрилось оберіть довжину ключа та його призначення. Довжину рекомендуємо залишити за замовчуванням (257 біт). У розділі «Призначення ключа» оберіть необхідне для Вас призначення згідно з таблицею.

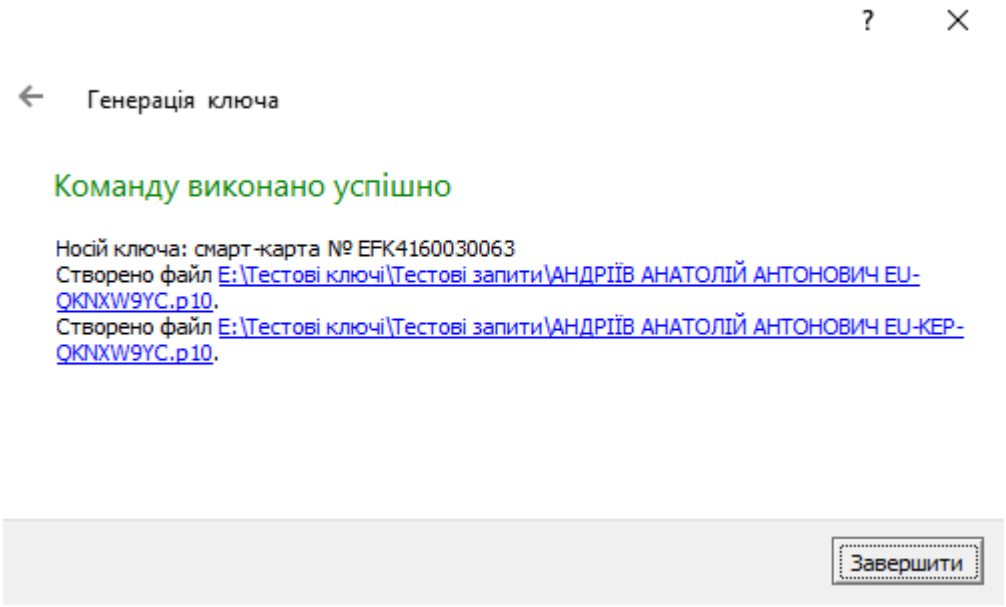
Призначення відкритого ключа:	
Електронний підпис	Електронний підпис або печатка. (генерується один ключ та один запит на сертифікат)
Узгодження ключа	Шифрування. (генерується один ключ та один запит на сертифікат)
Окремі ключі для ЕП та узгодження ключа	Окремі ключі для шифрування та ЕП (електронної печатки). (генерується два ключі та два запити на сертифікат)



В наступному вікні вкажіть шлях до каталогу, в який буде збережено файли запитів, натиснувши «Вибір». Після обрання каталогу натисніть «Далі».



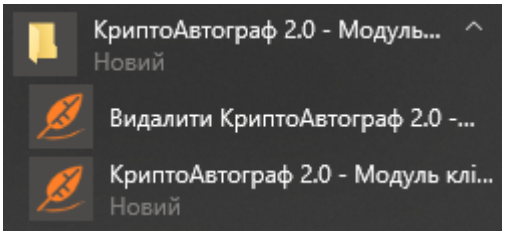
У вікні, що відкриється, зображено інформацію про завершення генерації ключа (ключів) та створення запиту (запитів) на сертифікат (сертифікати). Для продовження натисніть «Завершити».

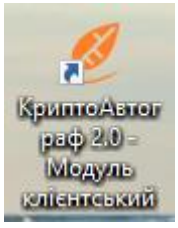


Формування запиту на сертифікат у файловий носій
Формування запиту на сертифікат юридичної особи - підписувача

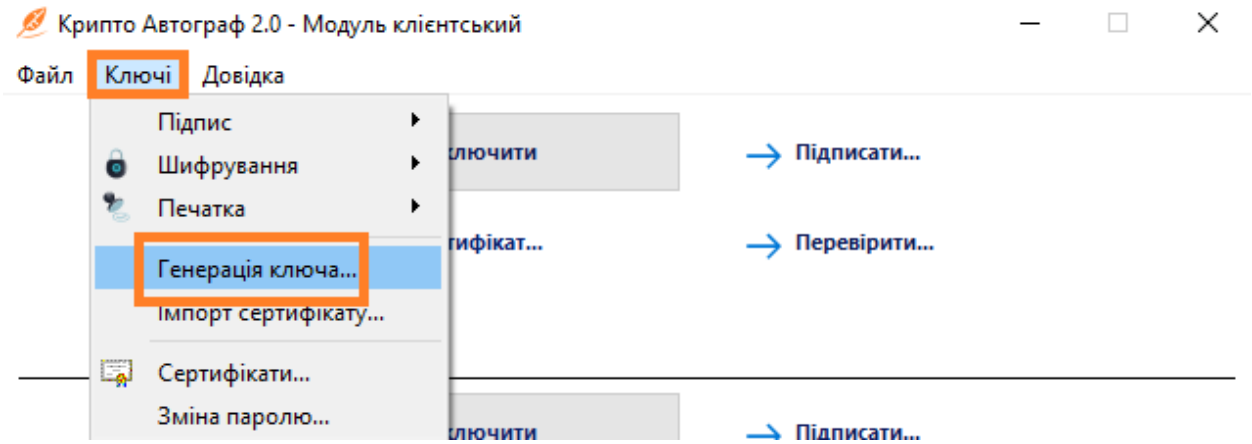
На «Робочому столі» ОС та в меню «Пуск» доступний ярлик для запуску встановленої клієнтської складової Засобу.

Запустіть програмне забезпечення використовуючи ярлик «Крипто Автограф 2.0 - Модуль клієнтський».



або


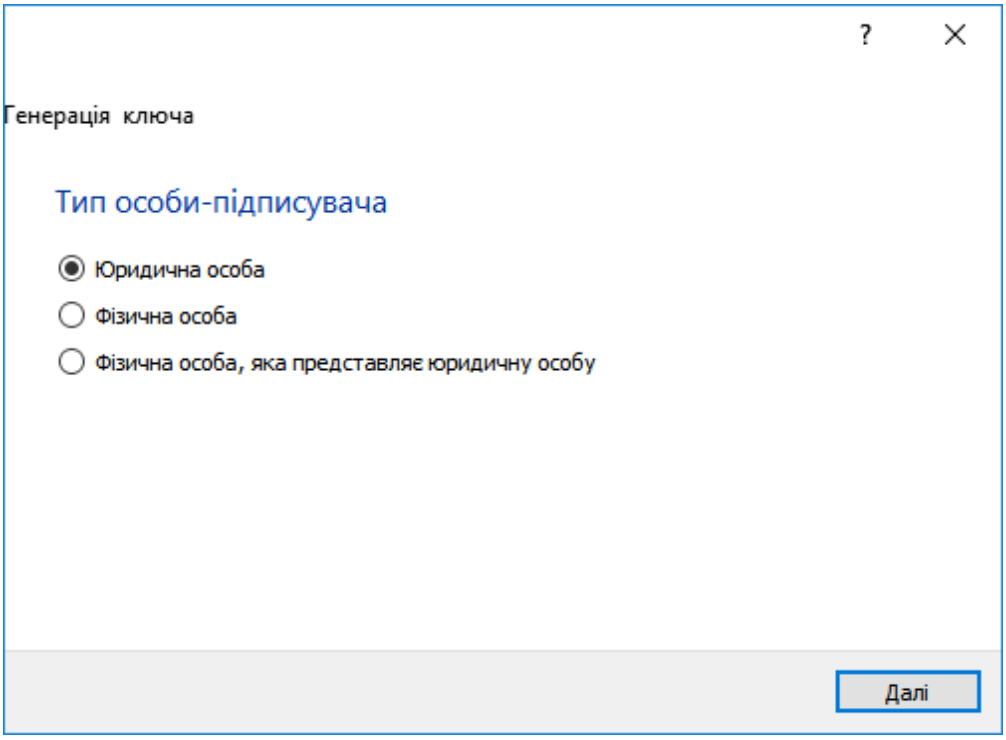
Запустивши програмне забезпечення використовуючи ярлик «Крипто Автограф 2.0 - Модуль клієнтський» відкриється вікно де необхідно обрати «Ключі» → «Генерація ключа».



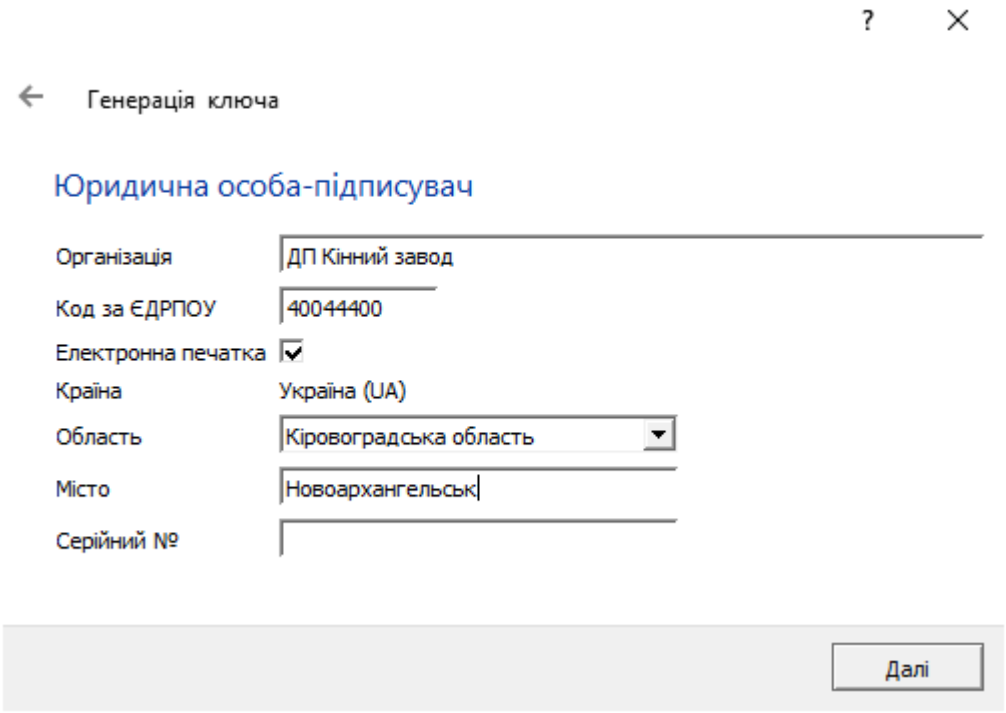
У вікні яке відкрилося необхідно обрати:

Юридична особа	Для формування сертифіката відкритого ключа електронного підпису (печатки) юридичної особи
Фізична особа	Для формування сертифіката відкритого ключа електронного підпису фізичної особи
Фізична особа, яка представляє юридичну особу	Для формування сертифіката відкритого ключа електронного підпису фізичної особи, що є працівником юридичної особи

Обираємо «Юридична особа» для формування криптографічних ключів та запиту на сертифікацію відкритого ключа в акредитованому центрі сертифікації ключів з метою отримання сертифіката відкритого ключа електронного підпису (печатки) або шифрування юридичної особи.



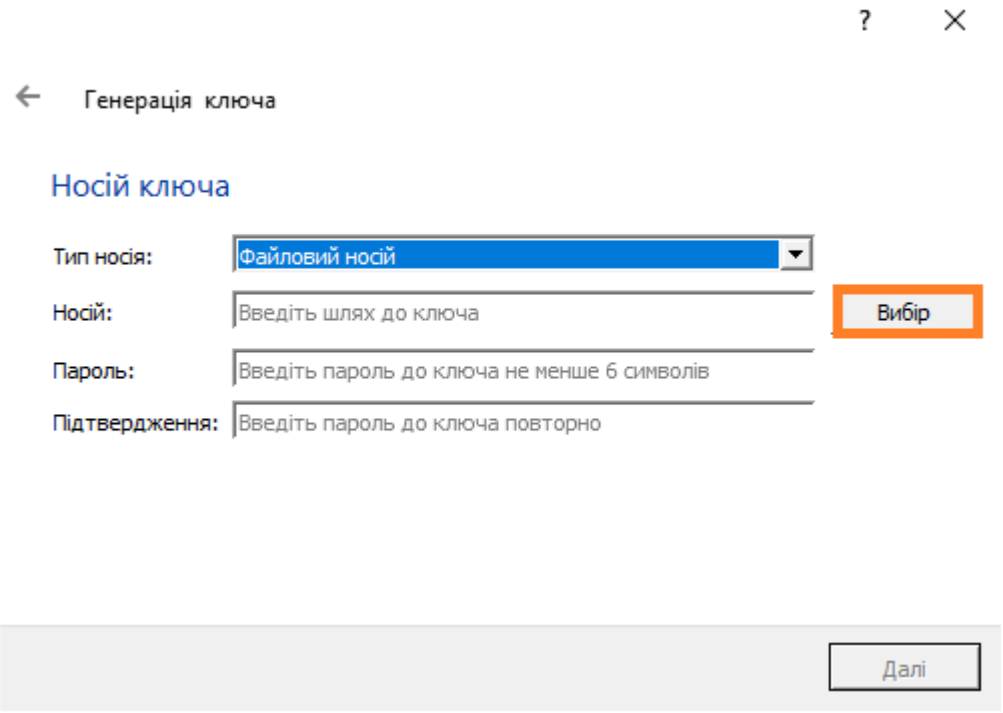
У вікні, що відкрилося необхідно зазначити інформацію про юридичну особу.



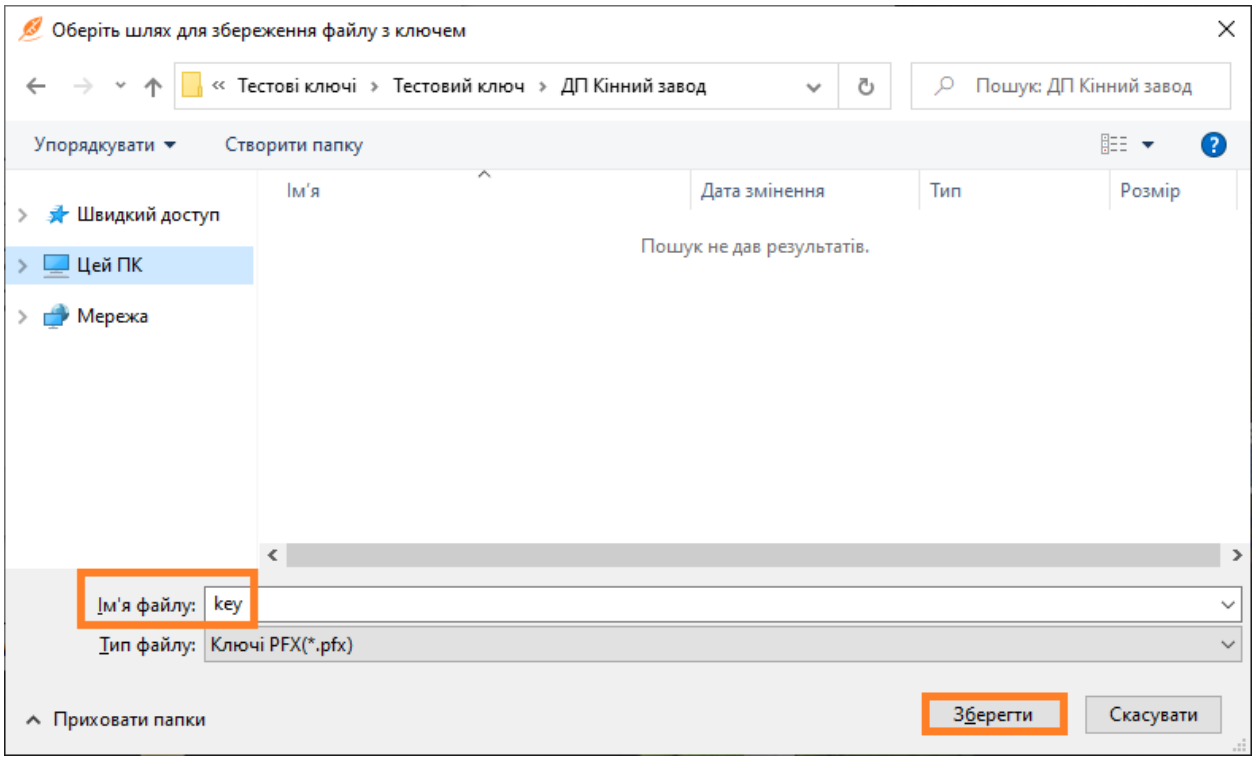
Важливо заповнювати інформацію відповідно до правил зазначених нижче:

ЗАГАЛЬНА ІНФОРМАЦІЯ	
ПОЛЕ	ЗНАЧЕННЯ ПОЛЯ
Організація	Повне (або офіційне скорочене) найменування організації - юридичної особи, за установчими документами (Статут) або відомостями про державну реєстрацію.
Код за ЄДРПОУ	Унікальний ідентифікаційний номер юридичної особи в Єдиному державному реєстрі підприємств та організацій України
Електронна печатка	Зробіть позначку в цьому полі, якщо бажаєте згенерувати електронну печатку
Область	Область, у якій зареєстрована організація - юридична особа. Примітка: Для міста Києва та Севастополя область не зазначається.
Місто	Місто, в якому зареєстрована організація - юридична особа.
Серійний №	Залиште поле незаповненим

Заповнивши інформацію натисніть «Далі» та в наступному вікні оберіть тип носія для генерації ключа. За замовчуванням буде обрано «Файловий носій», залиште цей вибір без змін. Після цього натисніть «Вибір» для обрання каталогу в який буде збережено ключ.

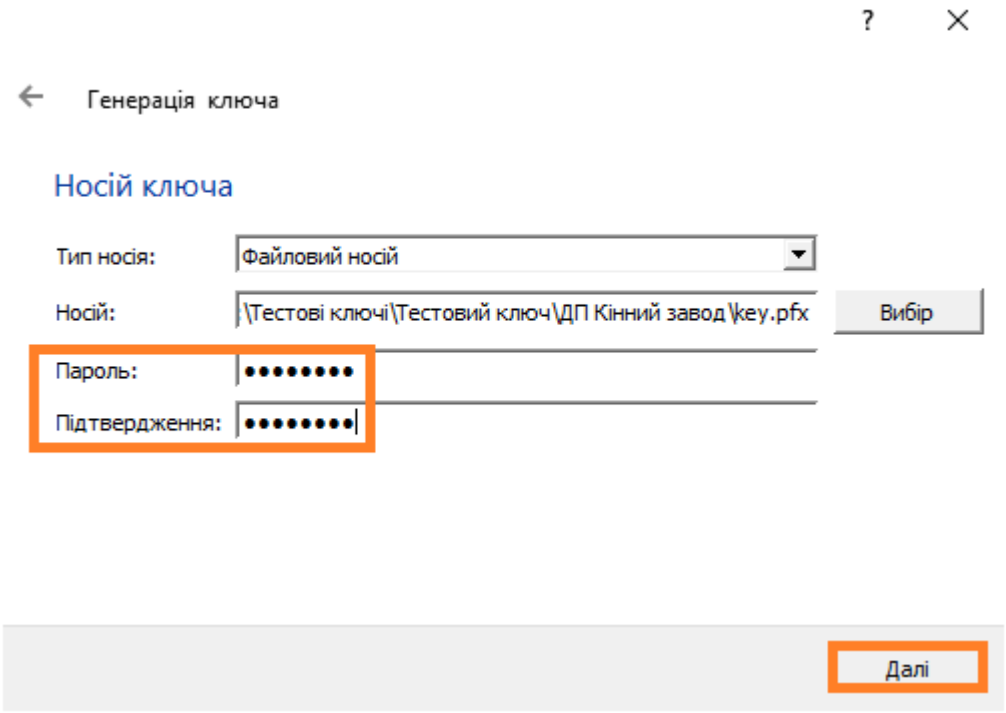


У вікні вибору каталогу для ключа також введіть ім’я файлу ключа та натисніть «Зберегти».



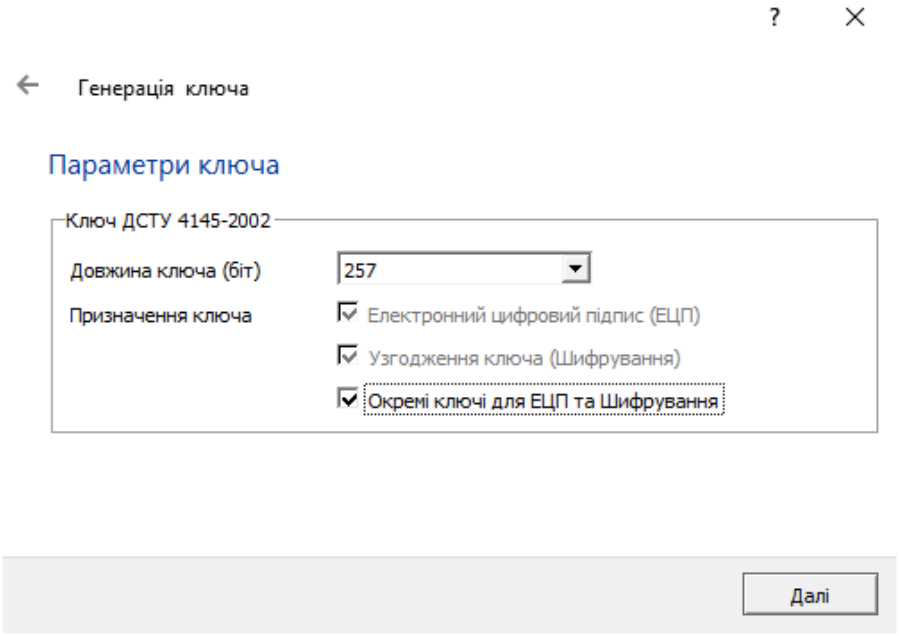
Далі введіть пароль (ПІН-код до ключа), введіть підтвердження паролю і натисніть «Далі». **Довжина ПІН-коду має бути не менше шести символів.**

Під час введення паролю зверніть увагу на те якою мовою вводите пароль і чи не включений у Вас «Caps Lock».

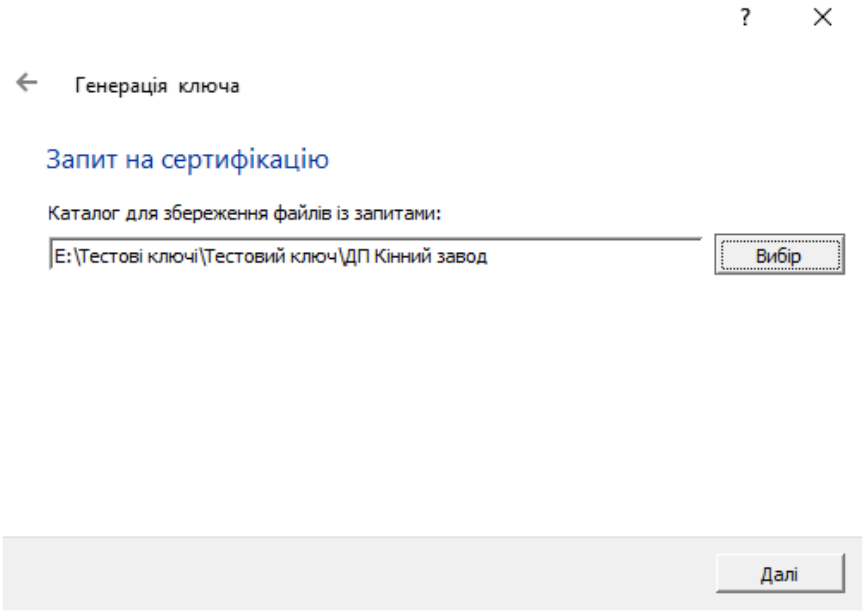


У вікні, що відкрилось оберіть довжину ключа та його призначення. Довжину рекомендуємо залишити за замовчуванням (257 біт). У розділі «Призначення ключа» оберіть необхідне для Вас призначення згідно з таблицею.

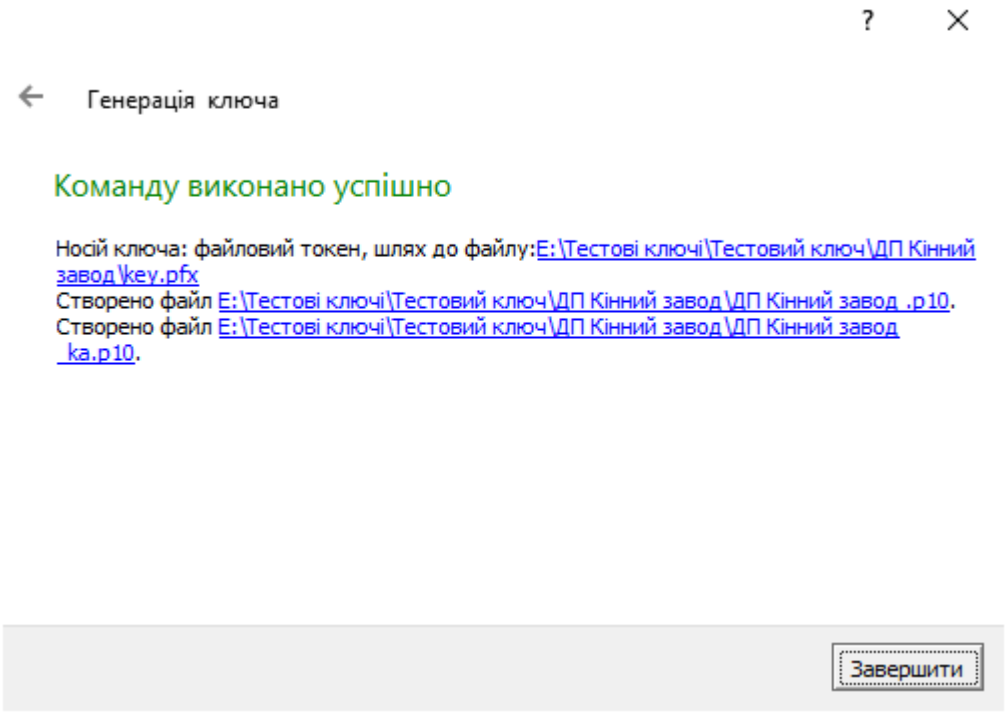
Призначення відкритого ключа:	
Електронний підпис	Електронний підпис або печатка. (генерується один ключ та один запит на сертифікат)
Узгодження ключа	Шифрування. (генерується один ключ та один запит на сертифікат)
Окремі ключі для ЕП та узгодження ключа	Окремі ключі для шифрування та ЕП (електронної печатки). (генерується два ключі та два запити на сертифікат)



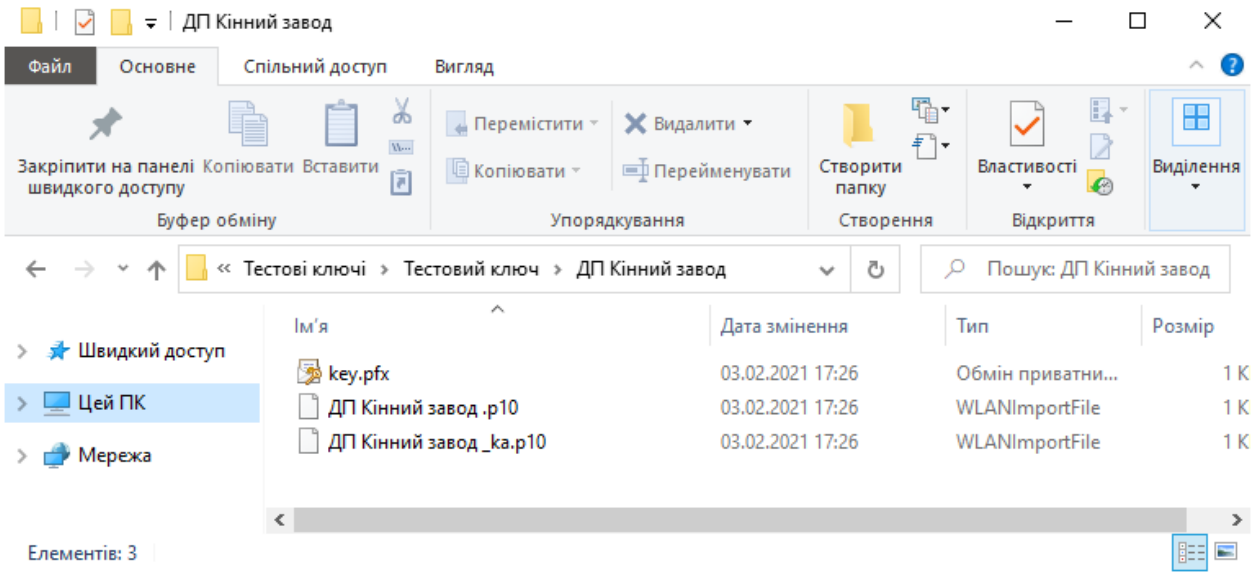
В наступному вікні вкажіть шлях до каталогу, в який буде збережено файли запитів, натиснувши «Вибір». Після обрання каталогу натисніть «Далі».



У вікні, що відкриється, зображено інформацію про завершення генерації ключа (ключів) та створення запиту (запитів) на сертифікат (сертифікати). Для продовження натисніть «Завершити».

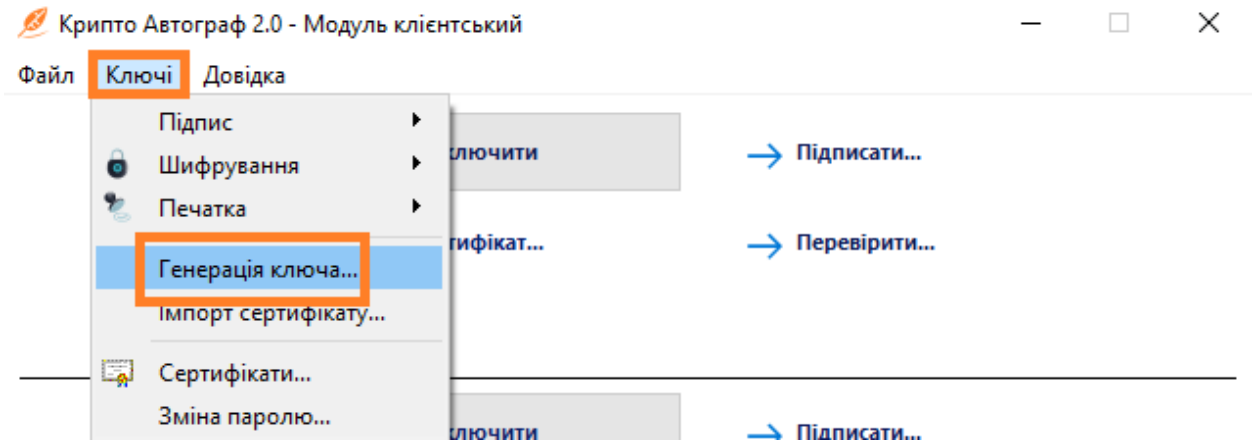


Нижче зображено згенерований ключ (у форматі .pfx) та два запити на сертифікат.

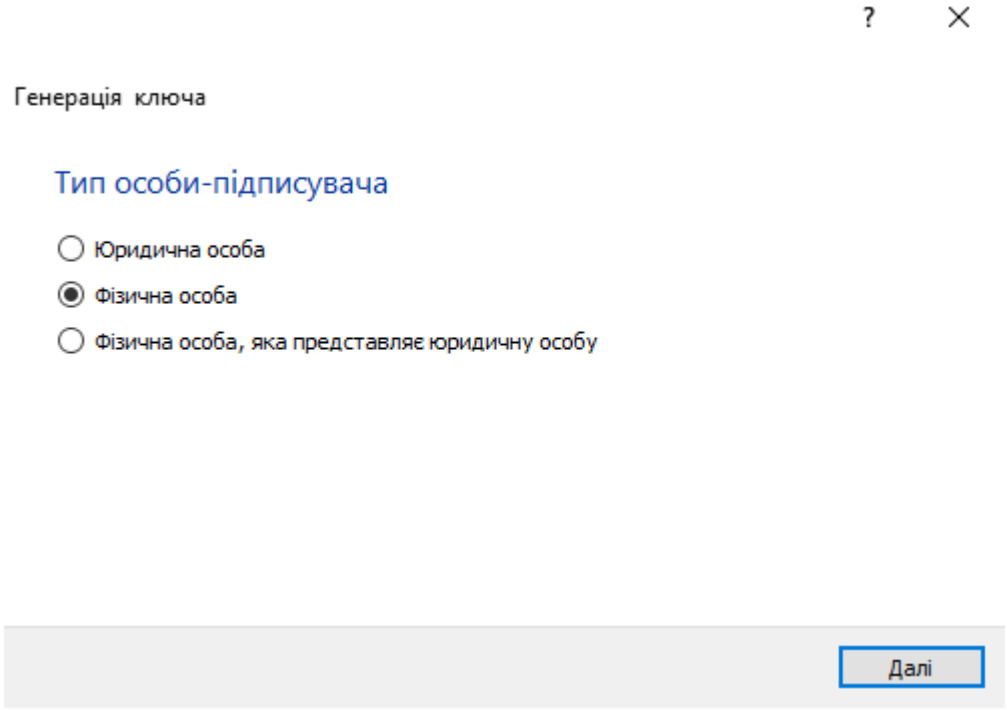


Формування запиту на сертифікат фізичної особи - підписувача

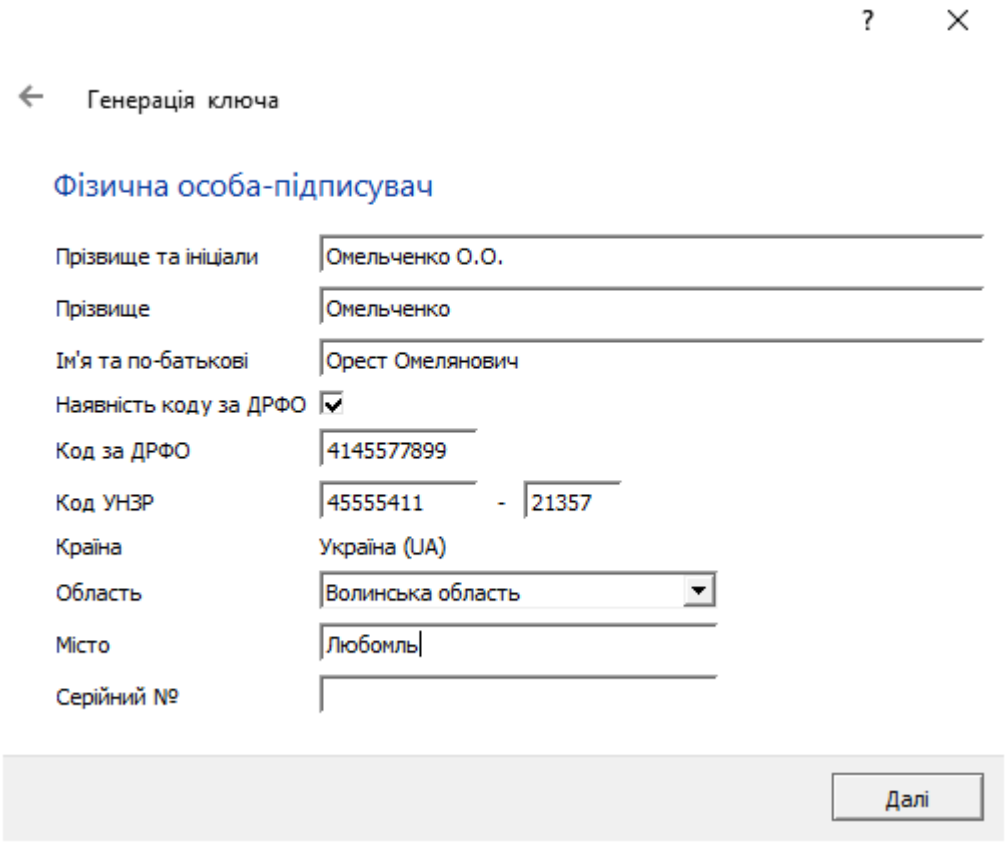
Запустивши програмне забезпечення використовуючи ярлик «КриптоАвтограф 2.0 - Модуль клієнтський» відкриється вікно де необхідно обрати «Ключі» → «Генерація ключа».



Обираємо «Фізична особа» для формування криптографічних ключів та запиту на сертифікацію відкритого ключа в акредитованому центрі сертифікації ключів з метою отримання сертифіката відкритого ключа електронного підпису або шифрування фізичної особи.



У вікні, що відкрилося необхідно зазначити інформацію про фізичну особу.

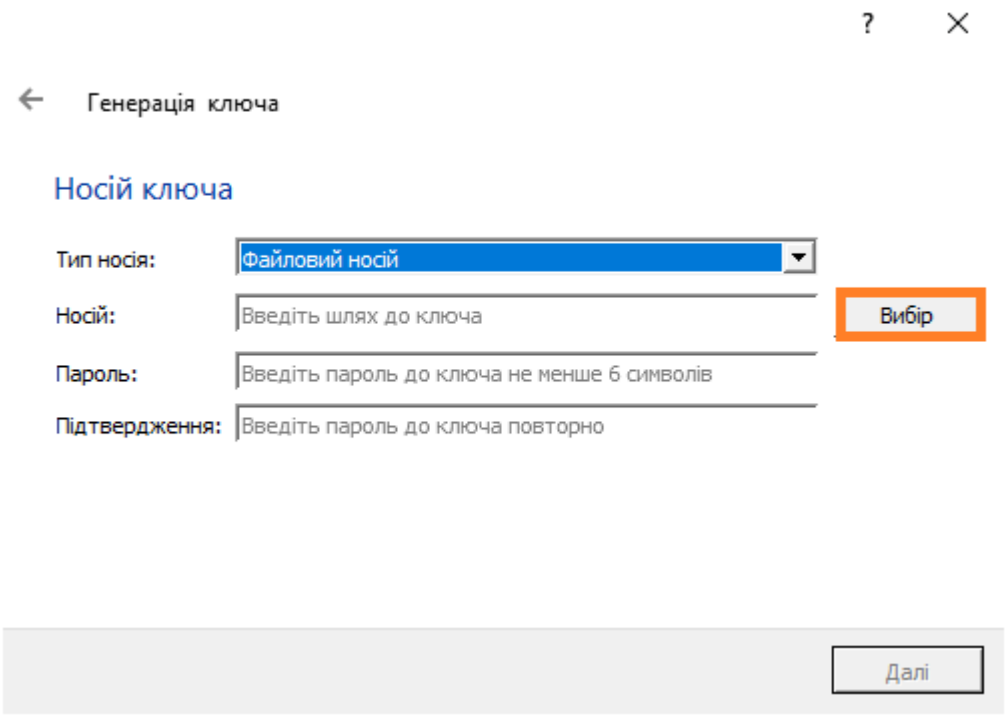


Важливо заповнювати інформацію відповідно до правил зазначених нижче:

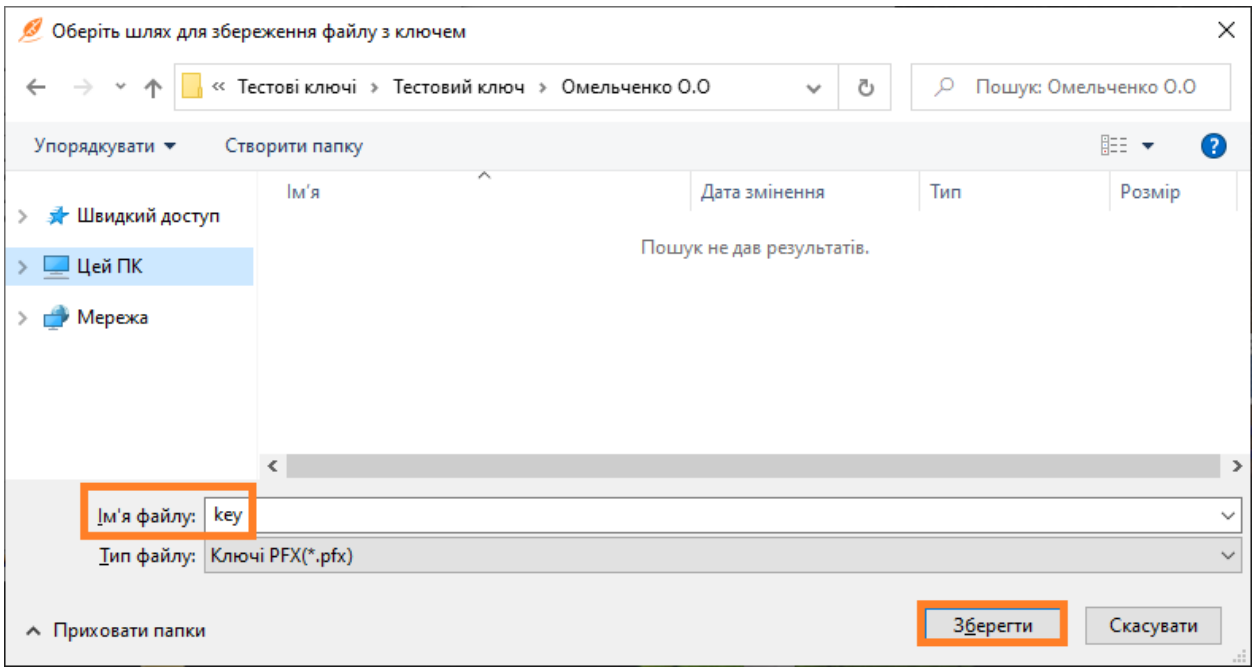
ЗАГАЛЬНА ІНФОРМАЦІЯ	
ПОЛЕ	ЗНАЧЕННЯ ПОЛЯ
Прізвище та ініціали	Прізвище та ініціали фізичної особи – підписувача.
Прізвище	Прізвище підписувача за паспортними даними.
Ім’я та по батькові	Ім’я та по батькові підписувача за паспортними даними.
Наявність коду за ДРФО	Поставте позначку у разі наявності коду за ДРФО (РНОКПП)
Код за ДРФО	Код за ДРФО підписувача (реєстраційний номер облікової картки платника податків)

Код УНЗР	Унікальний номер запису в Єдиному державному демографічному реєстрі
Область:	Область, у якій зареєстрована фізична особа – підписувач. Примітка: Для міста Києва та Севастополя область не зазначається.
Місто:	Місто, в якому зареєстрована фізична особа – підписувач.
Серійний №	Залиште поле незаповненим

Заповнивши інформацію натисніть «Далі» та в наступному вікні оберіть тип носія для генерації ключа. За замовчуванням буде обрано «Файловий носій», залиште цей вибір без змін. Після цього натисніть «Вибір» для обрання каталогу в який буде збережено ключ.

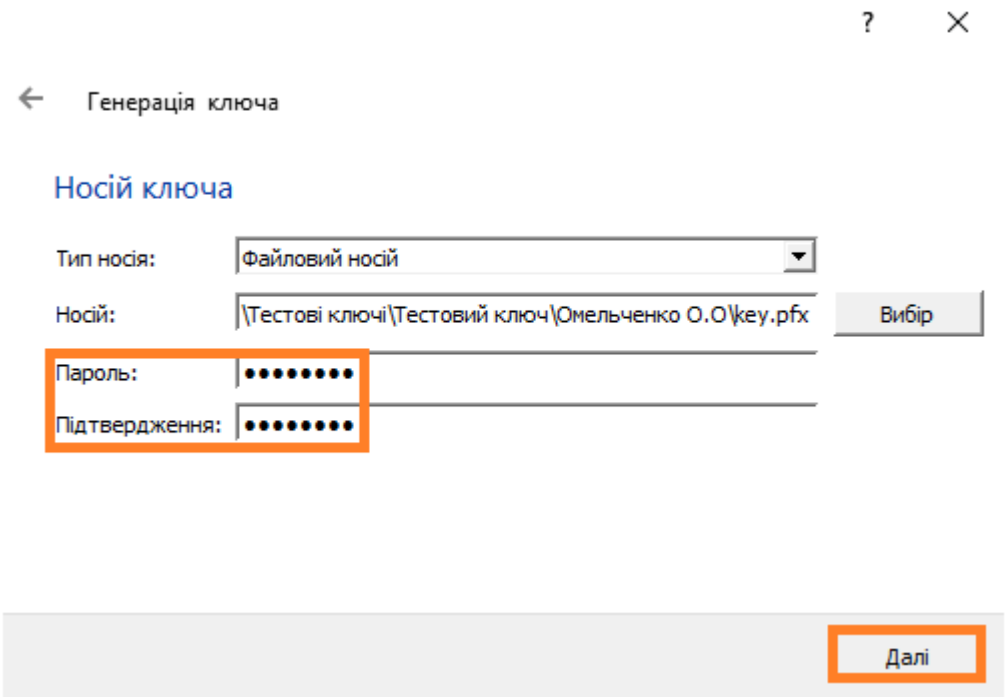


У вікні вибору каталогу для ключа також введіть ім’я файлу ключа та натисніть «Зберегти».



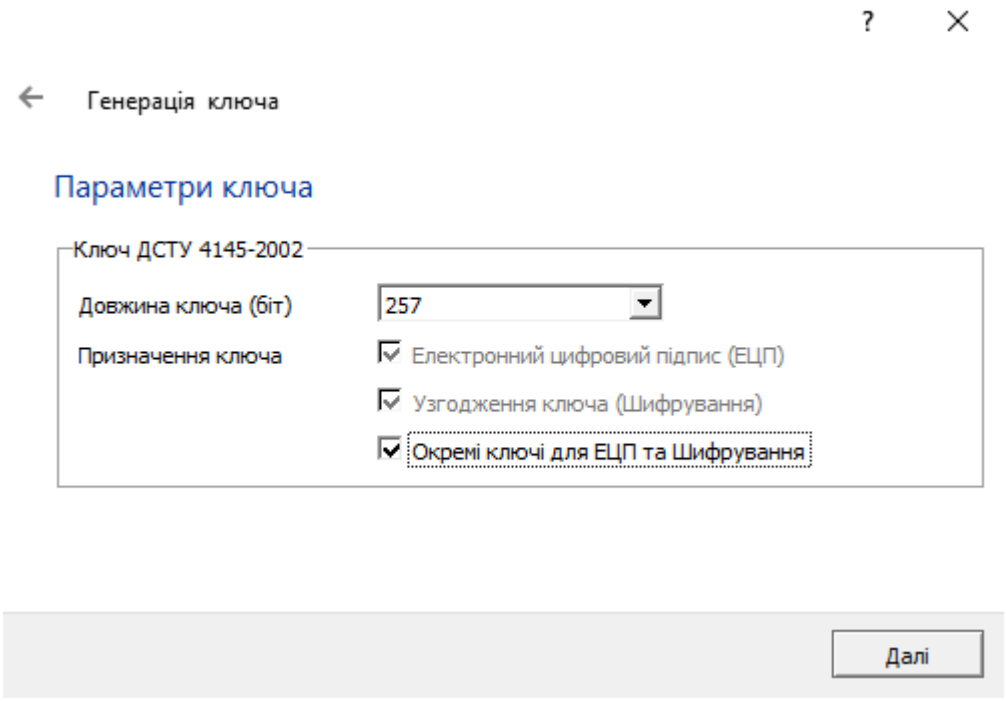
Далі введіть пароль (ПІН-код до ключа), введіть підтвердження паролю і натисніть «Далі». **Довжина ПІН-коду має бути не менше шести символів.**

Під час введення паролю зверніть увагу на те якою мовою вводите пароль і чи не включений у Вас «Caps Lock».

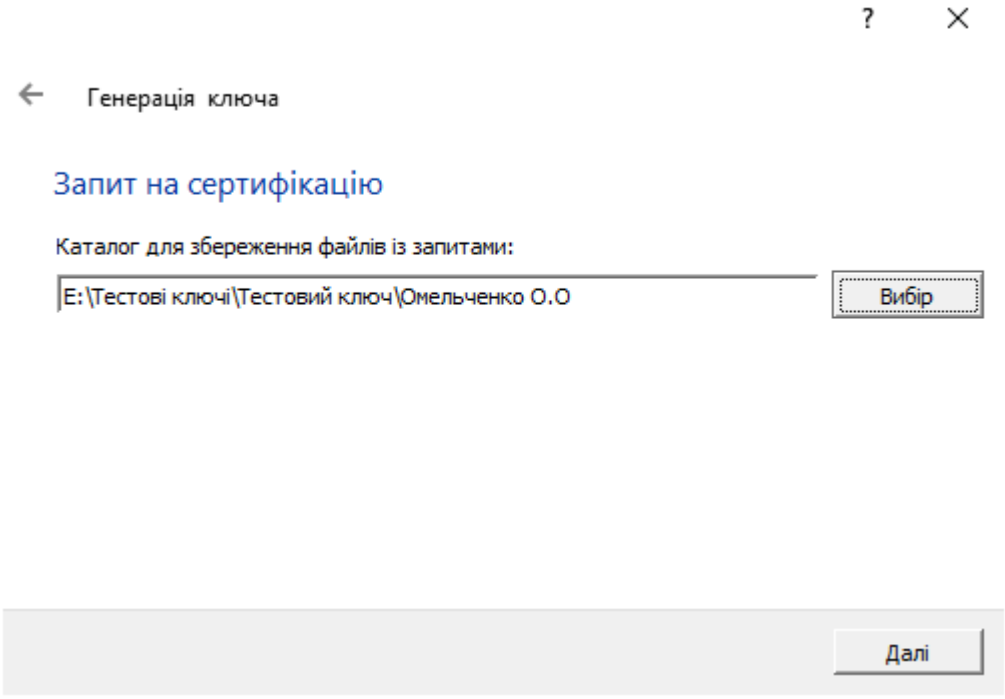


У вікні, що відкрилось оберіть довжину ключа та його призначення. Довжину рекомендуємо залишити за замовчуванням (257 біт). У розділі «Призначення ключа» оберіть необхідне для Вас призначення згідно з таблицею.

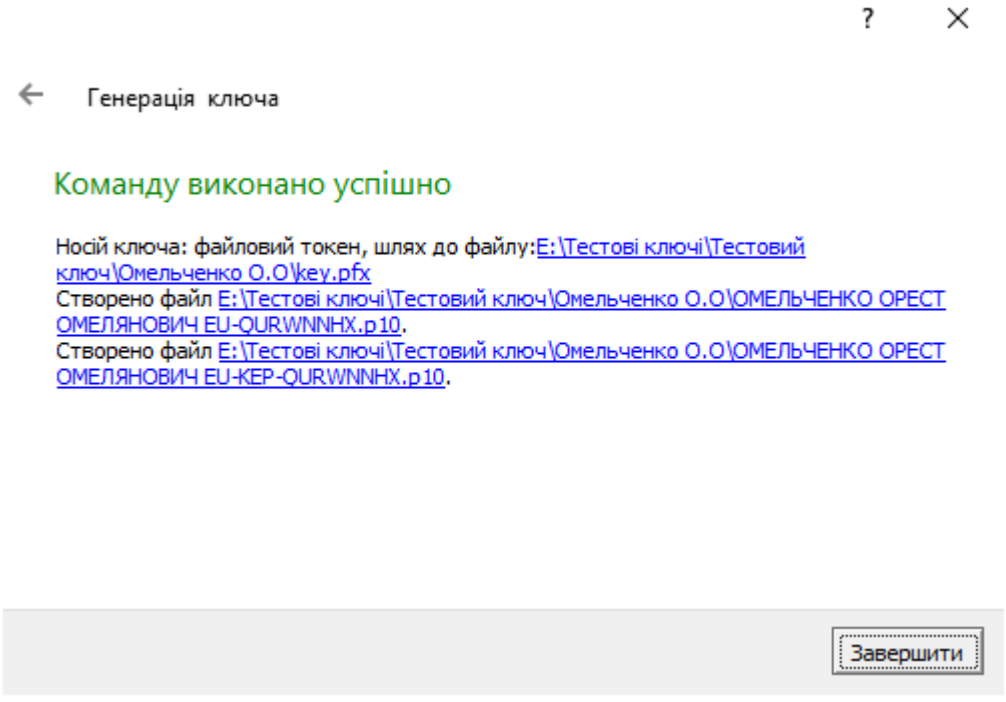
Призначення відкритого ключа:	
Електронний підпис	Електронний підпис або печатка. (генерується один ключ та один запит на сертифікат)
Узгодження ключа	Шифрування. (генерується один ключ та один запит на сертифікат)
Окремі ключі для ЕП та узгодження ключа	Окремі ключі для шифрування та ЕП (електронної печатки). (генерується два ключі та два запити на сертифікат)



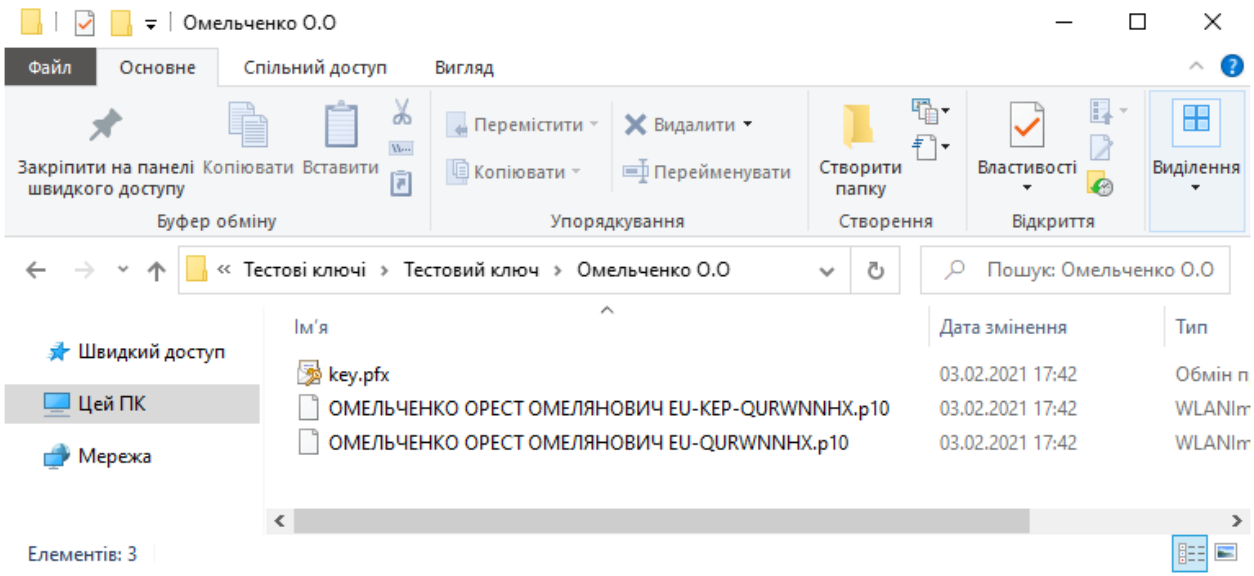
В наступному вікні вкажіть шлях до каталогу, в який буде збережено файли запитів, натиснувши «Вибір». Після обрання каталогу натисніть «Далі».



У вікні, що відкриється, зображено інформацію про завершення генерації ключа (ключів) та створення запиту (запитів) на сертифікат (сертифікати). Для продовження натисніть «Завершити».

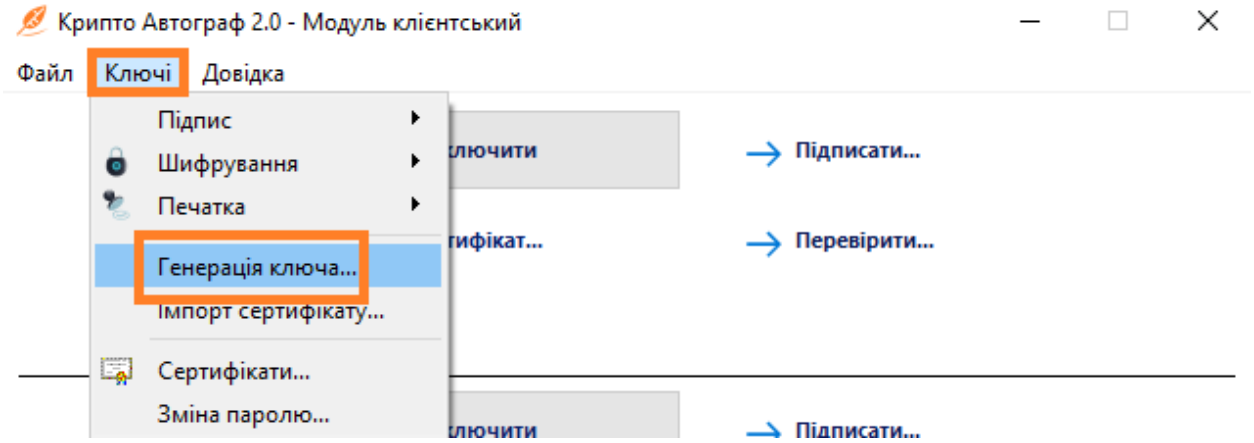


Нижче зображено згенерований ключ (у форматі .pfx) та два запити на сертифікат.



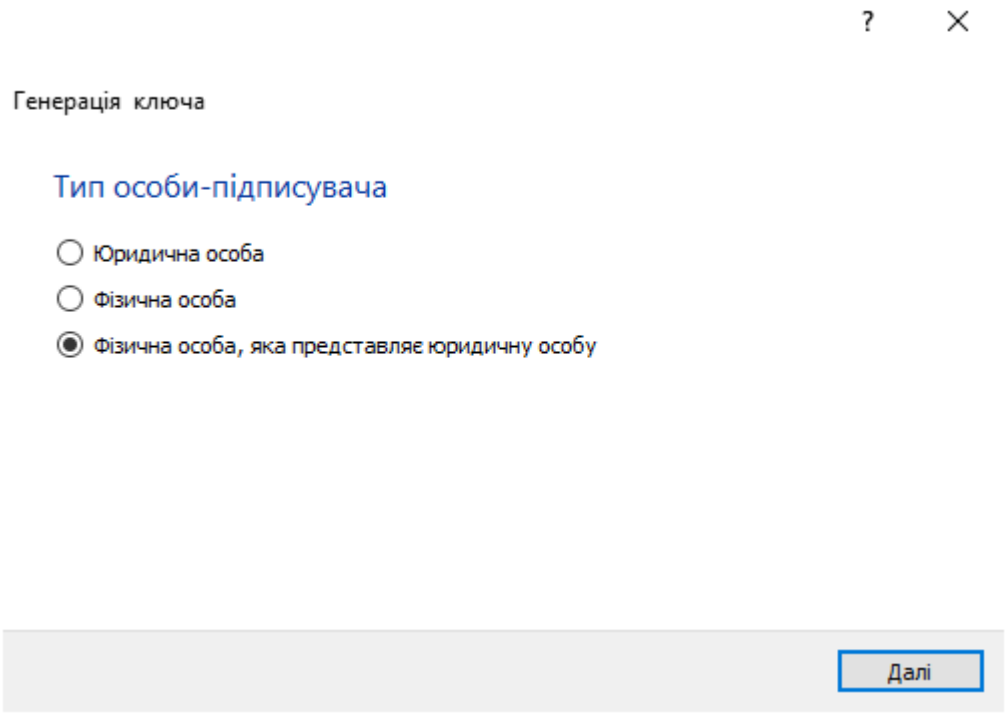
Формування запиту на сертифікат фізичної особи-підписувача, що є співробітником юридичної особи, або суб'єктом підприємницької діяльності

Запустивши програмне забезпечення використовуючи ярлик «КриптоАвтограф 2.0 - Модуль клієнтський» відкриється вікно де необхідно обрати «Ключі» → «Генерація ключа».

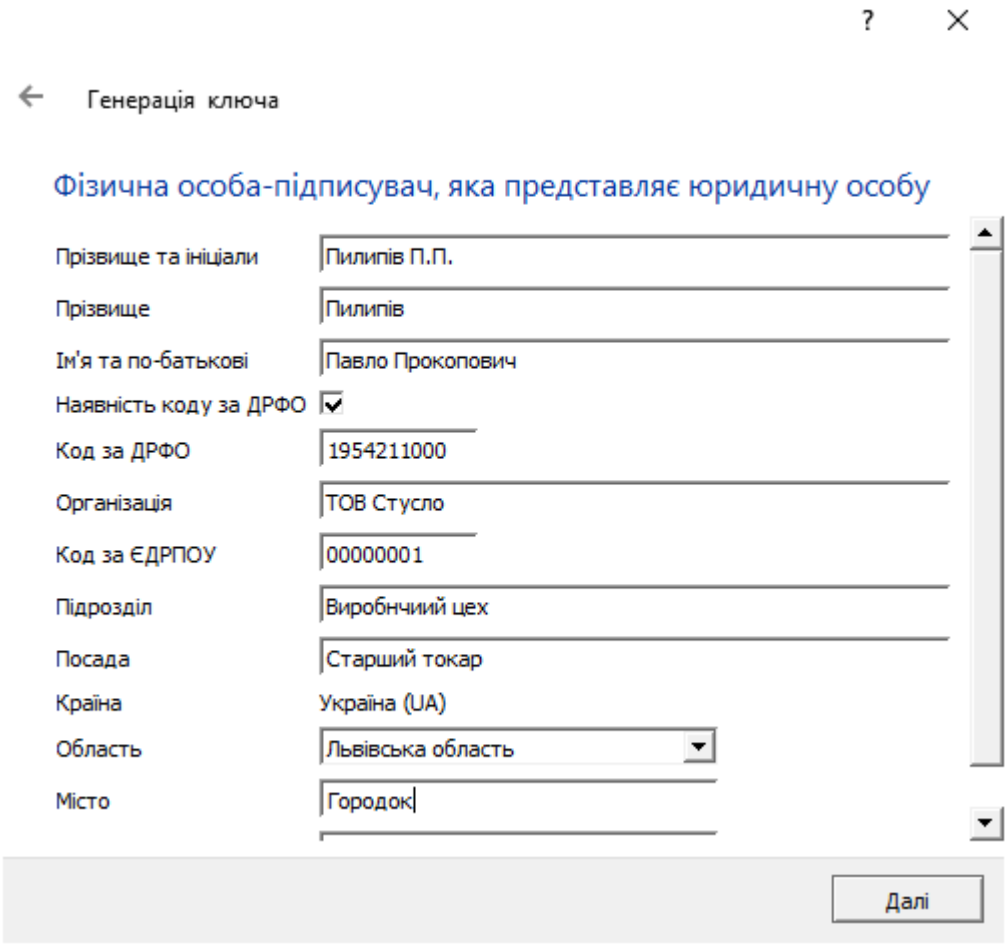


Обираємо «Фізична особа, яка представляє юридичну особу» для формування криптографічних ключів та запитів на сертифікацію відкритого ключа в акредитованому центрі сертифікації ключів з метою отримання сертифіката відкритого ключа електронного підпису або шифрування фізичної особи, що є співробітником організації - юридичної особи, або фізичної особи,

яка є суб’єктом підприємницької діяльності.



У вікні, що відкрилося необхідно зазначити інформацію про фізичну особу, що є співробітником організації - юридичної особи, або фізичної особи, яка є суб’єктом підприємницької діяльності.

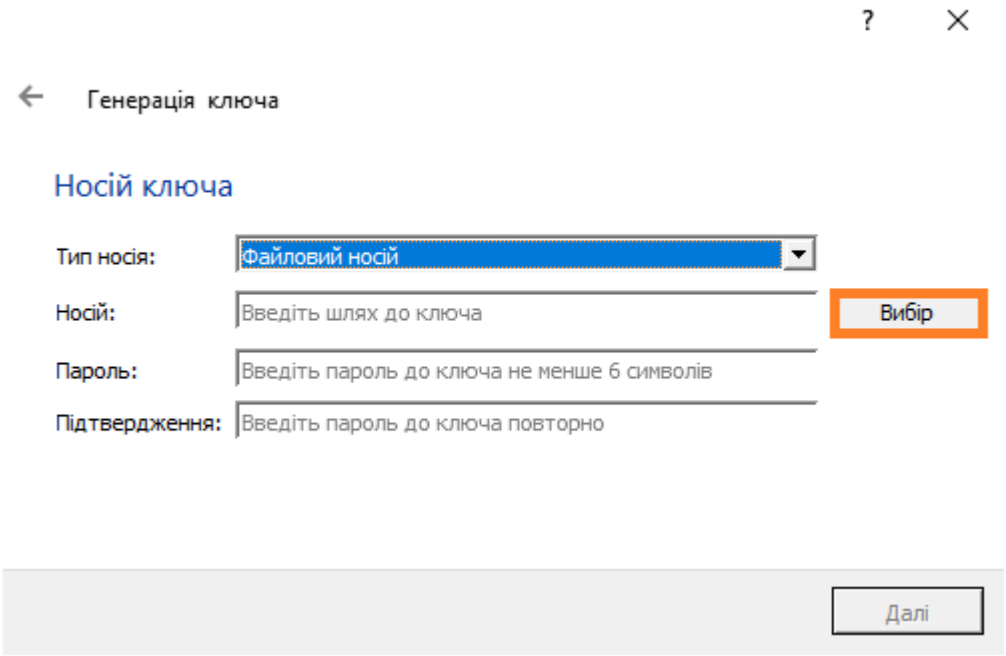


Важливо заповнювати інформацію відповідно до правил зазначених нижче:

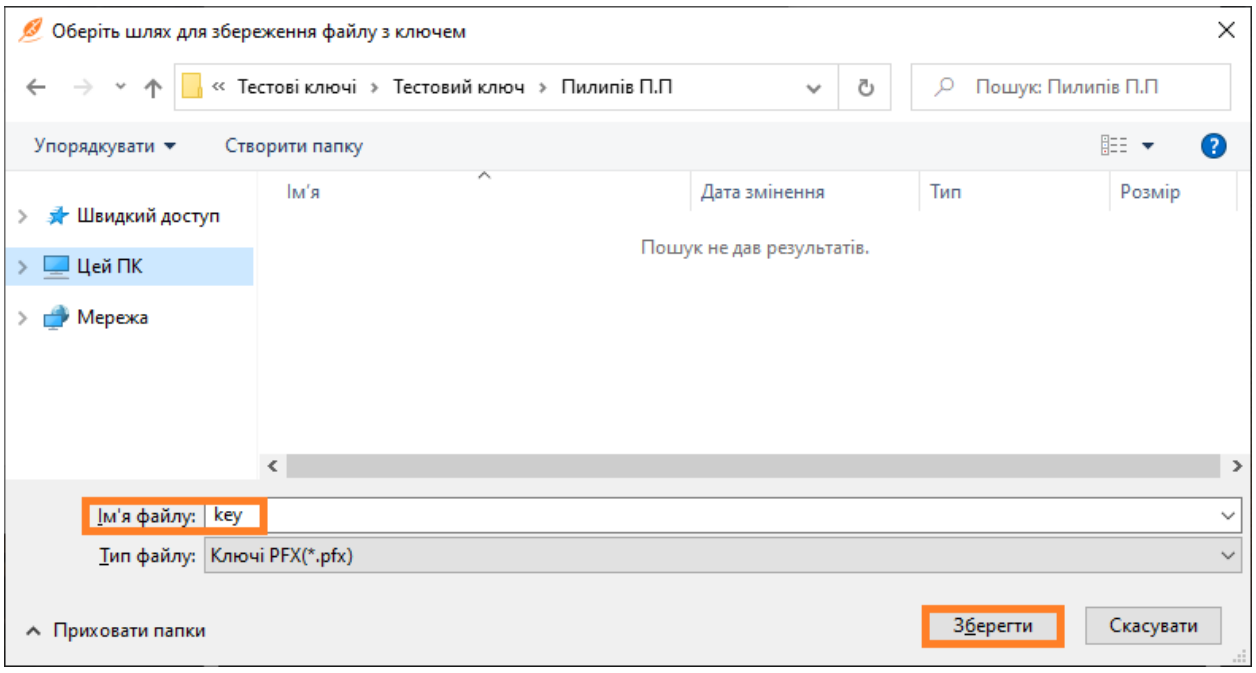
ЗАГАЛЬНА ІНФОРМАЦІЯ	
ПОЛЕ	ЗНАЧЕННЯ ПОЛЯ
Прізвище та ініціали:	Прізвище та ініціали фізичної особи – підписувала.
Прізвище:	Прізвище підписувача за паспортними даними.
Ім’я та по батькові:	Ім’я та по батькові підписувача за паспортними даними.
Наявність коду за ДРФО	Поставте позначку у разі наявності коду за ДРФО (РНОКПП)

Код за ДРФО	Код за ДРФО підписувача (реєстраційний номер облікової картки платника податків)
Організація	Повне (або офіційне скорочене) найменування організації - юридичної особи, за установчими документами (Статут) або відомостями про державну реєстрацію.
Код за ЄДРПОУ	Унікальний ідентифікаційний номер юридичної особи в Єдиному державному реєстрі підприємств та організацій України
Підрозділ	Підрозділ організації, згідно установчих документів, в якому працює фізична особа, що представляє юридичну особу
Посада	Посада в підрозділі, яку займає фізична особа, що представляє юридичну особу
Область:	Область, у якій зареєстрована організація, яка пов’язана з фізичною особою –підписувачем. Примітка: Для міста Києва та Севастополя область не зазначається.
Місто:	Місто, в якому зареєстрована організація, яка пов’язана з фізичною особою- підписувачем.
Серійний №	Залиште поле незаповненим

Заповнивши інформацію натисніть «Далі» та в наступному вікні оберіть тип носія для генерації ключа. За замовчуванням буде обрано «Файловий носій», залиште цей вибір без змін. Після цього натисніть «Вибір» для обрання каталогу в який буде збережено ключ.

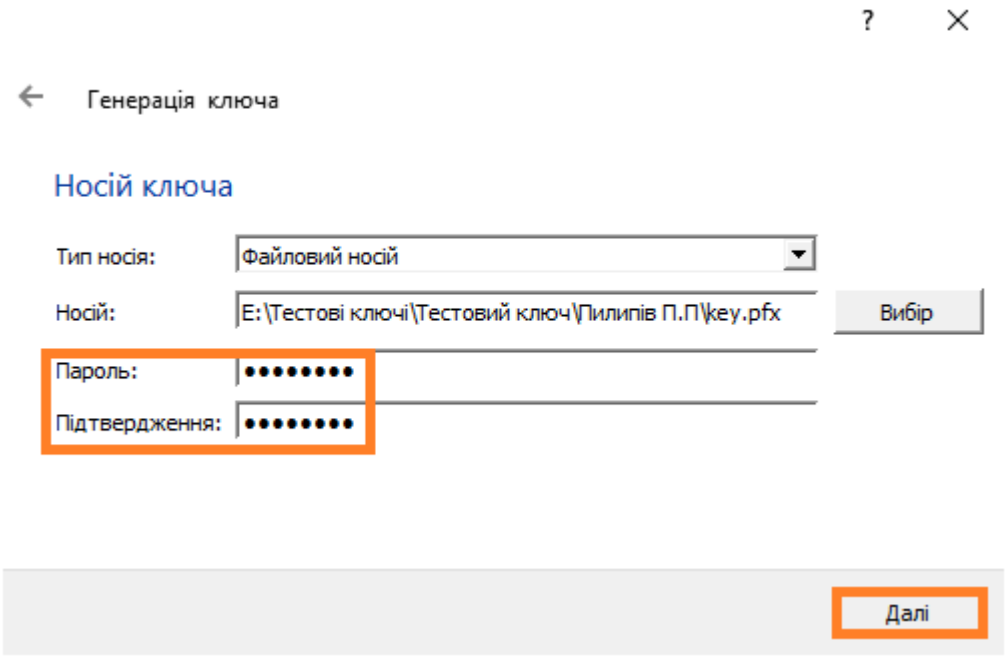


У вікні вибору каталогу для ключа також введіть ім’я файлу ключа та натисніть «Зберегти».



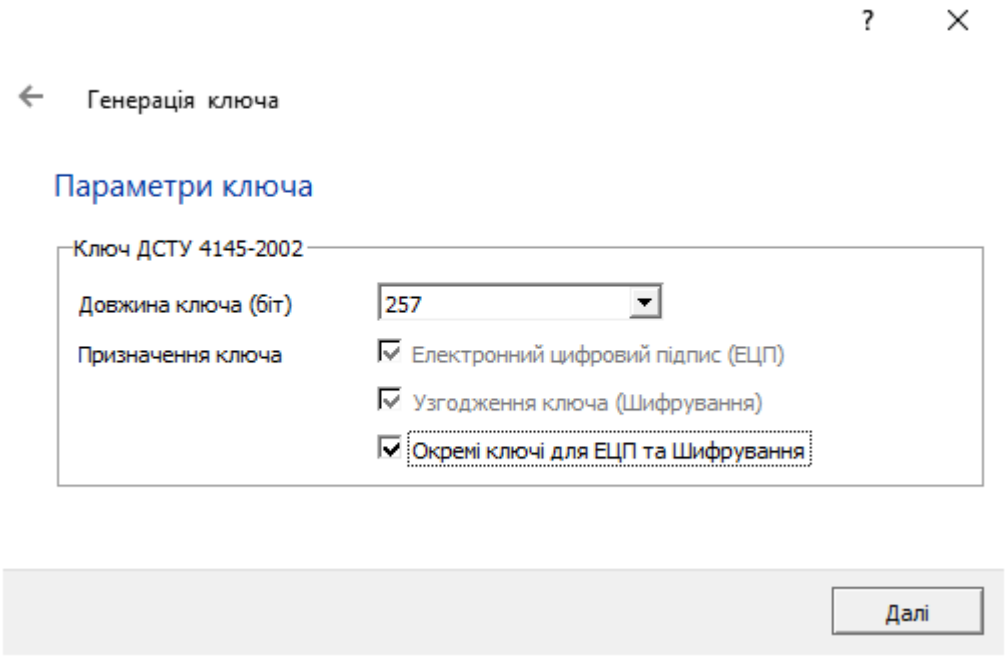
Далі введіть пароль (ПІН-код до ключа), введіть підтвердження паролю і натисніть «Далі». **Довжина ПІН-коду має бути не менше шести символів.**

Під час введення паролю зверніть увагу на те якою мовою вводите пароль і чи не включений у Вас «Caps Lock».

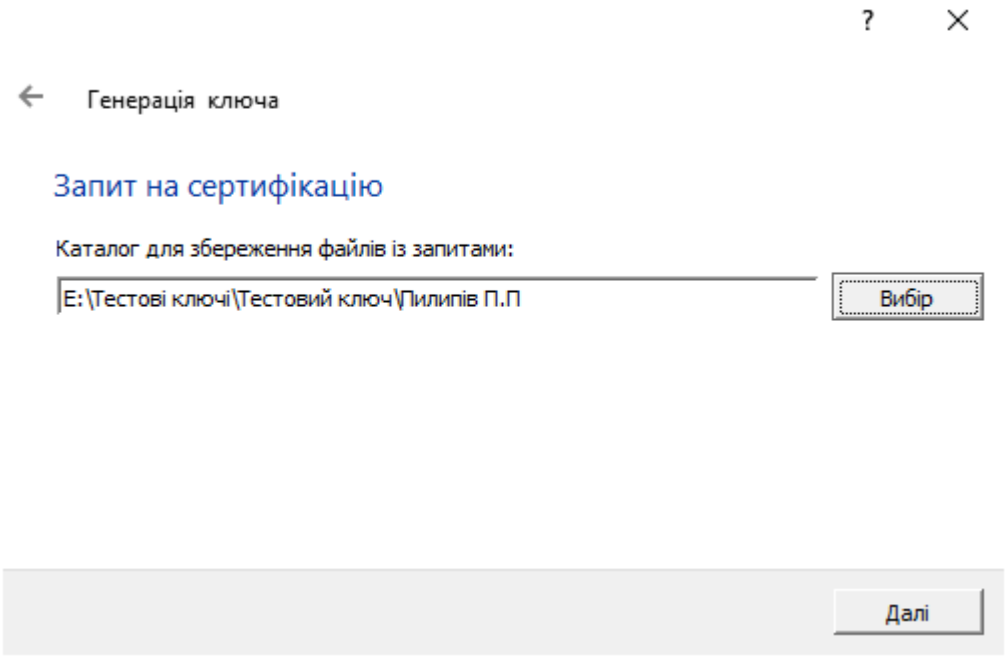


У вікні, що відкрилось оберіть довжину ключа та його призначення. Довжину рекомендуємо залишити за замовчуванням (257 біт). У розділі «Призначення ключа» оберіть необхідне для Вас призначення згідно з таблицею.

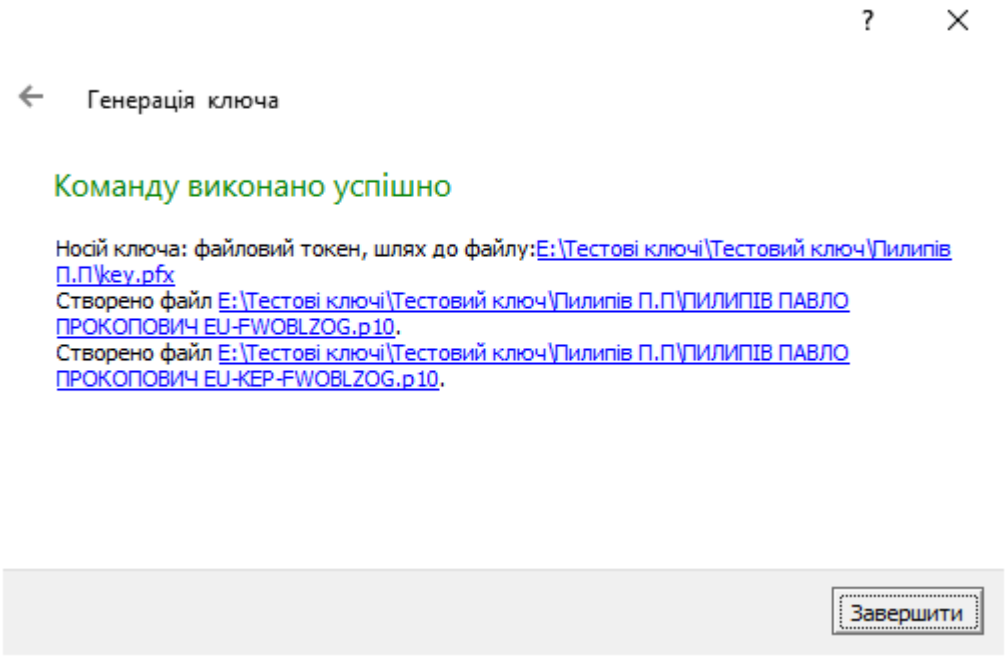
Призначення відкритого ключа:	
Електронний підпис	Електронний підпис або печатка. (генерується один ключ та один запит на сертифікат)
Узгодження ключа	Шифрування. (генерується один ключ та один запит на сертифікат)
Окремі ключі для ЕП та узгодження ключа	Окремі ключі для шифрування та ЕП (електронної печатки). (генерується два ключі та два запити на сертифікат)



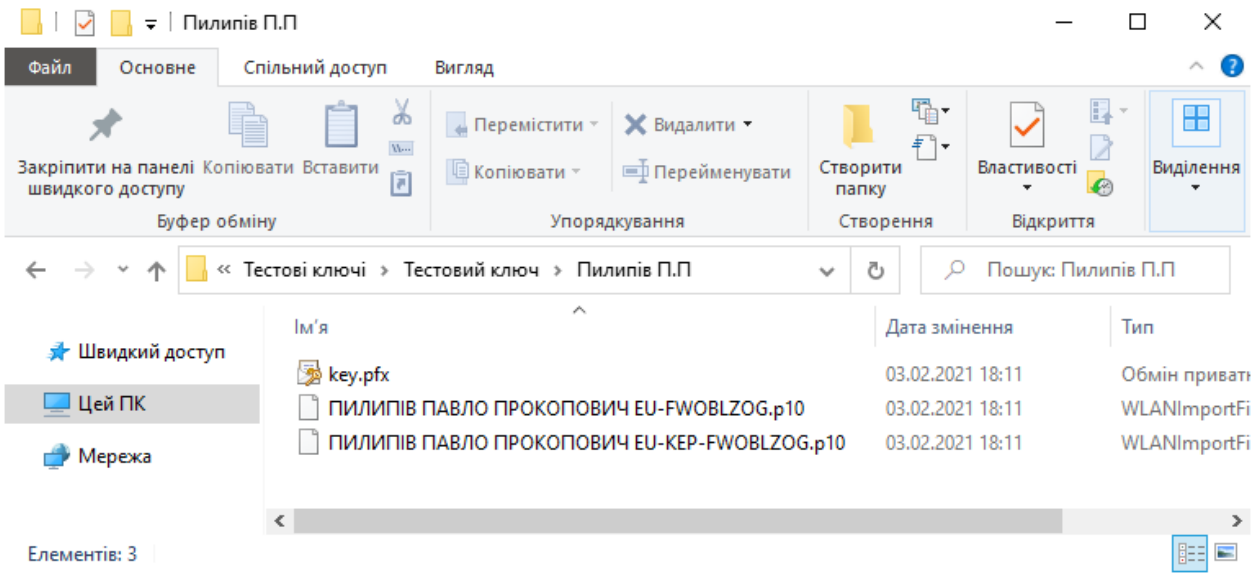
В наступному вікні вкажіть шлях до каталогу, в який буде збережено файли запитів, натиснувши «Вибір». Після обрання каталогу натисніть «Далі».



У вікні, що відкриється, зображено інформацію про завершення генерації ключа (ключів) та створення запиту (запитів) на сертифікат (сертифікати). Для продовження натисніть «Завершити».



Нижче зображено згенерований ключ (у форматі .pfx) та два запити на сертифікат.

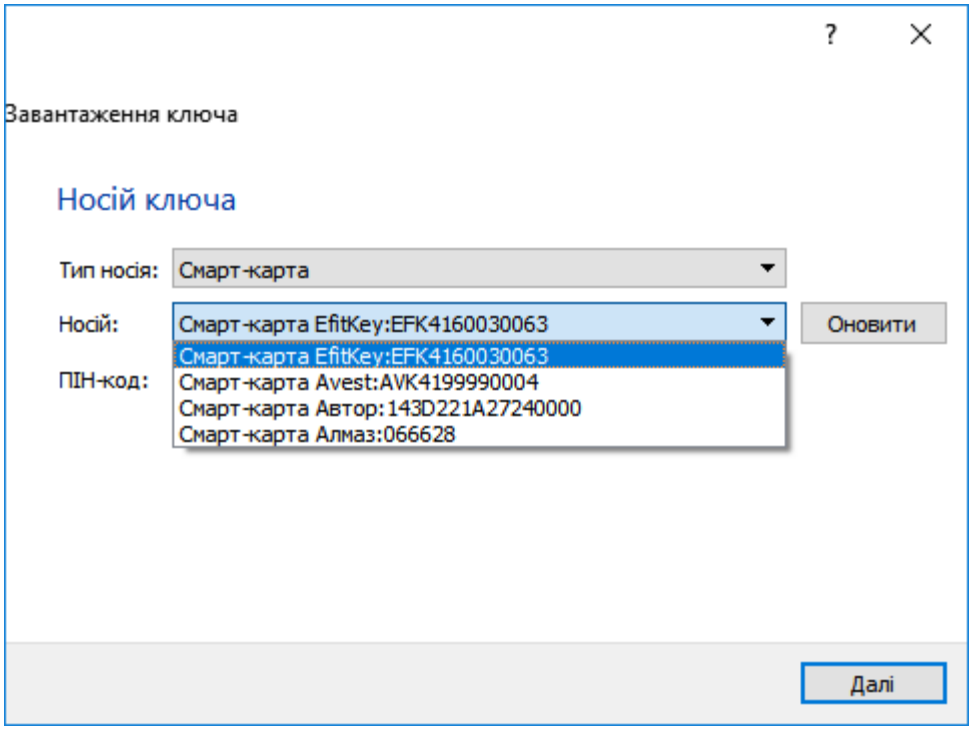


РОБОТА З ЗНКІ

ЗНКІ, що підтримуються Засобом

Крипто Автограф підтримує наступні ЗНКІ:

- Efit Key;
- AvestKey;
- Автор SecureToken-337;
- Автор SecureToken-338;
- Алмаз 1-К;
- Кристал-1.



Варто зазначити, що на разі Засіб працює з смарт-картами «iToken», лише при умові, що ключі ЕП на ньому було згенеровано в Засобі. Смарт-карта при цьому доступна для роботи лише в Засобі, та буде недоступна, наприклад, в програмному забезпеченні Користувач КНЕДП.

Налаштування електронних ключів «Алмаз-1К» для роботи в Засобі.

Нижче буде описано процедуру підготовки носіїв за умови відсутності на них ключів та за умови, що на носії вже є діючі ключі.

Налаштування ЗНКІ "Алмаз - 1К" для роботи в Засобі КЗІ Крипто Автограф за умови ВІДСУТНОСТІ ключів на носії

Для підключення електронного ключа «Алмаз-1К» в Засобі необхідно ініціалізувати носій.

Зверніть увагу, що ініціалізація призведе до видалення ключів і сертифікатів, отриманих раніше.

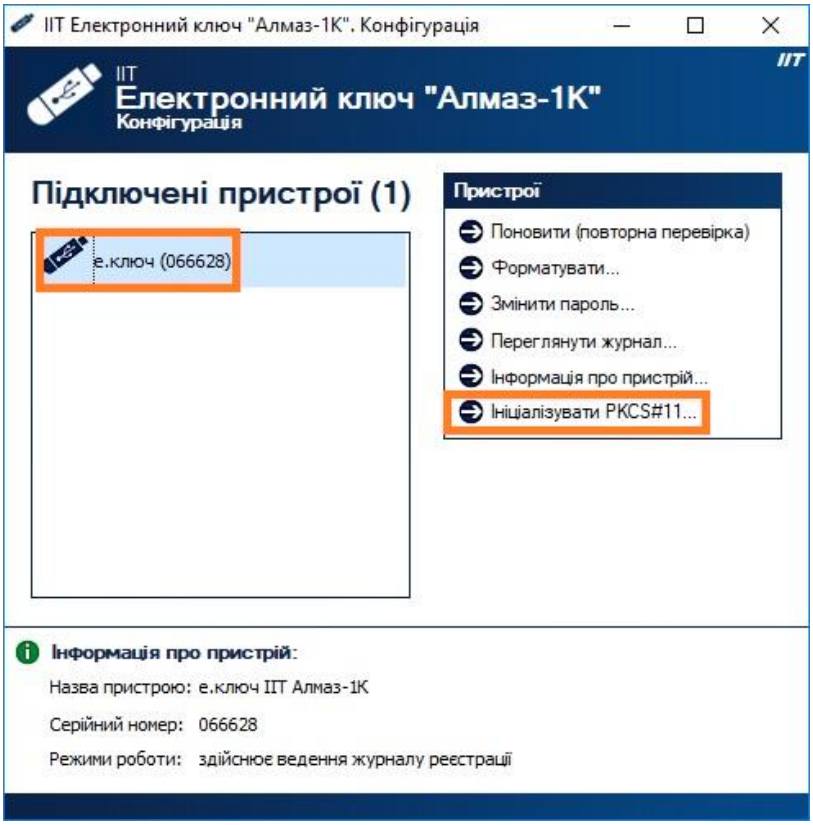
Для ініціалізації необхідно завантажити програмне забезпечення «ІІТ Е.ключ Алмаз-1К. Конфігурація».

ПЗ доступне за посиланням:

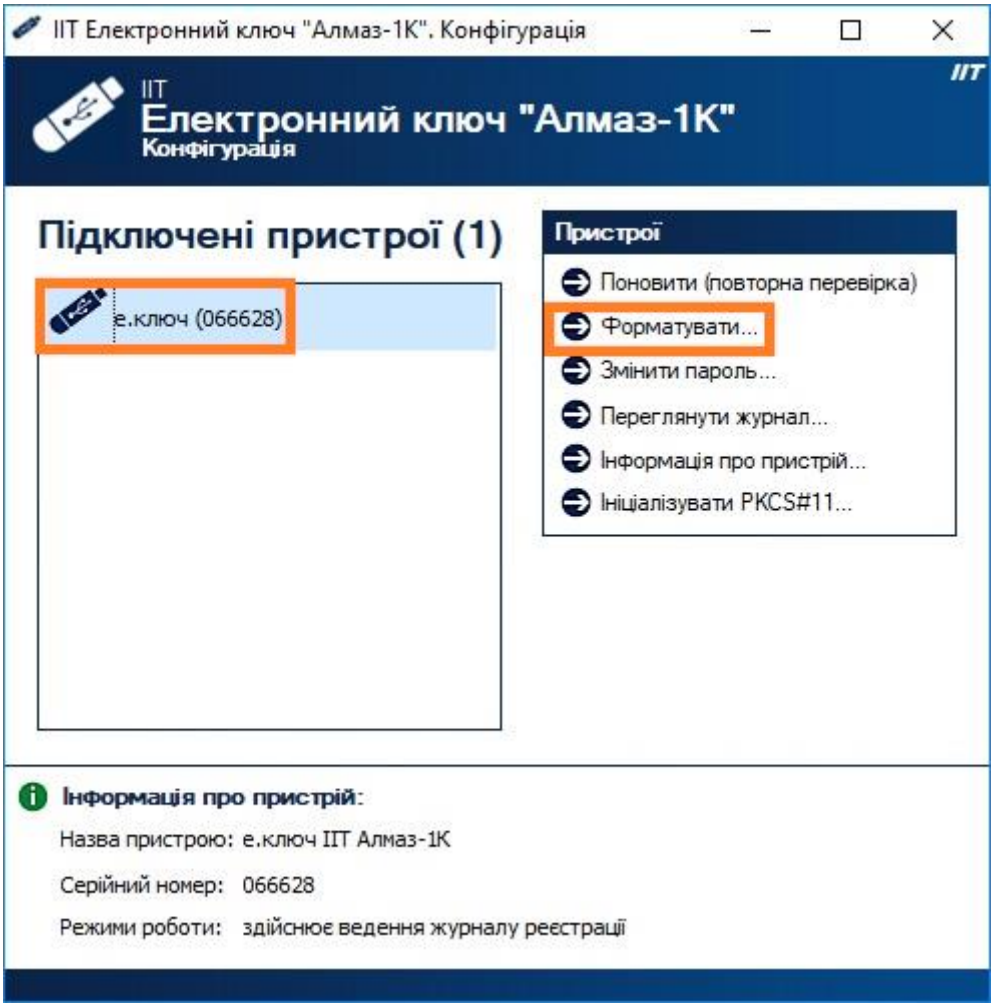
https://smartsolutions.kiev.ua/download/soft/Almaz1C.exe

Остання версія ПЗ, вказаного вище, що доступна для завантаження з офіційного сайту виробника, може призвести до критичної помилки, яка унеможливлює використання електронного ключа «Алмаз-1К» у Крипто Автографі. Тому рекомендується встановлювати стару версію, яка доступна за посиланням, зазначеним вище.

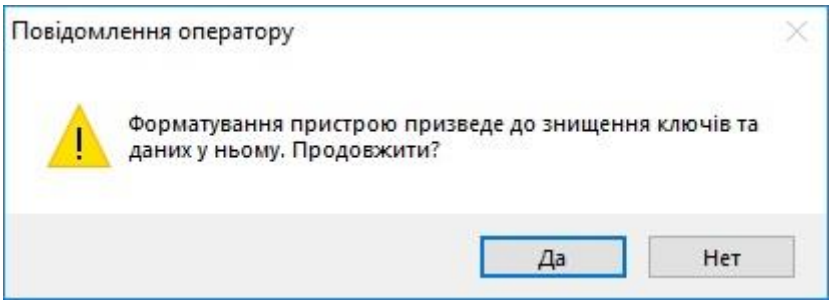
Після встановлення ПЗ, підключіть носій до комп’ютера та запустіть ПЗ. У вікні, що відкрилось та зображено нижче, в лівій частині екрану оберіть носій, в правій- натисніть «Ініціалізувати».



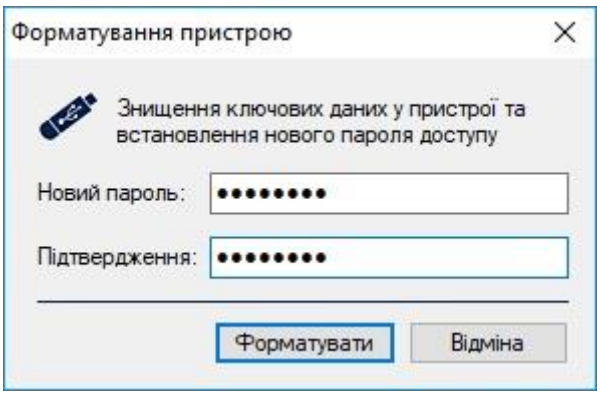
Якщо на Вашому носієві вже є ключі, необхідно буде спочатку відформатувати носій, про що повідомить ПЗ. Для форматування натисніть «Форматувати».

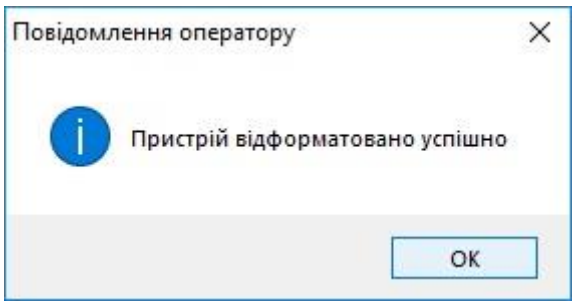


У вікні, що відкрилось натисніть «Так».

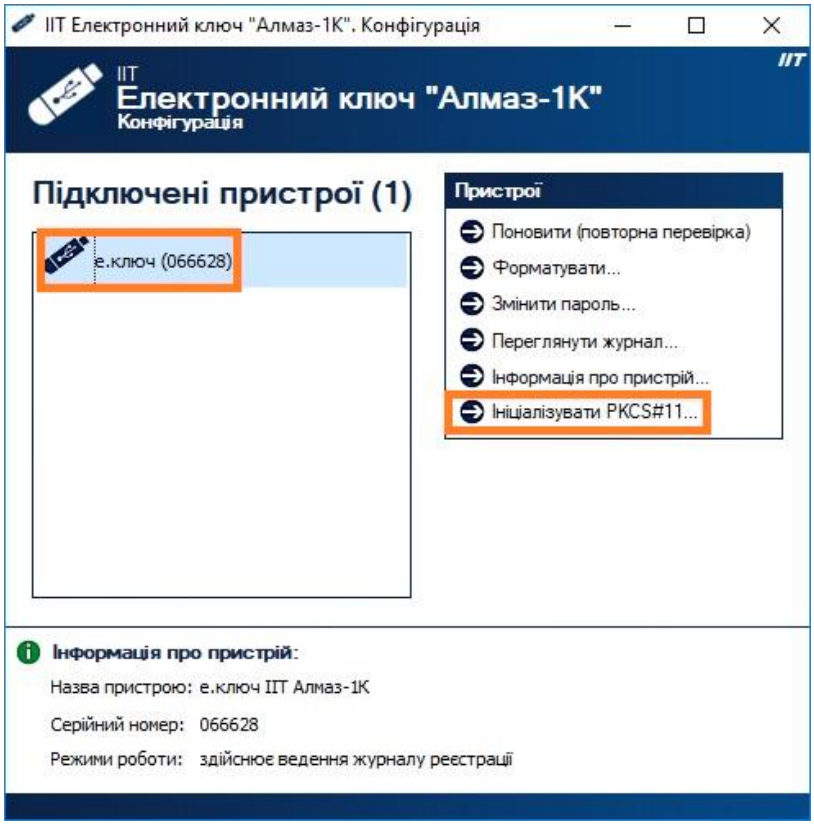


В наступному вікні введіть ПІН-код до носія та підтвердьте його, після цього натисніть «Форматувати».

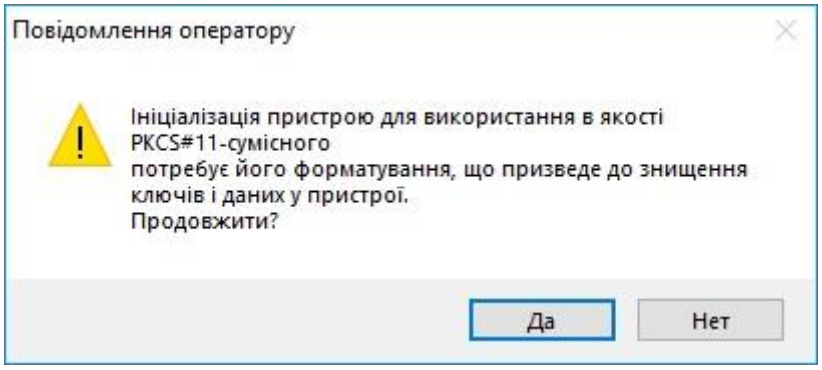




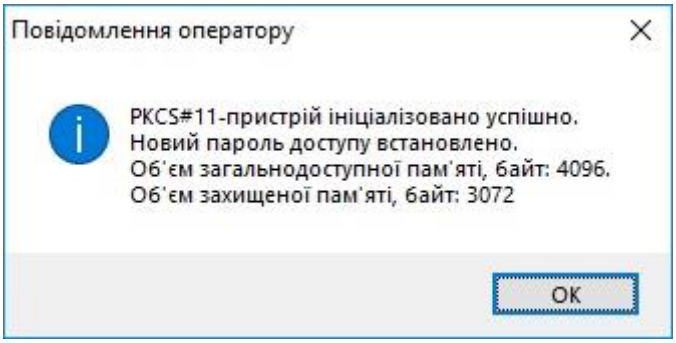
Після форматування повторно запустіть ініціалізацію.



Натисніть «Так».



Повторно введіть ПІН-код та підтвердьте його.



Після вдалої ініціалізації необхідно згенерувати ключі.

Після отримання сертифікатів необхідно перенести їх до відповідних каталогів. Скопіюйте два файли сертифікатів та перенесіть їх в каталоги «My Crt» та «My Certificates and CRLs 13», які знаходяться на диску С.

Налаштування ЗНКІ "Алмаз - 1К" для роботи в Засобі КЗІ Крипто Автограф за умови НАЯВНОСТІ ключів на носії

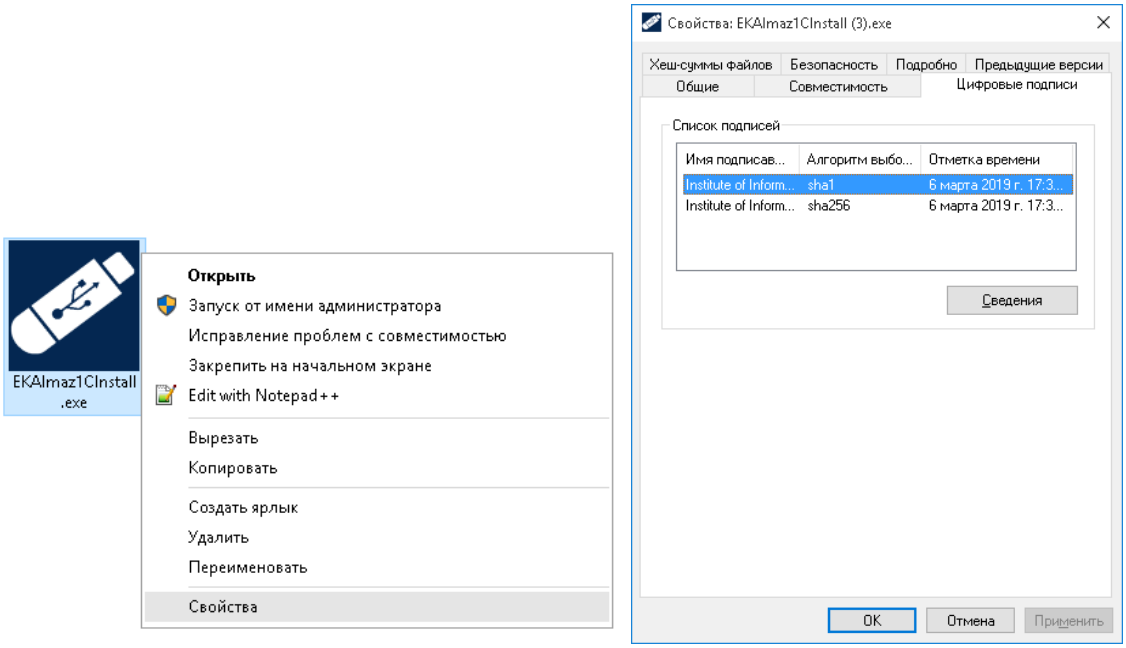
Для підключення електронного ключа «Алмаз-1К», який вже «персоналізовано» тобто, який вже містить ключові дані електронного підпису, що отримані в КНЕДП необхідно завантажити програмне забезпечення «ІІТ Е.ключ Алмаз-1К. Конфігурація», за посиланням:

Для ініціалізації необхідно завантажити програмне забезпечення «ІІТ Е.ключ Алмаз-1К. Конфігурація».

ПЗ доступне за посиланням:

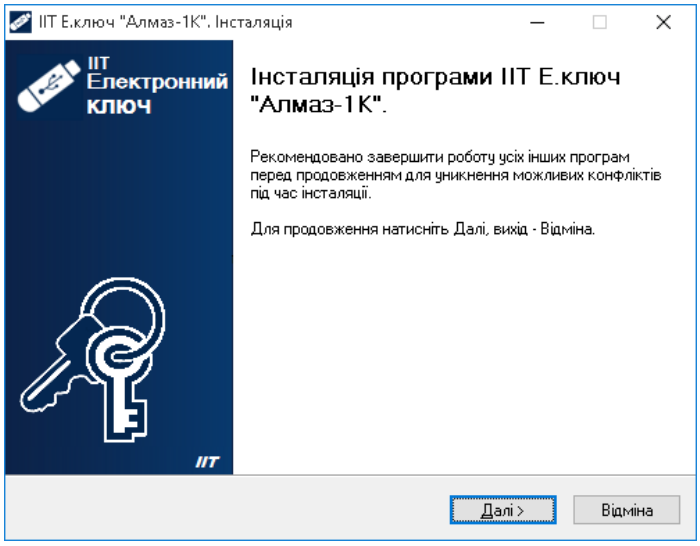
https://smartsolutions.kiev.ua/download/soft/Almaz1C.exe

Остання версія ПЗ, вказаного вище, що доступна для завантаження з офіційного сайту виробника, може призвести до критичної помилки, яка унеможливлює використання електронного ключа «Алмаз-1К» у Крипто Автографі. Тому рекомендується встановлювати стару версію, яка доступна за посиланням, зазначеним вище.

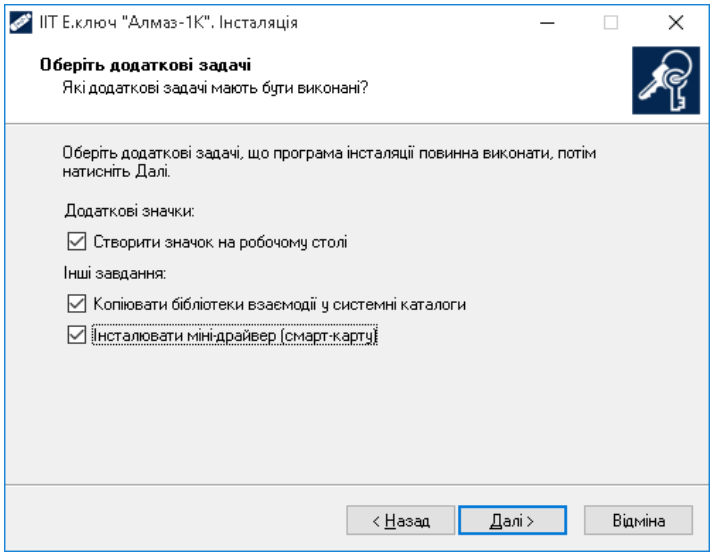


Після завантаження програмного забезпечення «ІІТ Е.ключ Алмаз-1К. Конфігурація» та перевірки відповідності його версії необхідно здійснити встановлення.

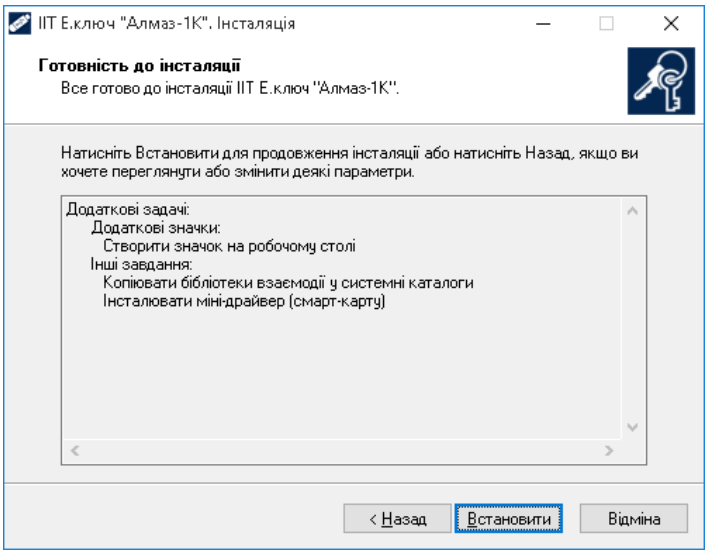
Для встановлення інсталяційного пакету необхідно запустити виконуючий файл EKAlmaz1CInstall.exe через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої кнопки миші. Після запуску на екрані з’явиться вікно встановлення програмного забезпечення, необхідно натиснути кнопку «Далі»



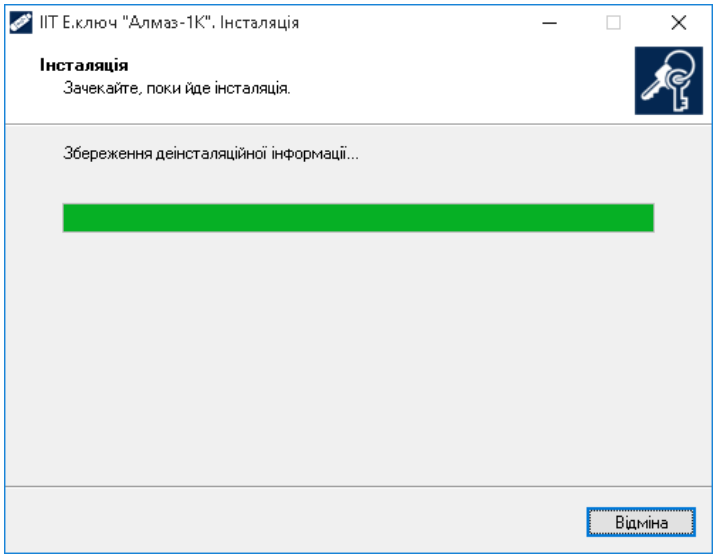
У вікні, яке відкрилося та наведено нижче на рисунку необхідно обрати наступні компоненти для встановлення «Створити значок на робочому столі», «Копіювати бібліотеки взаємодії у системний каталог», «Інсталювати міні-драйвер (смарт-карту)» та потім натиснути кнопку «Далі».



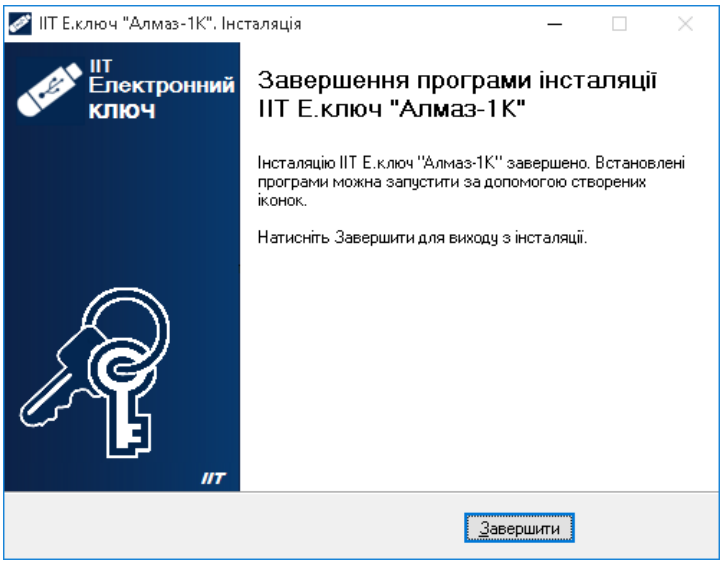
У вікні, яке відкрилося та наведено нижче натисніть кнопку «Встановити».



Дочекайтеся завершення процесу встановлення даного програмного забезпечення.



У вікні яке відкрилося та наведено нижче натисніть кнопку «Завершити» тим самим успішно завершити встановлення програмного забезпечення «ІІТ Е.ключ Алмаз-1К. Конфігурація».



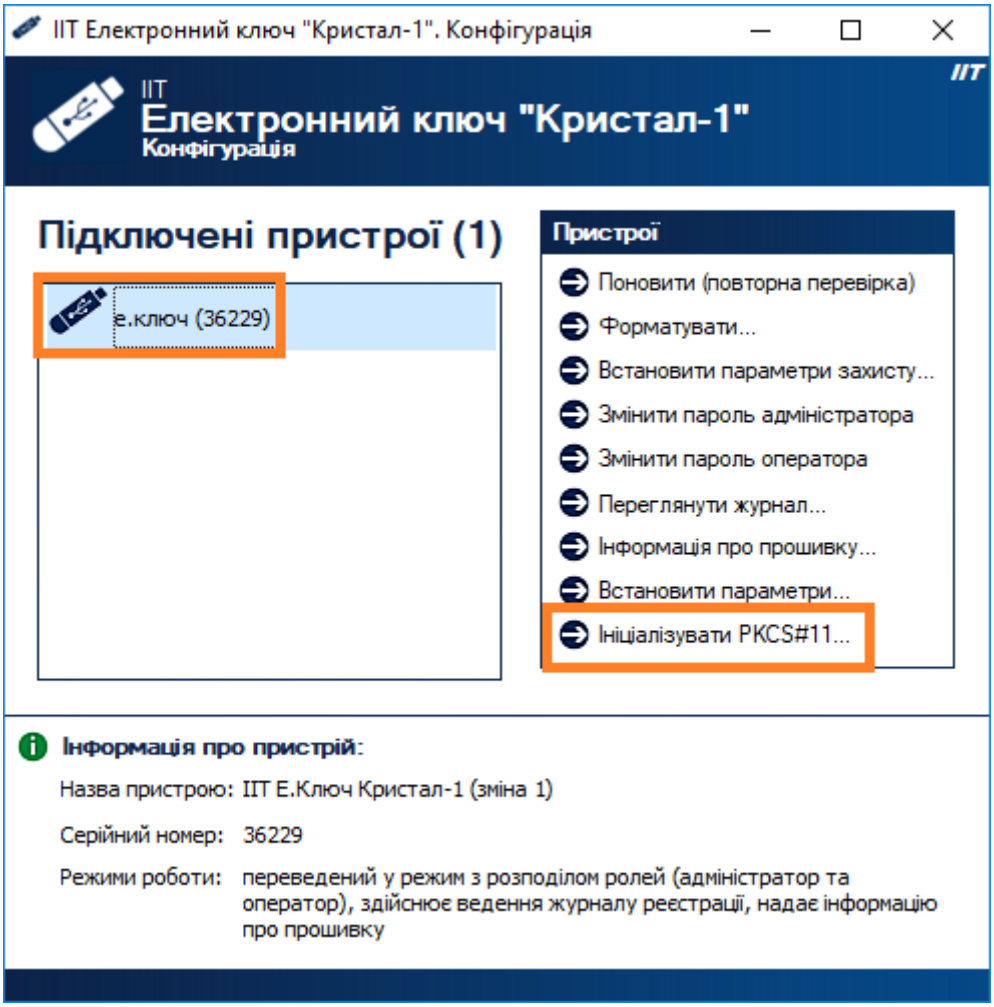
Примітка: Особливості встановлення програмного забезпечення «ІІТ Е.ключ Алмаз-1К. Конфігурація» можуть змінюватися його розробником у більш нових версіях даного програмного забезпечення.

Налаштування ЗНКІ "Кристал - 1" для роботи в Засобі КЗІ Крипто Автограф за умови ВІДСУТНОСТІ ключів на носії

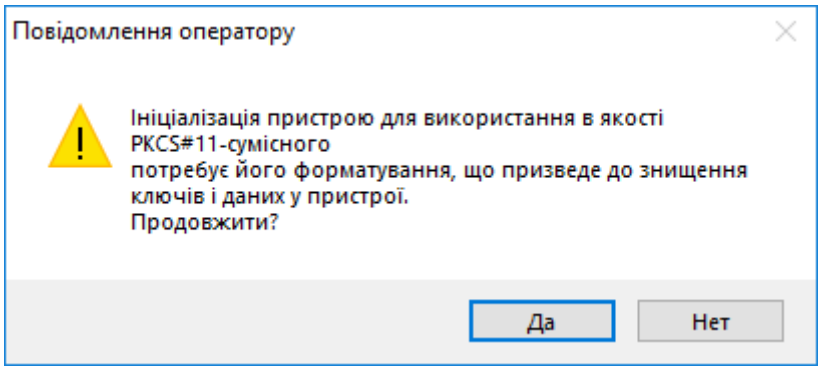
Зверніть увагу, що згідно з інформацією виробника ЗНКІ «Кристал-1» АТ ІІТ, для роботи з даним ЗНКІ на комп'ютерах під управлінням операційної системи Microsoft Windows 10 та Microsoft Windows 11, необхідно в налаштуваннях BIOS вимкнути параметр Secure Boot. Якщо на Вашому комп'ютері ЗНКІ «Кристал-1» відображається в диспетчері пристроїв без помилок – вимикати параметр Secure Boot.

Для ініціалізації необхідно завантажити програмне забезпечення «ІІТ електронний ключ Кристал-1. Конфігурація», ПЗ доступне за посиланням: https://smartsolutions.kiev.ua/download/soft/Crystal1.exe

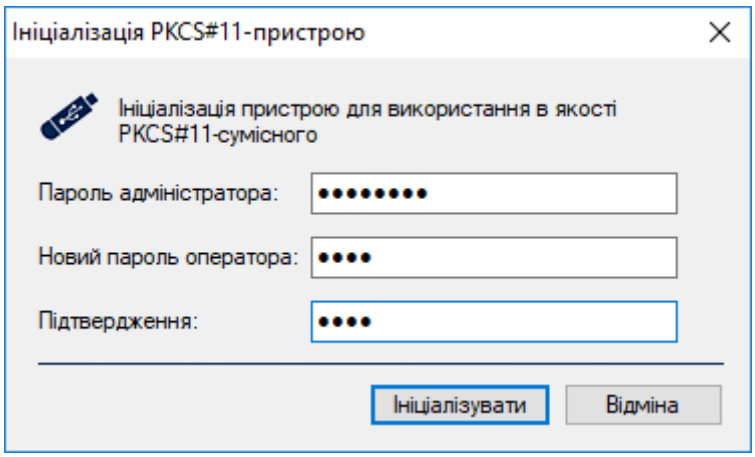
Після встановлення ПЗ, підключіть носій до комп'ютера та запустіть ПЗ. У вікні, що відкрилось та зображено нижче, в лівій частині екрану оберіть носій, в правій натисніть «Ініціалізувати PKCS#11».



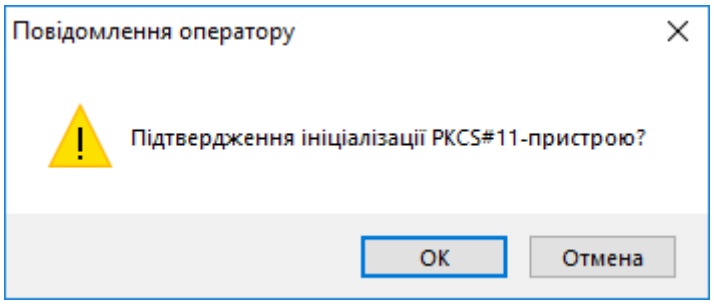
У вікні, що відкрилось і зображено нижче, підтвердьте ініціалізацію.



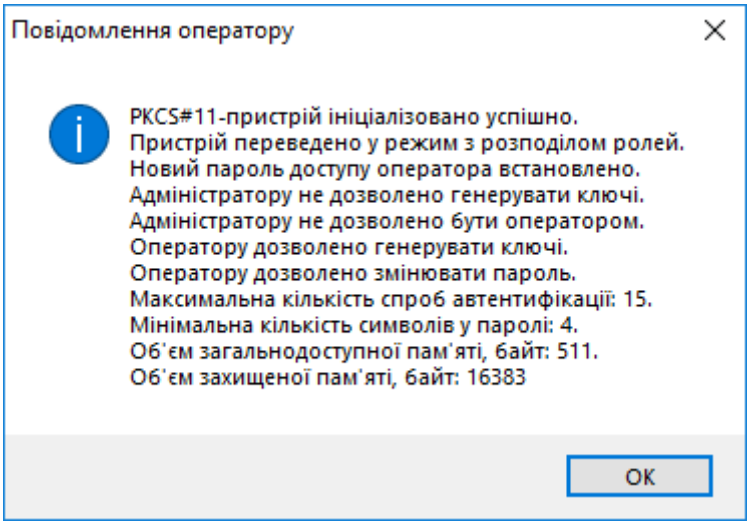
Далі введіть пароль адміністратора та пароль оператора. Перший буде використовуватись для налаштувань електронного ключа, другий – для підключення ключів. Після введення паролів натисніть «Ініціалізувати».



Натисніть «ОК» для підтвердження.



Вікно, що зображено нижче, свідчить про успішну ініціалізацію ключа. Натисніть «ОК»



Після вдалої ініціалізації необхідно згенерувати ключі. Для цього запустіть ПЗ «Крипто Автограф». В горизонтальному меню оберіть пункт «Ключі», в меню, що відкрилось оберіть «Генерація ключа».

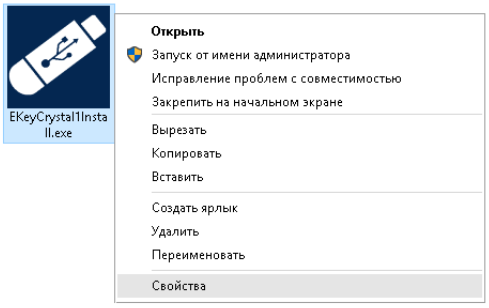
Налаштування ЗНКІ "Кристал - 1" для роботи в Засобі КЗІ Крипто Автограф за умови НАЯВНОСТІ ключів на носії

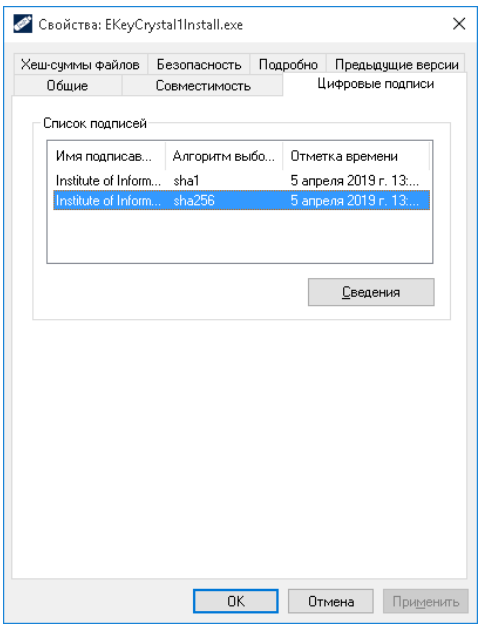
Зверніть увагу, що згідно з інформацією виробника ЗНКІ «Кристал-1» АТ ІІТ, для роботи з даним ЗНКІ на комп'ютерах під управлінням операційної системи Microsoft Windows 10 та Microsoft Windows 11, необхідно в налаштуваннях BIOS вимкнути параметр Secure Boot. Якщо на Вашому комп'ютері ЗНКІ «Кристал-1» відображається в диспетчері пристроїв без помилок – вимикати параметр Secure Boot.

Для підключення електронного ключа «Кристал-1», який вже «персоналізовано» тобто, який вже містить ключові дані електронного підпису, що отримані в КНЕДП необхідно завантажити програмне забезпечення «ІІТ електронний ключ Кристал-1. Конфігурація», за посиланням:

https://smartsolutions.kiev.ua/download/soft/Crystal1.exe

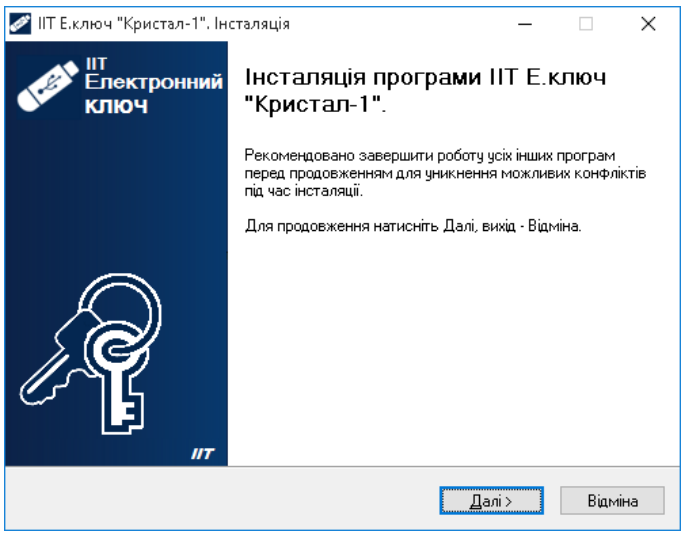
Примітка: Версія програмного забезпечення «ІІТ електронний ключ Кристал-1. Конфігурація» повинна бути не пізнішою ніж за дату публікації 5 квітня 2019 року, за наявним цифровим підписом інсталяційного пакету.



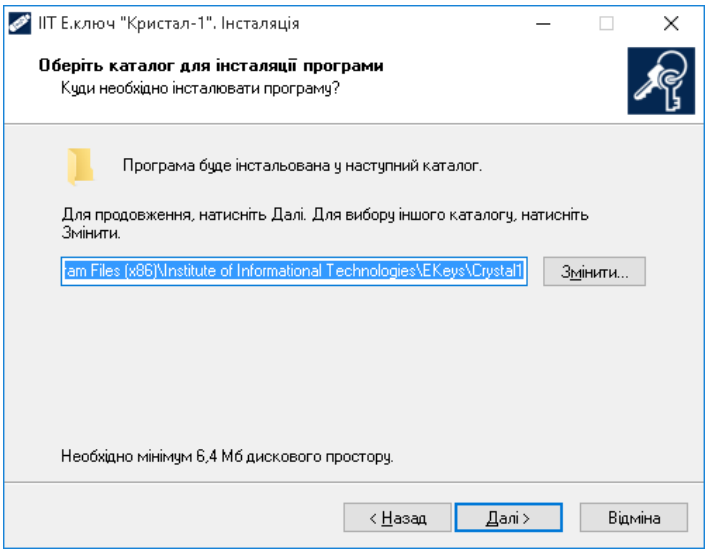


Після завантаження програмного забезпечення «ІІТ електронний ключ Кристал-1. Конфігурація» та перевірки відповідності його версії необхідно здійснити встановлення.

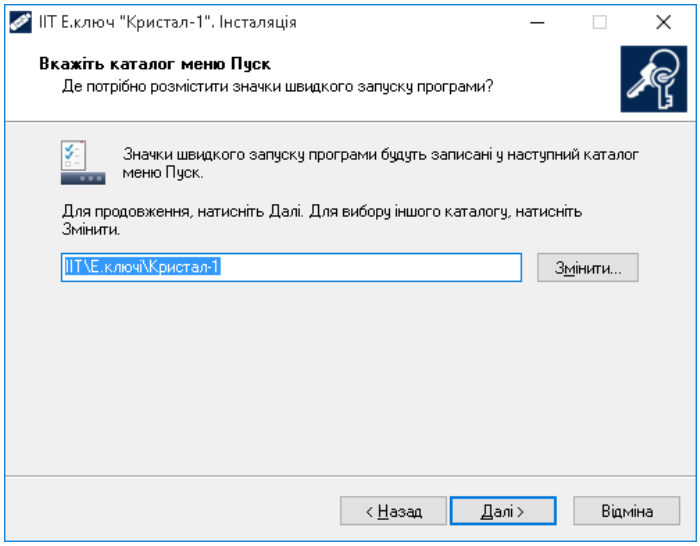
Для встановлення інсталяційного пакету необхідно запустити виконуючий файл EKeyCrystal1Install.exe через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої кнопки миші. Після запуску на екрані з'явиться вікно встановлення програмного забезпечення, необхідно натиснути кнопку «Далі »



У вікні, яке відкрилося та наведено нижче натисніть кнопку «Далі».

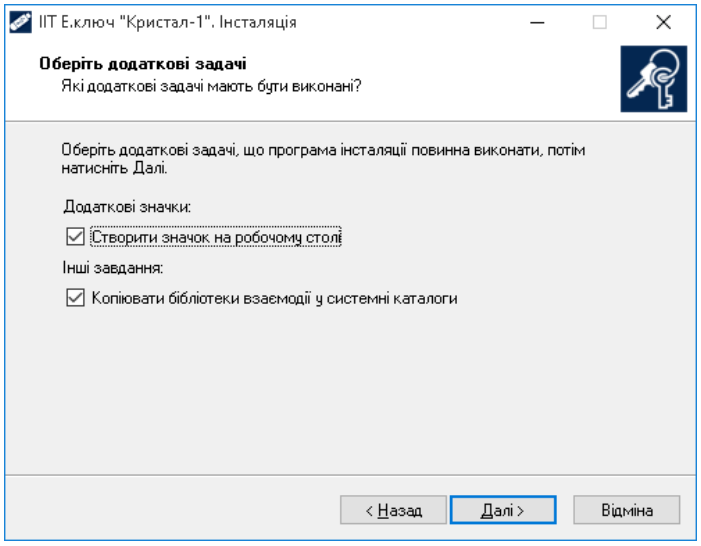


У вікні, яке відкрилося та наведено нижче натисніть кнопку «Далі >».

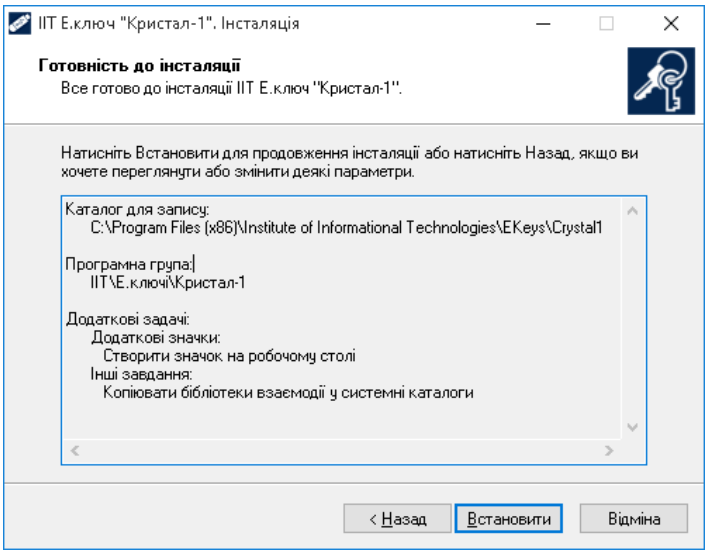


У вікні, яке відкрилося та наведено нижче на рисунку оберіть наступні компоненти для встановлення «Створити значок на робочому столі»,

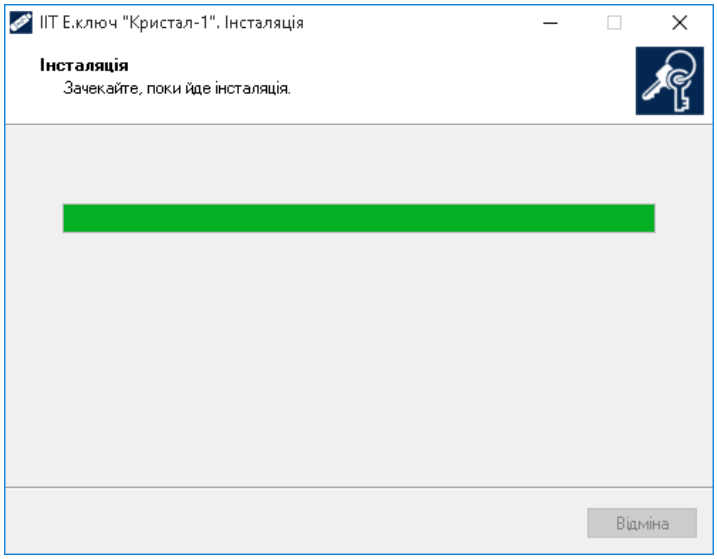
«Копіювати бібліотеки взаємодії у системний каталог» та потім натиснути кнопку «Далі».



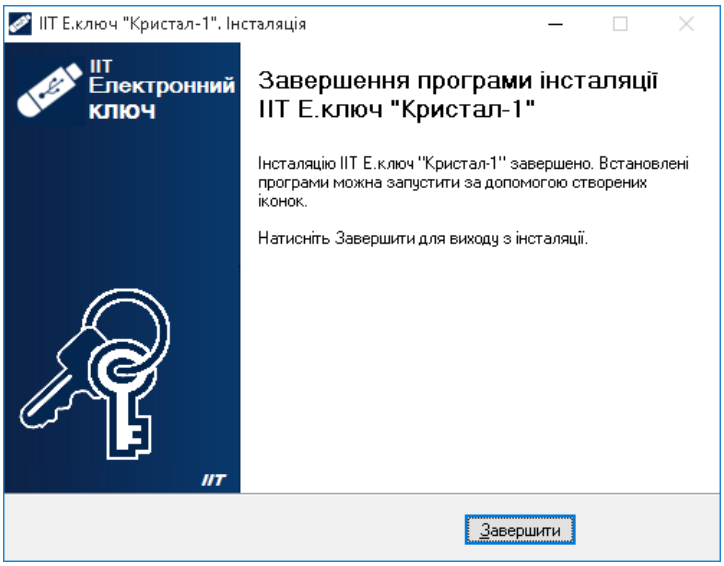
У вікні, яке відкрилося та наведено нижче натисніть кнопку «Встановити».



Дочекайтеся завершення процесу встановлення даного програмного забезпечення.



У вікні яке відкрилося та наведено нижче натисніть кнопку «Завершити» тим самим успішно завершити встановлення програмного забезпечення «ІІТ електронний ключ Кристал-1. Конфігурація».



Примітка: Особливості встановлення програмного забезпечення «ІІТ електронний ключ Кристал-1. Конфігурація» можуть змінюватися його розробником у більш нових версіях даного програмного забезпечення.

Перед запуском програмного забезпечення «Крипто Автограф» скопіюйте Ваші сертифікати відкритого ключа електронного підпису до каталогу C:\My Crt

СЕРТИФІКАТИ

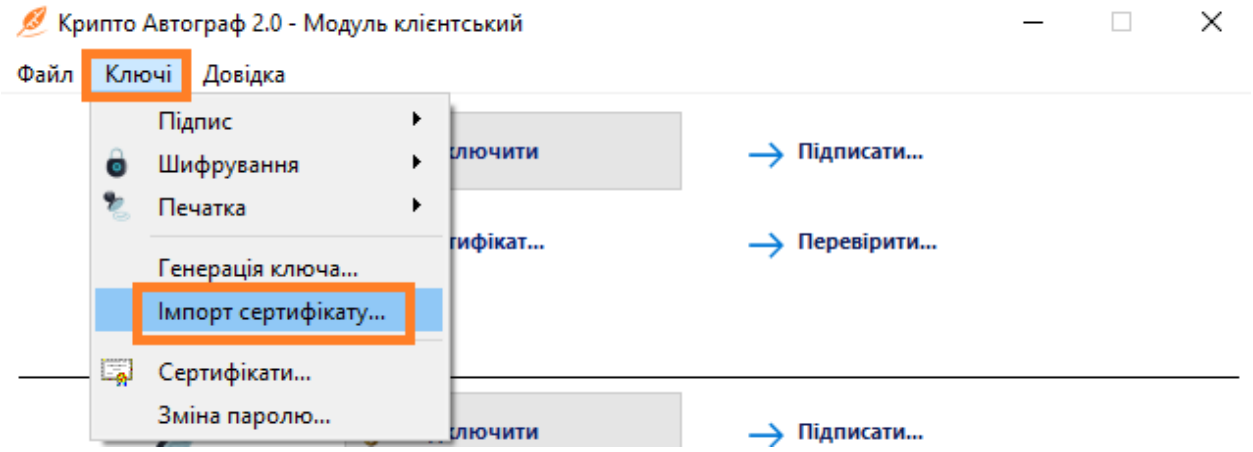
Після генерації ключів та запитів на сертифікат відкритого ключа необхідно звернутися до КНЕДП для генерації сертифікатів на основі згенерованих Вами запитів. Оберіть КНЕДП з переліку доступних, наприклад, на сайті Центрального засвідчувального органу (https://czo.gov.ua/ca-registry). Ознайомтесь з процедурою отримання сертифікатів на сайті обраного КНЕДП, заповніть необхідні документи, скопіюйте файли запитів на знімний носій та зверніться безпосередньо у відділення КНЕДП. Під час заповнення документів рекомендуємо дати згоду на публікацію сертифікатів на сайті КНЕДП.

Отримавши Ваші запити, співробітник КНЕДП допоможе згенерувати сертифікати. Після цього вони будуть опубліковані на сайті КНЕДП (у випадку якщо Ви дали згоду на публікацію). Завантажте сертифікати для їх подальшого імпорту.

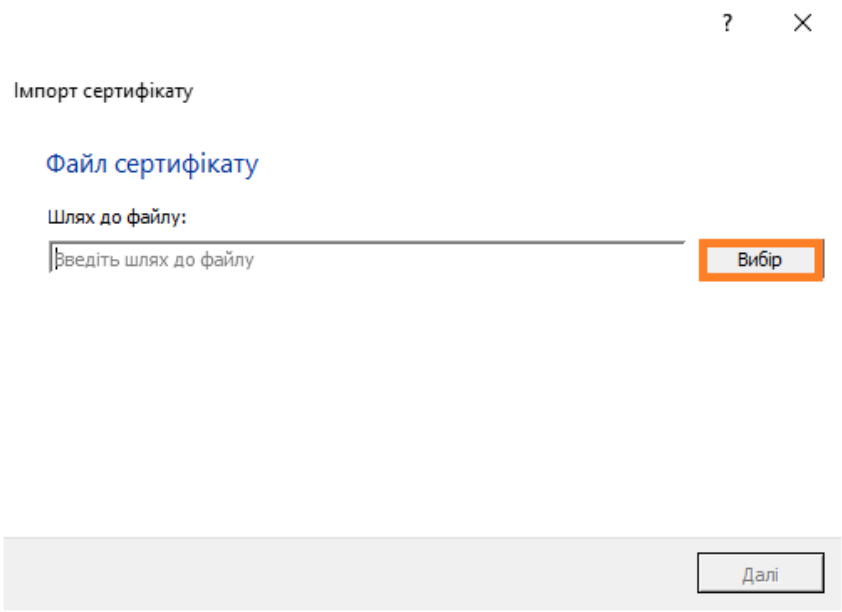
Імпорт сертифікатів

Якщо Ви користуєтесь ключами формату Key-6.dat, .jks, .zs2 необхідно скопіювати сертифікати в каталог C:\My Crt (за замовчуванням), або інший, якщо Ви змінювали його на етапі налаштування Засобу.

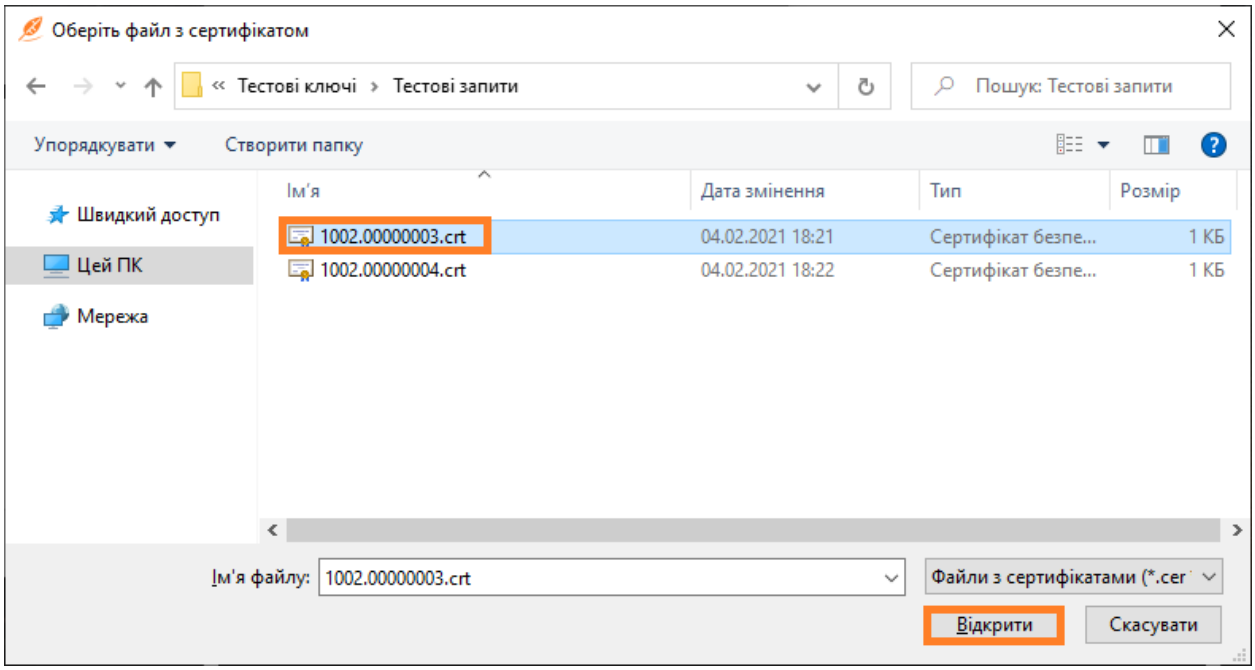
Для імпорту сертифікатів на ЗНКІ натисніть кнопку «Ключі» в горизонтальному меню, потім оберіть «Імпорт сертифікату».



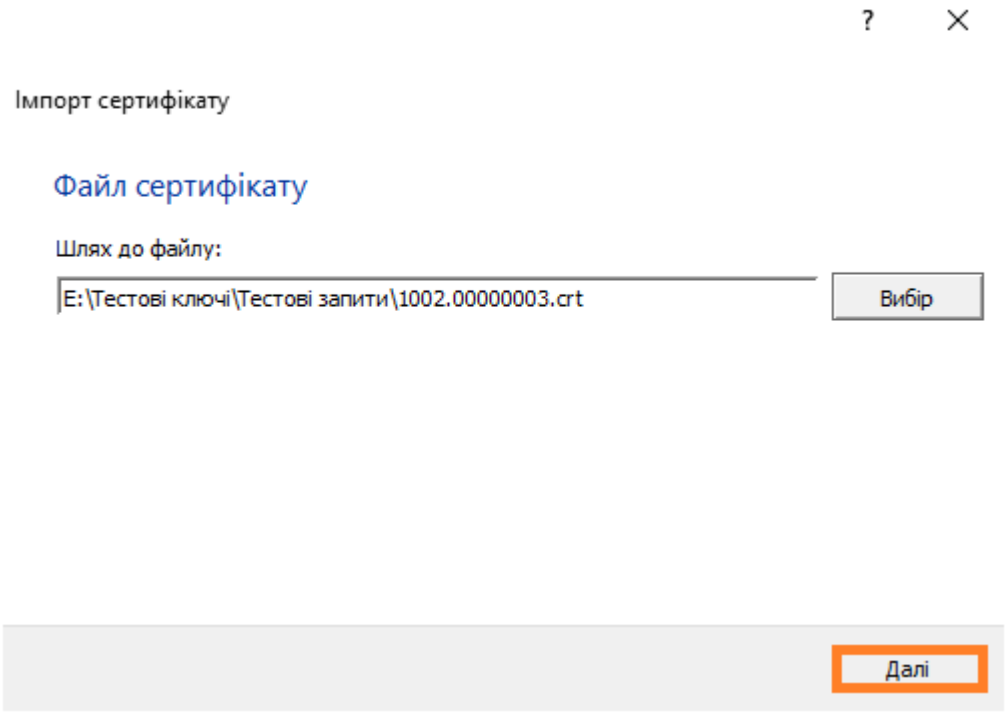
У вікні, що відкрилось і зображено нижче, натисніть кнопку «Вибір» для вибору сертифікату, що необхідно імпортувати.



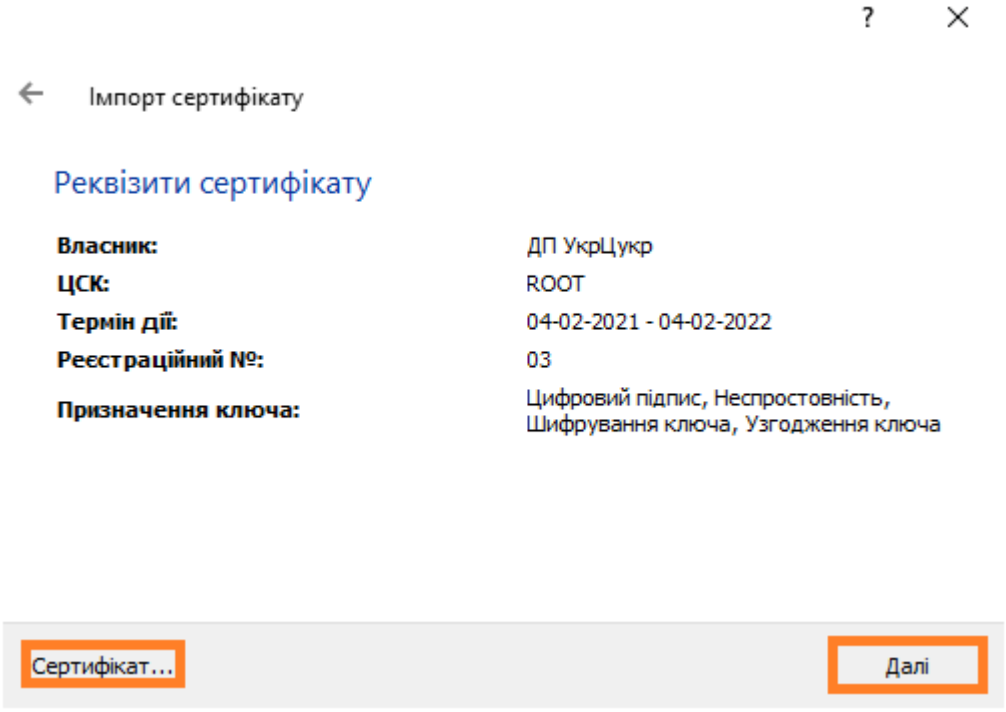
Оберіть в файловому провіднику сертифікат, після обрання натисніть «Відкрити».



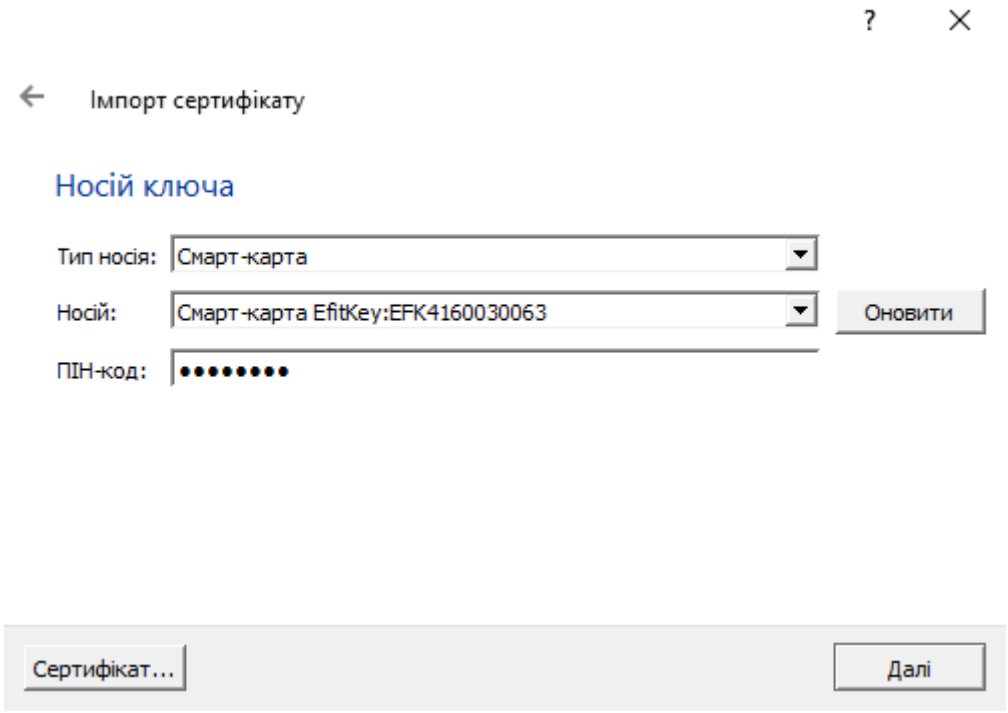
Після вибору натисніть «Далі».



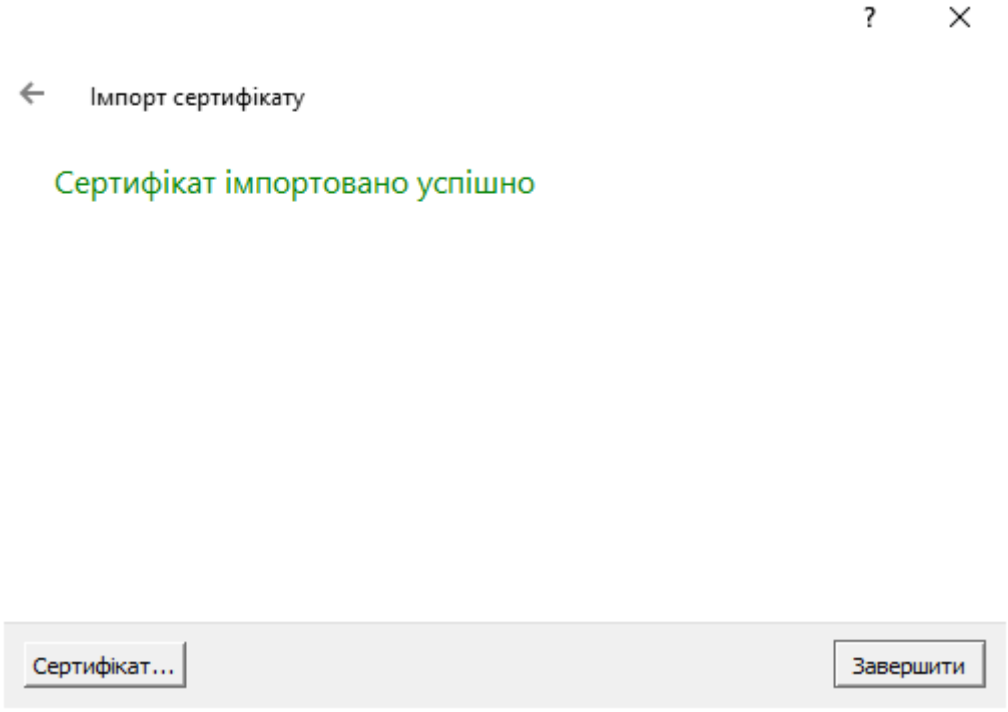
В наступному вікні зображено реквізити власника сертифікату. Натисніть «Далі». Для перегляду сертифікату натисніть «Сертифікат».



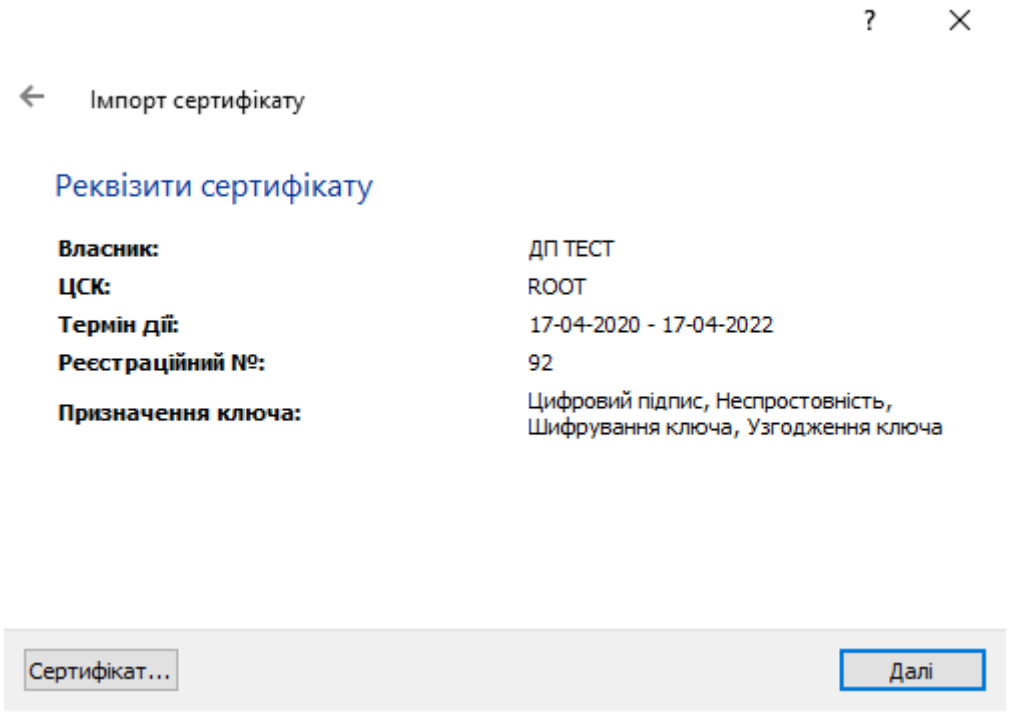
В наступному вікні оберіть носій ключа. В нашому випадку буде розглянуто імпорт на смарт-карту Efit Key. Обравши носій, введіть ПІН-код смарт-карти та натисніть «Далі»



Вікно, що відкрилось і зображено нижче, свідчить про успішний імпорт сертифікату. Натисніть «Завершити».

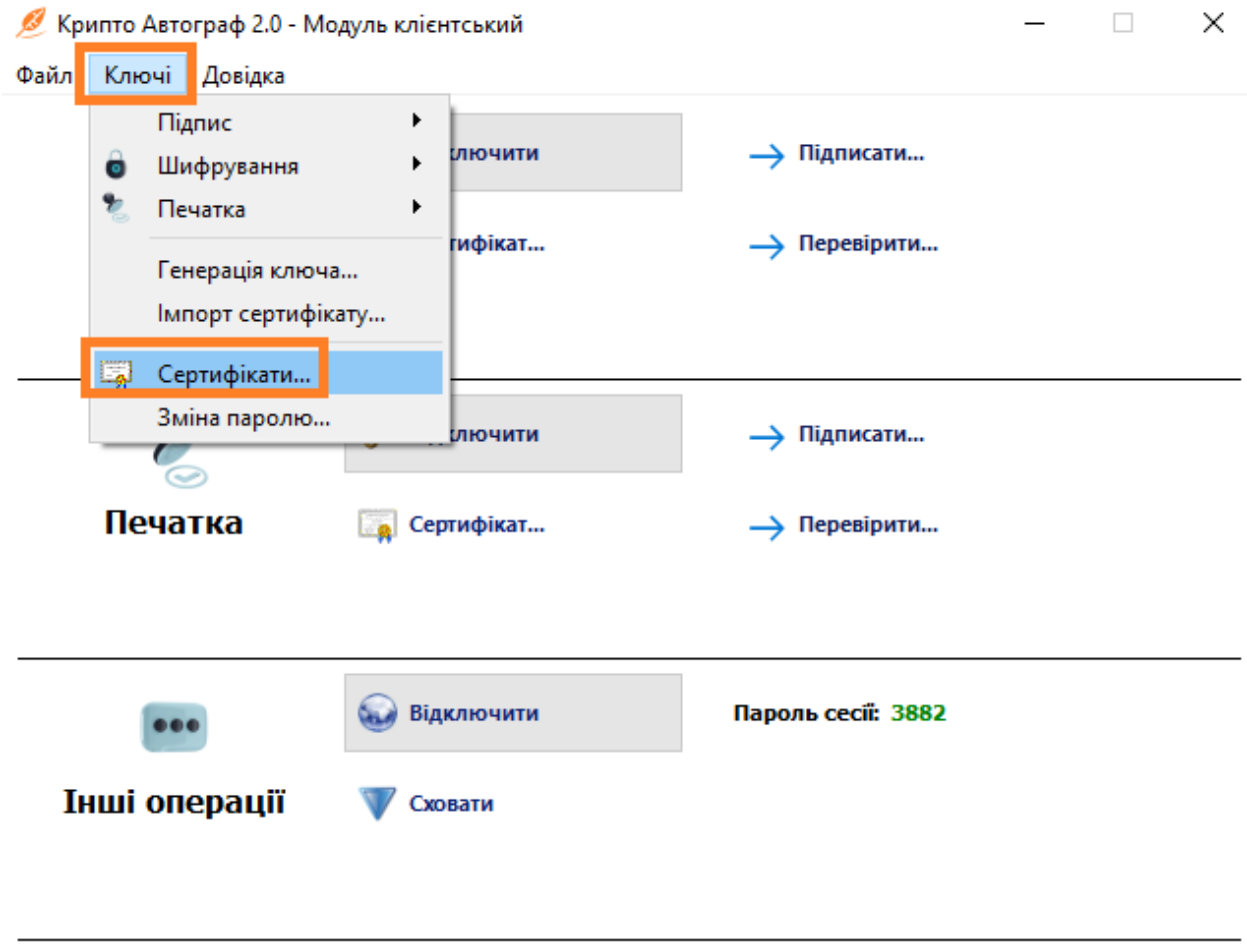


Якщо під час генерації ключів було обрано «Окремі ключі для ЕП та узгодження ключа» необхідно повторити процедуру імпорту з другим сертифікатом. Процедура імпорту другого сертифікату аналогічна до вищеописаної. Нижче зображено вікно з реквізитами другого сертифікату. Порівнявши з реквізитами першого ключа видно, що реєстраційні номери і призначення ключа різні.

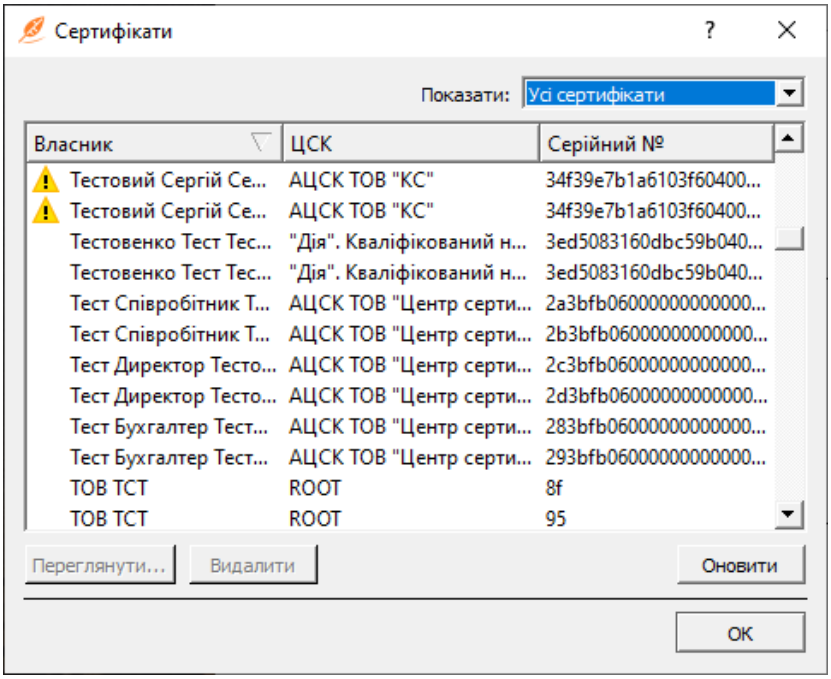


Перегляд сертифікатів

Для перегляду сертифікатів, наявних в каталозі C:\My Crt (за замовчуванням), натисніть в горизонтальному меню кнопку «Ключі», потім – «Сертифікати».

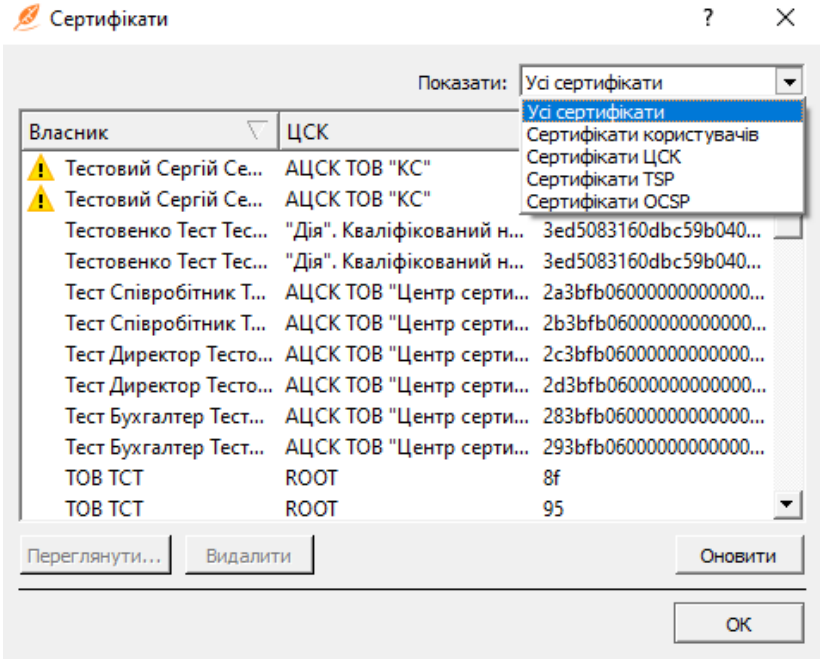


У вікні, що відкрилось і зображено нижче, Ви можете переглянути всі сертифікати наявні в каталозі.

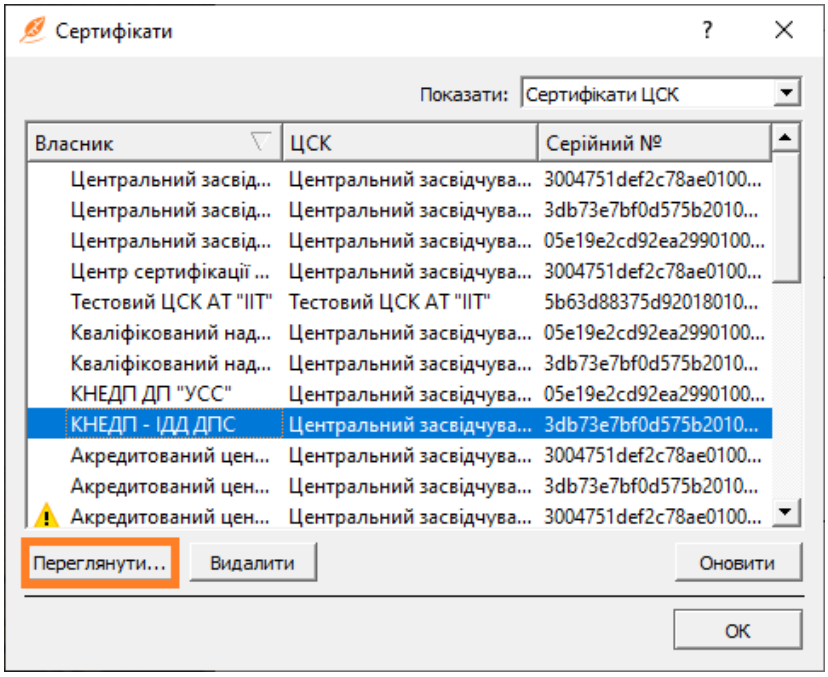


Натисніть на випадаючий список в правому верхньому куті вікна для сортування сертифікатів за призначенням. Доступно п’ять варіантів сортування:

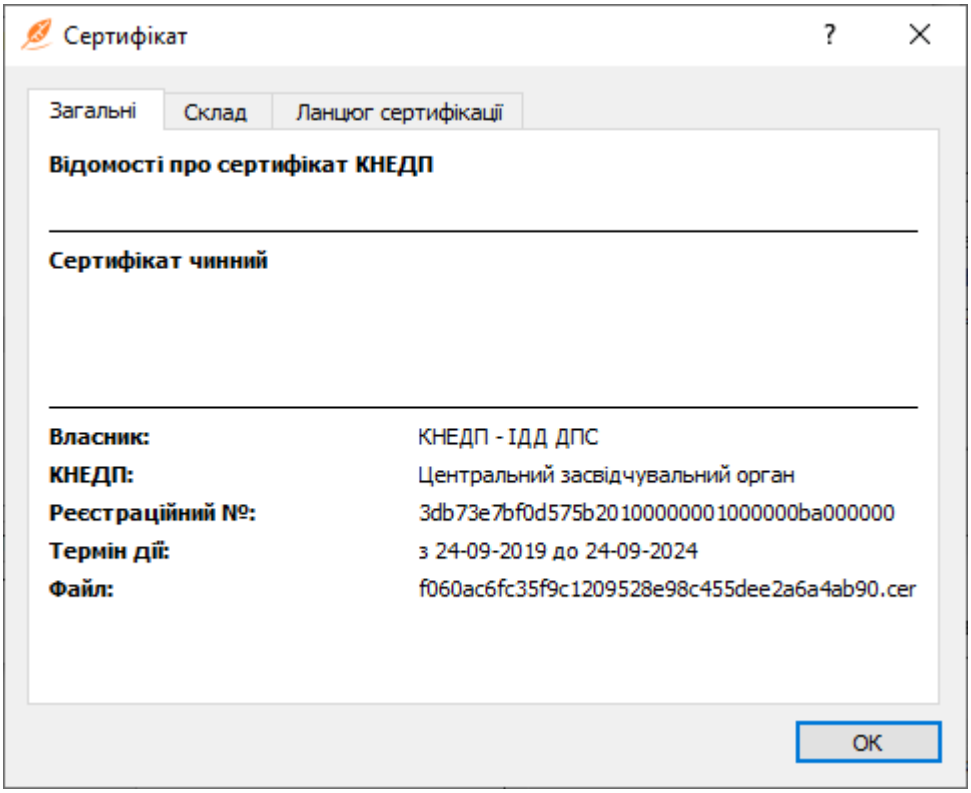
- Усі сертифікати – відображаються усі наявні сертифікати;
- Сертифікати користувачів – відображаються сертифікати відкритого ключа користувача, саме ті, які Ви отримали в КНЕДП;
- Сертифікати ЦСК – відображаються кореневі сертифікати КНЕДП;
- Сертифікати TSP – відображаються сертифікати серверів, що працюють з протоколом TSP;
- Сертифікати OCSP – відображаються сертифікати серверів, що працюють з протоколом OCSP.



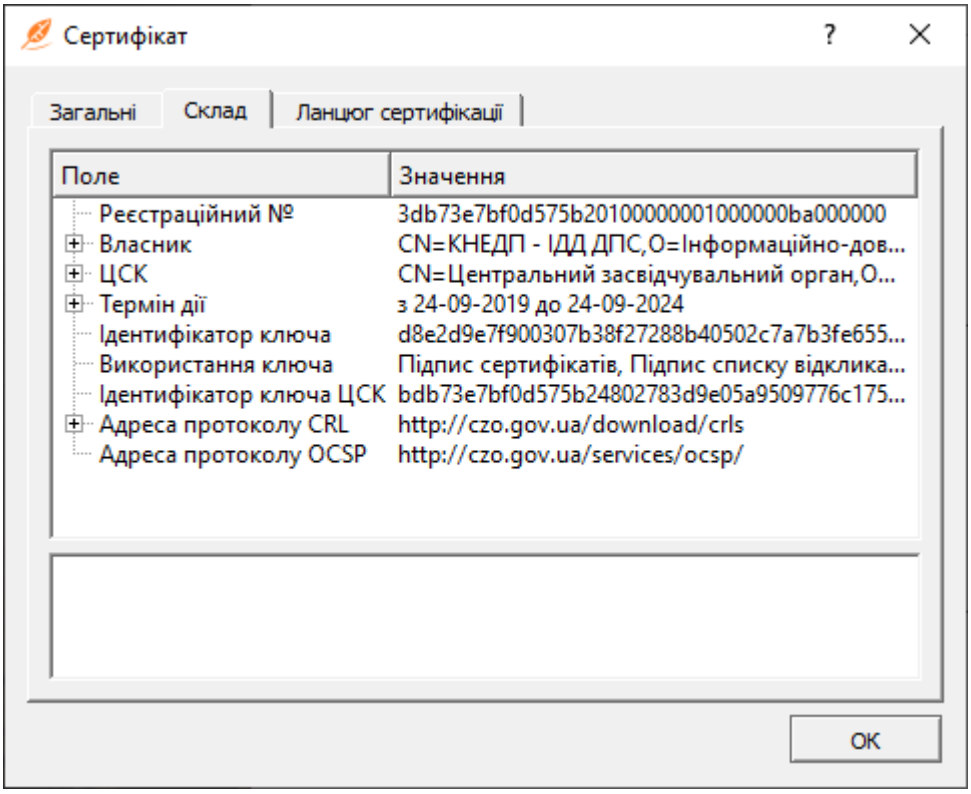
Нижче зображено перелік сертифікатів відсортований за ознакою «Сертифікати ЦСК». Для перегляду інформації про сертифікат виділіть його лівою клавішею миші та натисніть «Переглянути».



У вікні, що відкрилось і зображено нижче, на першій вкладці «Загальні» зображено відомості про сертифікат, про його чинність, термін дії, його власника, реєстраційний номер, КНЕДП, яким було видано даний сертифікат та ім’я файлу цього сертифікату у каталозі C:\My Crt.

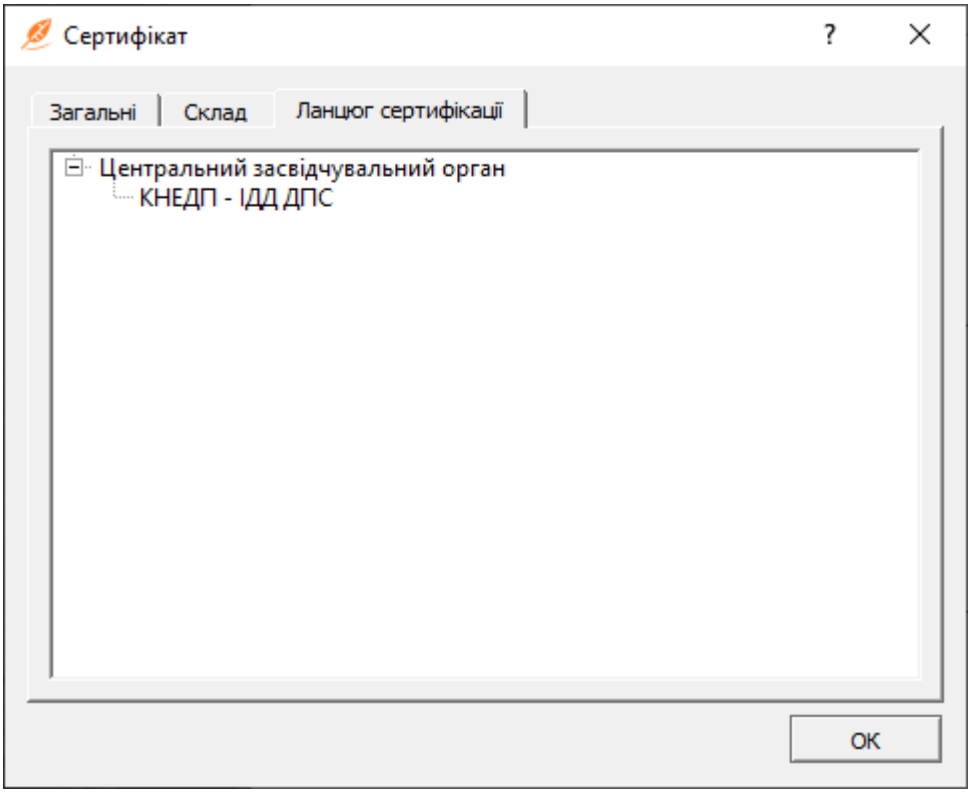


На наступній вкладці «Склад» зображено технічну інформацію про сертифікат.

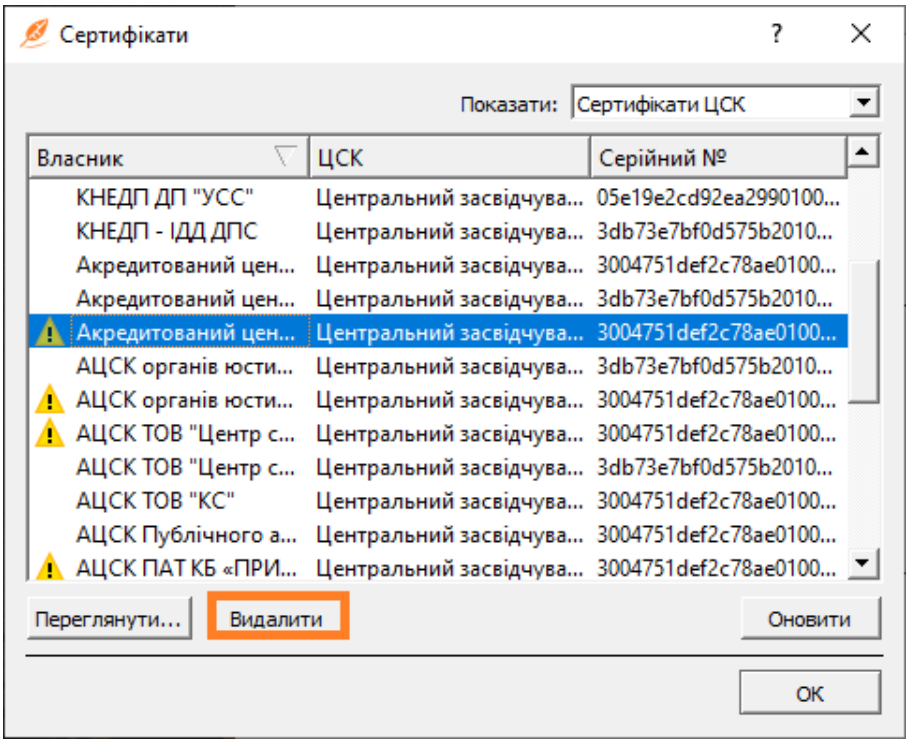


На третій вкладці «Ланцюг сертифікації» зображено послідовність видачі сертифікатів і КНЕДП, що їх видали. Наприклад, кореневий сертифікат КНЕДП буде на другому рівні ланцюга сертифікації, а Ваш особистий сертифікат – на третьому рівні.

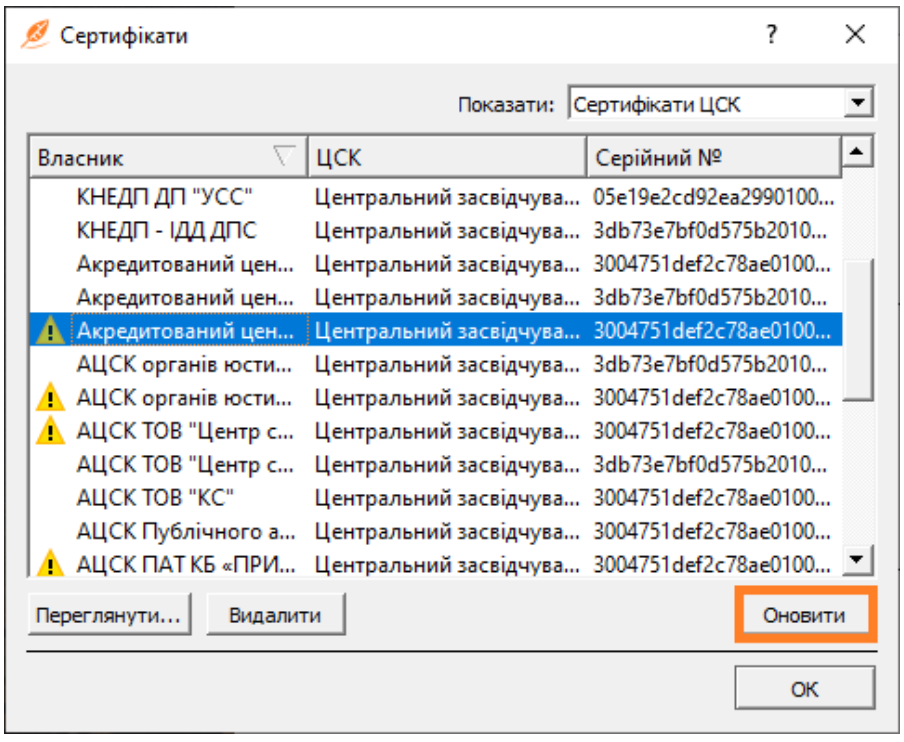
Для завершення перегляду відомостей натисніть «ОК» в правому нижньому куті вікна.



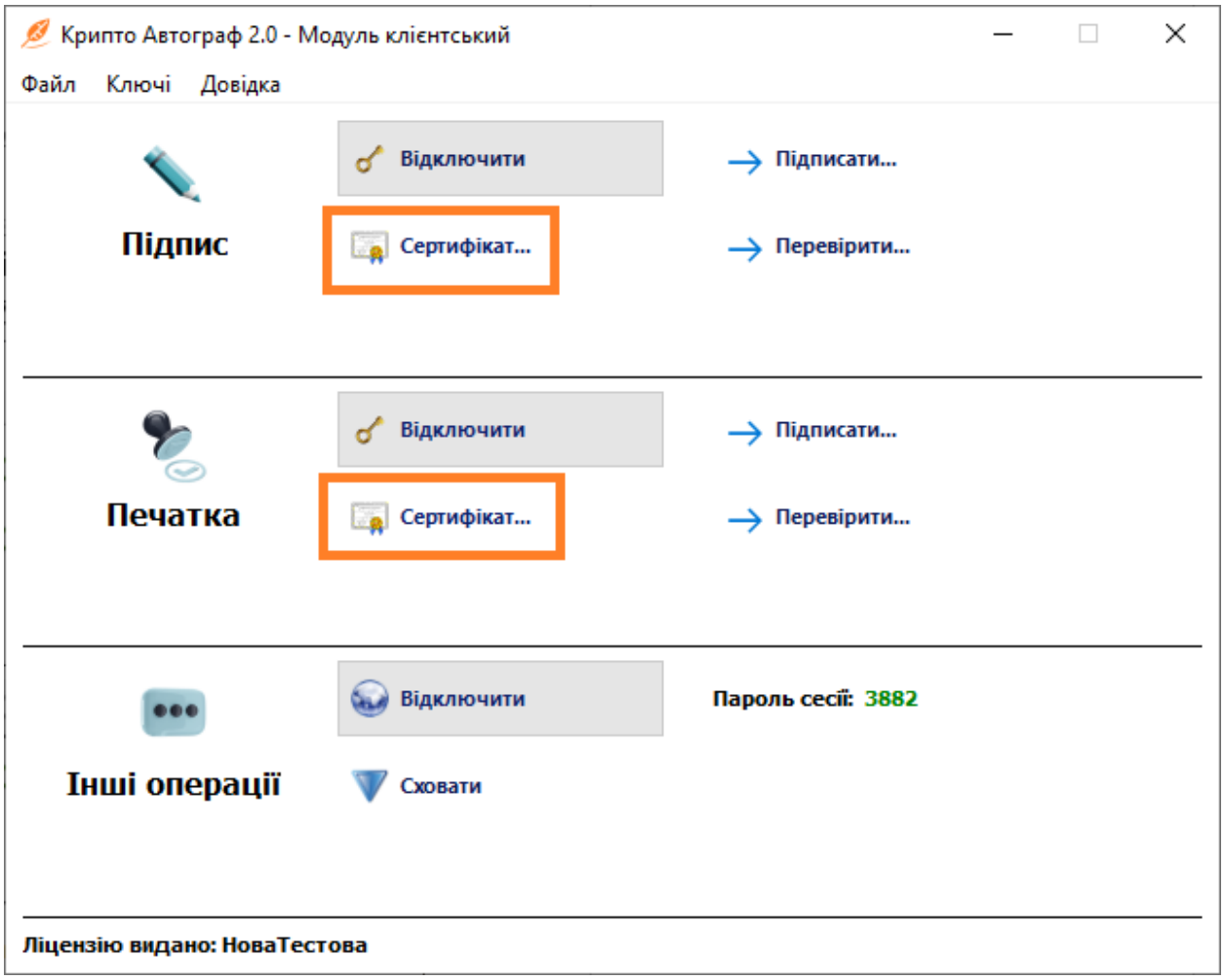
Для видалення сертифікату – виділіть сертифікат натисканням лівої клавіші миші та натисніть «Видалити». Зверніть увагу, що сертифікат видалиться не лише з переліку, а і з каталогу C:\My Crt (за замовчуванням).



У разі якщо Ви скопіювали нові сертифікати в каталог C:\My Crt (за замовчуванням), але їх немає в переліку – натисніть кнопку «Оновити». Після натискання Засіб може деякий час не відповідати, оскільки будуть тривати онлайн-перевірки статусу сертифікатів.

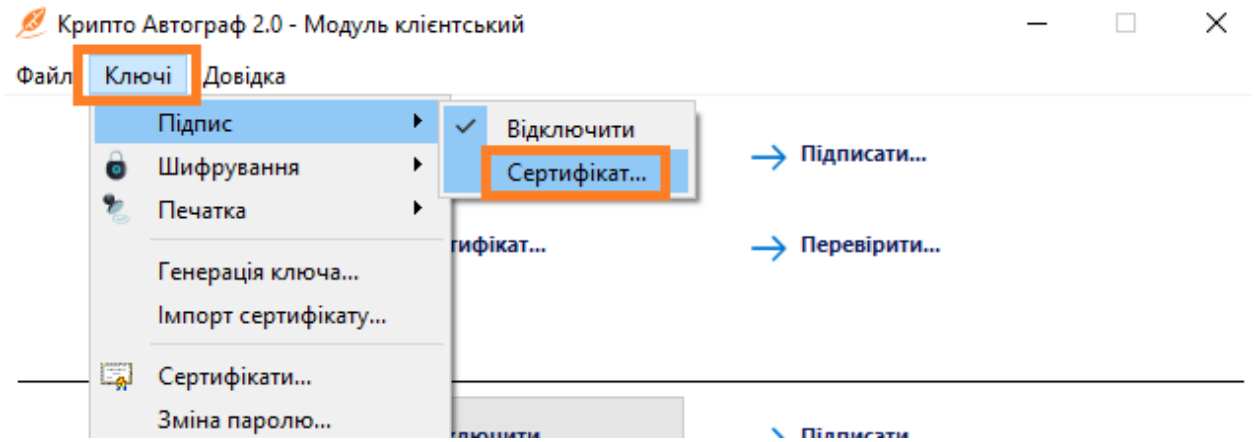


Для перегляду сертифікатів підключених ключів можна скористатися кнопками «Сертифікат» в графічному інтерфейсі Засобу. Кнопки знаходяться в кожному з трьох розділів: «Підпис», «Шифрування», «Печатка».



Після натискання на одну з цих кнопок відкриється вікно відомостей про конкретний сертифікат даного ключа ЕП, електронної печатки чи ключа шифрування.

Також можна скористатися горизонтальним меню, оберіть пункт «Ключі, далі оберіть один з трьох пунктів: «Підпис», «Шифрування» чи «Печатка», потім оберіть «Сертифікат».



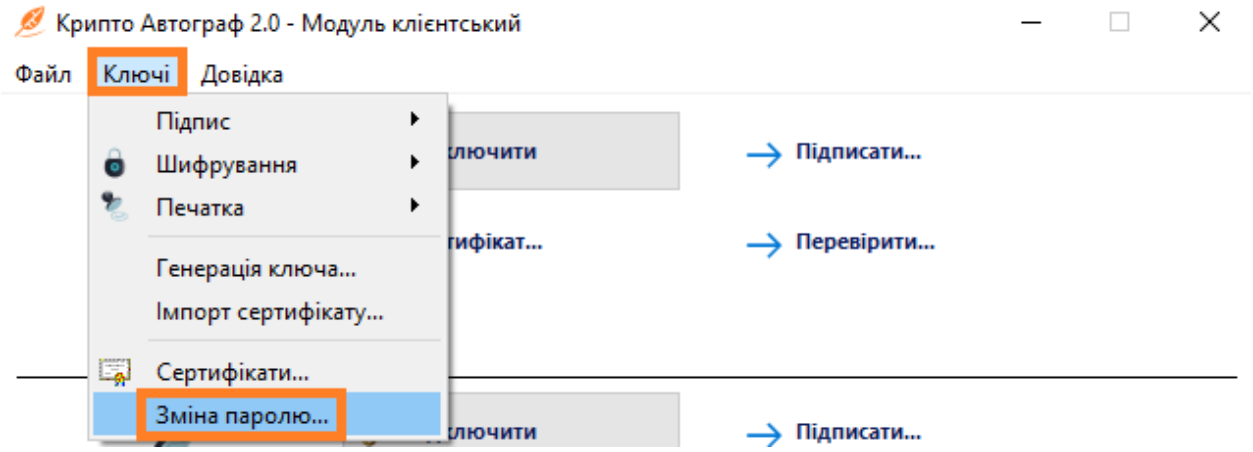
Автоматичне завантаження кореневих сертифікатів КНЕДП

Періодично кожен КНЕДП формує нові кореневі сертифікати. Їх необхідно також завантажувати в каталог C:\My Crt для коректної роботи Засобу, перевірки підписаних файлів та побудови повних ланцюгів сертифікації. Для зручності реалізовано механізм, коли Засіб звертається до серверу і у разі виявлення нових кореневих сертифікатів КНЕДП, автоматично завантажує їх до каталогу C:\My Crt.

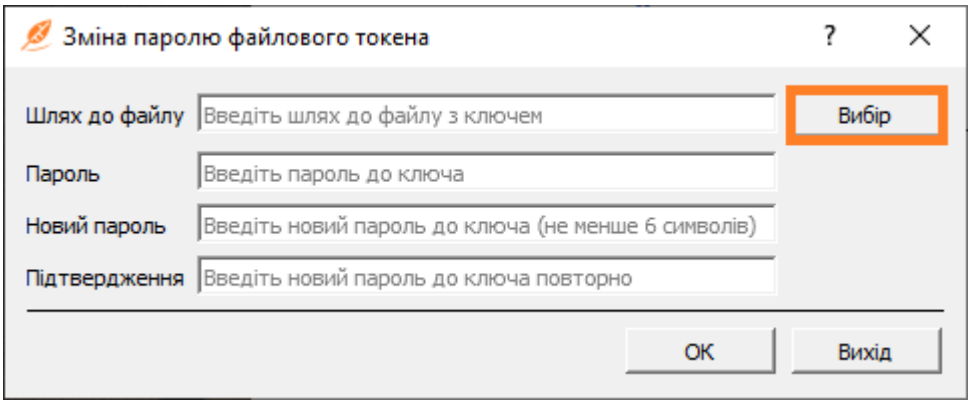
ЗМІНА ПАРОЛЮ

Для зміни паролю файлового токену оберіть в горизонтальному меню пункт «Ключі», далі натисніть «Зміна паролю». Зміна можлива в файлових токенах наступних форматів:

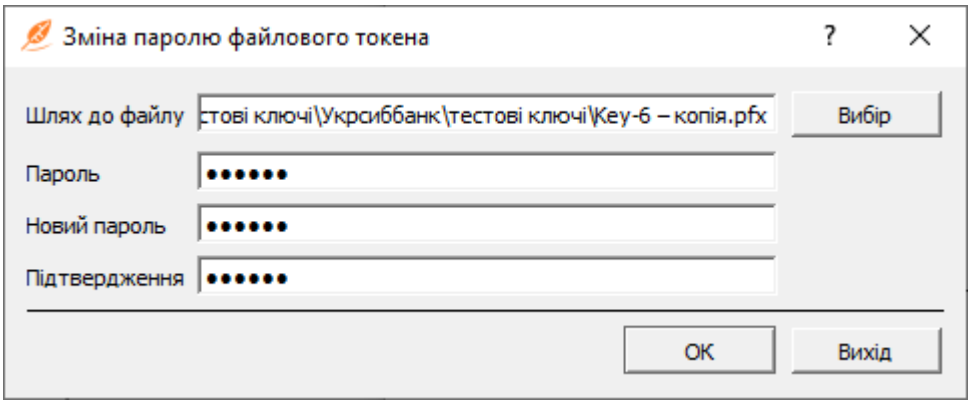
- .pk8;
- .cnt;
- .tok;
- .pfx.



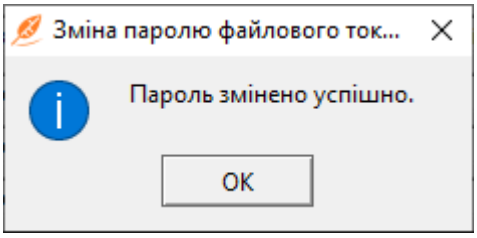
У вікні, що відкрилося і зображено нижче, натисніть кнопку «Вибір» для обрання файлового токену, в якому Ви бажаєте змінити пароль.



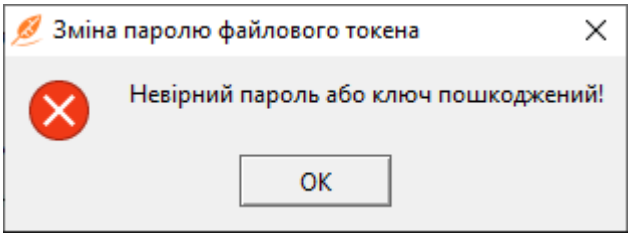
Обравши файловий токен, введіть діючий пароль, новий пароль і підтвердження нового паролю. Після введення паролів натисніть «ОК» для завершення процедури зміни.



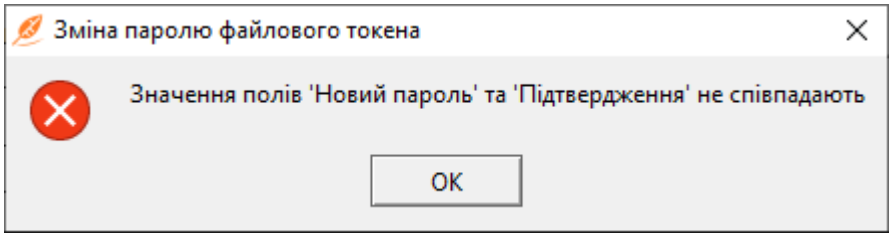
В результаті процедури має з’явитися вікно про успішну зміну паролю. Натисніть «ОК».



У разі введення невірного діючого паролю з’явиться помилка зображена нижче.



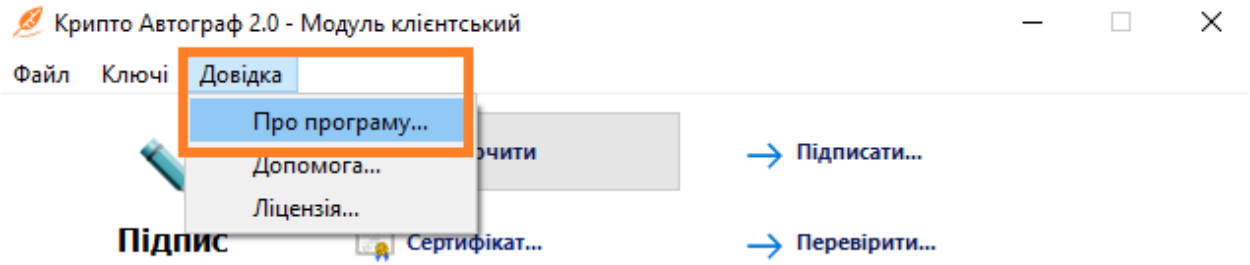
У разі невідповідності нового паролю і його підтвердження з’явиться помилка зображена нижче.

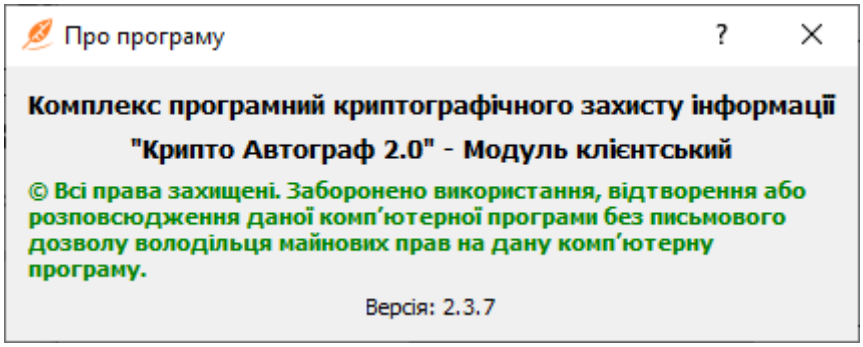


ДОВІДКА

Версія Засобу

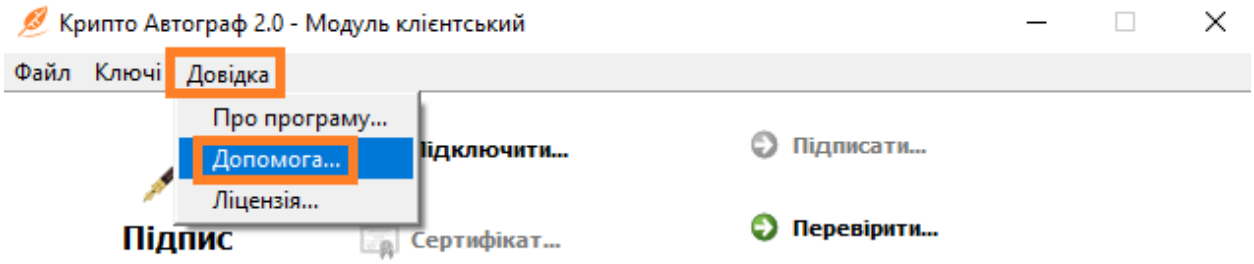
Для того щоб дізнатися версію встановленої програми в горизонтальному меню оберіть пункт «Довідка», потім натисніть «Про програму».





Допомога

У разі виникнення питань щодо роботи Засобу, Ви можете звернутися до технічної підтримки ТОВ «Науково-виробниче підприємство "СМАРТ СОЛЮШЕНС». Для цього перейдіть за посиланням: http://smartsolutions.kiev.ua/uk/kontakty



ПРОТОКОЛЮВАННЯ ПОДІЙ КЛІЄНТСЬКОЇ КОМПОНЕНТИ ЗАСОБУ

Клієнтська складова Засобу веде протоколювання власної роботи у файлі протоколу (log-file). Запустіть Засіб з правами адміністратора після цього За замовченням файл протоколу зберігається тут: C:\Program Files (x86)\CryptoAutograph→ файл (CryptoAutograph.log).

Орієнтовно файл протоколу містить наступну форму викладення змісту:

2018.12.22|11:49:19|W|Start application

2018.12.22|11:49:20|W|Web-module: started [port:11111, mode: non secure]

2018.12.22|11:49:22|E|Loading file error: File length limit. Path:C:/My Crt\UA-39384476.crl [ca_crl.cpp:298]

2018.12.22|12:43:23|W|CommandSignData(3d94b18):OCSP request: url: http://acskidd.gov.ua/services/ocsp/

2018.12.22|12:43:23|W|HTTP request: url:http://acskidd.gov.ua/services/ocsp/

2018.12.22|12:43:23|W|CommandSignData(3d94b18):CommandResult:[code:0, desc:Success, key:UserKey[current=KeyPair[isValid:1, cert=Certificate[subject=Тестовий Тест Тестович, issuer=Акредитований центр сертифікації ключів ІДД ДФС, sn=33b6cb7bf721b9ce04000000cbd11a00ef5e5700, ku=[data sign, non repudation], val=27-04-2017 00:00:00-27-04-2019 00:00:00]], keysCount=2]]

2018.12.22|12:43:23|W|Crypto command (file) result: CommandResult:[code:0, desc:Success, key:UserKey[current=KeyPair[isValid:1, cert=Certificate[subject=Тестовий Тест Тестович, issuer=Акредитований центр сертифікації ключів ІДД ДФС, sn=33b6cb7bf721b9ce04000000cbd11a00ef5e5700, ku=[data sign, non repudation], val=27-04-2017 00:00:00-27-04-2019 00:00:00]], keysCount=2]]

2018.12.22|12:43:35|W|CommandVerifyData(3d94b18):CommandResult:[code:0, desc:Success]

2018.12.22|12:43:35|W|Crypto command (file) result: CommandResult:[code:0, desc:Success]

2018.12.22|12:43:54|W|CommandEncryptData(3dde040):OCSP request: url: http://acskidd.gov.ua/services/ocsp/

2018.12.22|12:43:54|W|HTTP request: url:http://acskidd.gov.ua/services/ocsp/

2018.12.22|12:43:54|W|CommandEncryptData(3dde040):OCSP request: url: http://acskidd.gov.ua/services/ocsp/

2018.12.22|12:43:54|W|HTTP request: url:http://acskidd.gov.ua/services/ocsp/

2018.12.22|12:43:55|W|CommandEncryptData(3dde040):CommandResult:[code:0, desc:Success, key:UserKey[current=KeyPair[isValid:1, cert=Certificate[subject=Тестовий Тест Тестович, issuer=Акредитований центр сертифікації ключів ІДД ДФС, sn=33b6cb7bf721b9ce04000000cbd11a00f05e5700, ku=[key agree], val=27-04-2017 00:00:00-27-04-2019 00:00:00]], keysCount=2]]

2018.12.22|12:43:55|W|Crypto command (file) result: CommandResult:[code:0, desc:Success, key:UserKey[current=KeyPair[isValid:1, cert=Certificate[subject=Тестовий Тест Тестович, issuer=Акредитований центр сертифікації ключів ІДД ДФС, sn=33b6cb7bf721b9ce04000000cbd11a00f05e5700, ku=[key agree], val=27-04-2017 00:00:00-27-04-2019 00:00:00]], keysCount=2]]

2018.12.22|12:44:17|W|CommandDecryptData(3cf5548):CommandResult:[code:9, desc:Not found user key for decrypt]

2018.12.22|12:44:17|W|Crypto command (file) result: CommandResult:[code:9, desc:Not found user key for decrypt]

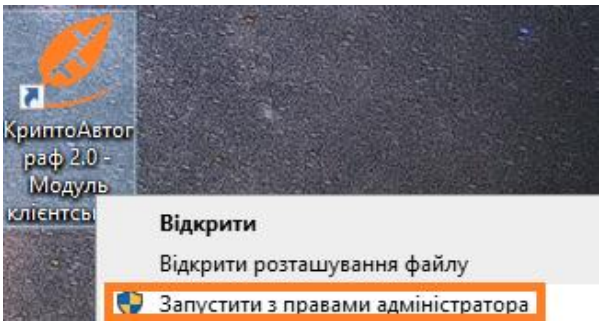
Роз’яснення основних подій зафіксованих в файлі протоколу.

ПОМИЛКА	ЗНАЧЕННЯ
License read success	Ліцензійний файл в наявності
Error (java.io.FileNotFoundException:	Ліцензійний файл відсутній
Error reading private key	Помилка використання (читання) особистого ключа
Private key read successfully	Особистий ключ успішно використаний (зчитаний)
Return code=22	Невідповідність ідентифікаторів відкритого та особистого ключа. Сертифікат відкритого ключа пошкоджено, відсутній, обрано особистий ключ відмінний від сертифіката відкритого ключа.
Return code=23	Введено невірний пароль доступу до особистого ключа
Return code=30	Невірний формат вхідних даних
Return code=31	Невірний формат сертифіката відкритого ключа
Return code=35	Невірний формат підписаних даних - конверту електронного підпису (Cryptographic Message Syntax)
Return code=38	Невірний формат конверту з шифрованими даними (формат криптографічного повідомлення)
Sign file success:	Дані (файл) успішно підписані

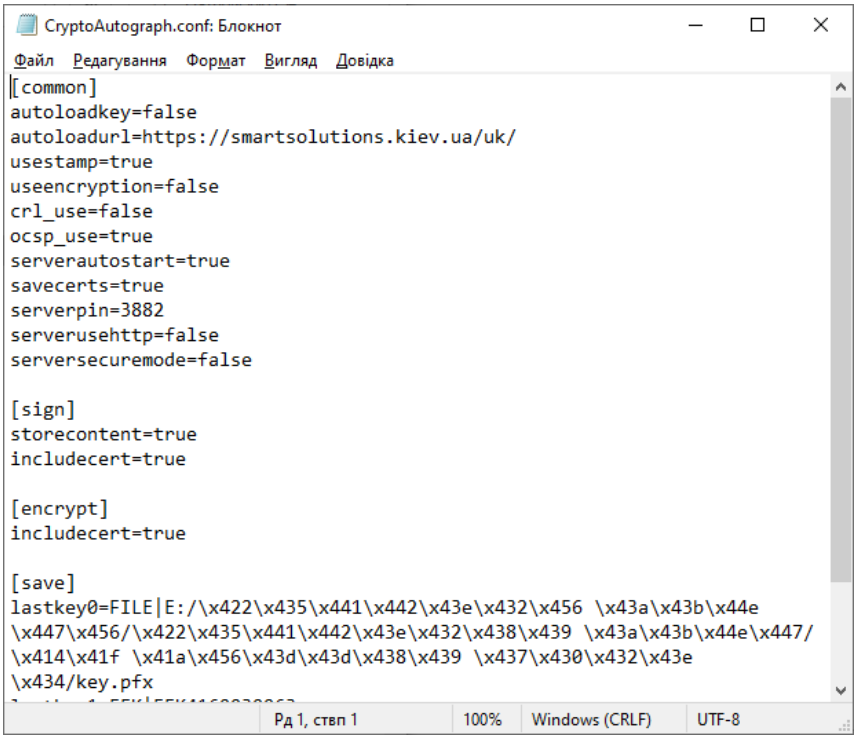
VerifySign file success	ЕП даних (файлу) успішно перевірено
Crypt file success	Дані (файл) успішно зашифровані
Decrypt file success	Дані (файл) успішно розшифровані

КОНФІГУРАЦІЯ ЗАСОБУ

Для конфігурація Засобу шляхом редагування файлу конфігурації необхідно запустити Засіб з правами адміністратора.



Після запуску з правами адміністратора в каталозі C:\My Crt з’явиться файл конфігурації: «CryptoAutograph.conf». Відкрийте його будь-яким текстовим редактором. Нижче зображено приблизний зміст файлу.



Нижче в таблиці вказані і описані параметри файлу конфігурації.

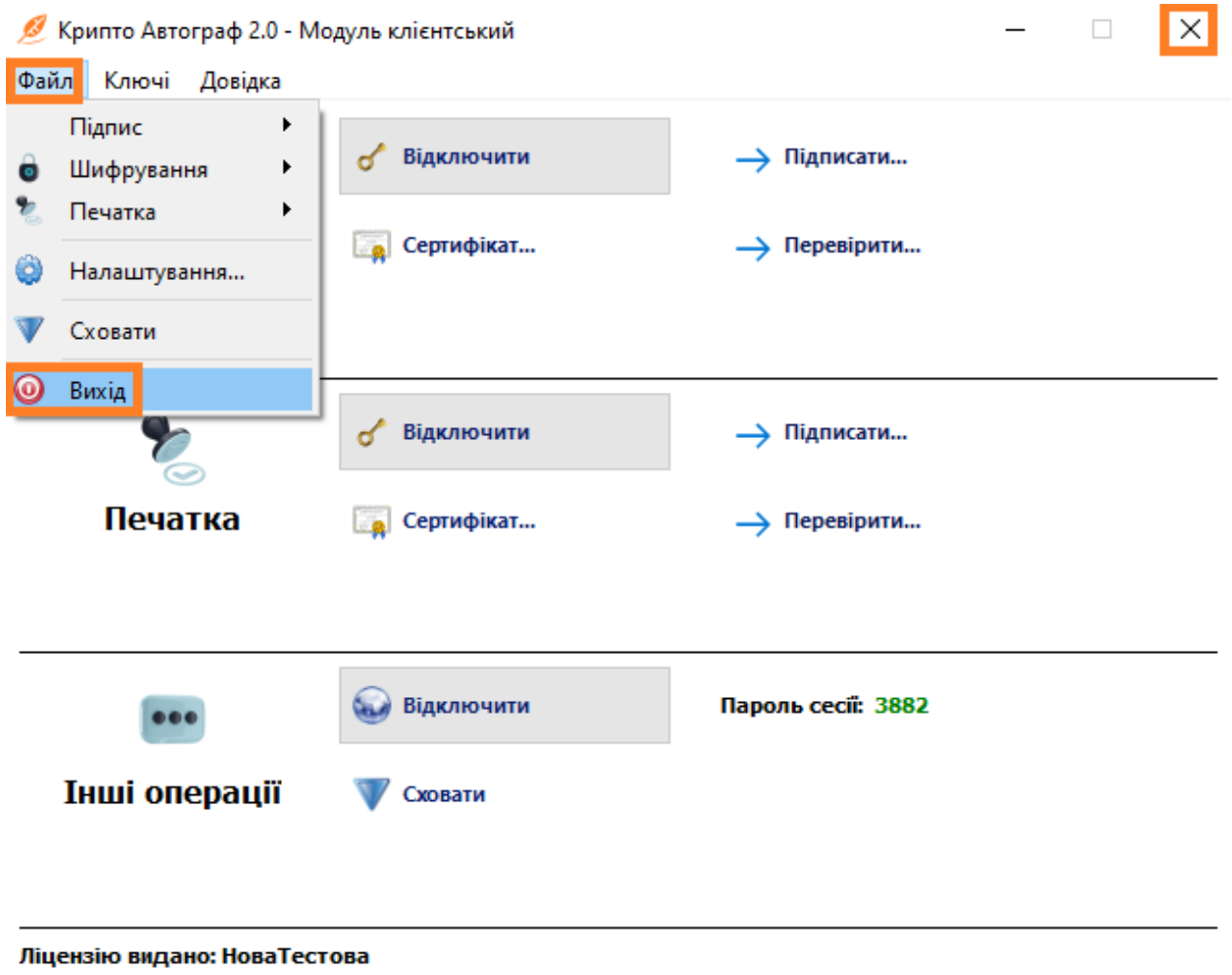
ПАРАМЕТР	ОПИС (ЗНАЧЕННЯ)
Секція [common]	
certs	Шлях до файлового сховища (certs=C:\My Crt)
port	Порт серверної компоненти Засобу (port=11111)
serverautostart	Включати веб-модуль під час запуску Засобу (для взаємодії з серверною компонентою) (true/false)
serversecuremode	Включати захищений режим WSS (для протоколу HTTPS) (для взаємодії з серверною компонентою) (true/false)
serverusehttp	Включати HTTP (для взаємодії з серверною компонентою) (true/false)
supportiit	Доступність ключів типу Key6.dat (true/false)
savecerts	Збереження сертифікатів з електронних конвертів (true/false)
maxfilesize	Максимальний розмір оброблюваних для підпису/шифрування файлів (за замовчуванням 50 МБ, значення вказується у байтах) (maxfilesize=52428800)
crl_use	Використання списків відкликаних сертифікатів (CBC, CRL) (true/false)
ocsp_use	Використання протоколу визначення статусу сертфіката (true/false)
usestamp	Використання електронної печатки (true/false). Додає/прибирає в графічне меню розділ «Печатка».
useencryption	Використання шифрування (true/false). Додає/прибирає в графічне меню розділ «Шифрування».
autoloadkey	Автоматичне підключення ключа ЕП з флеш-накопичувача (true/false)

autoloadurl	Шлях до ключа ЕП з флеш-накопичувача. Працює при умові, що autoloadkey=true. (autoloadurl=F:\Key-6.dat)
serverpin	Використання фіксованого паролю сесії веб-модуля (serverpin=1111)
certs_download_url	Посилання на серверний каталог з кореневими сертифікатами та файлом їх опису (certs.json). За замовчуванням certs_download_url= https://smartsolutions.kiev.ua/download/CryptoAutograph/certs
certs_download_timeout	Затримка перед запитом на файл certs.json. За замовчуванням 60 секунд, вказується у секудах.
Секція [sign]	
storecontent	Додавати до конверту дані (true/false)
includecert	Додавати до конверту сертифікат підписувача (true/false)
addtimestamp	Використовувати позначку часу (true/false)
tsurl	Посилання на сервер позначки часу (tsurl=)
Секція [encrypt]	
includecert	Додавати до конверту сертифікат відправника (true/false)
Секція [proxy]	
use	Використання проксі-сервера (true/false)
host	IP-адреса проксі сервера (host=165.20.12.49)
port	Порт проксі-сервера (port=3128)
auth	Авторизація користувача на проксі-сервері (true/false)
user	Обліковий запис для доступу (user=login)
pass	Пароль облікового запису (pass=passw0rd)

Секція [http]	
max_request_size	Максимальний розмір файлу, що може бути прийнятий на API (значення вказується у байтах)

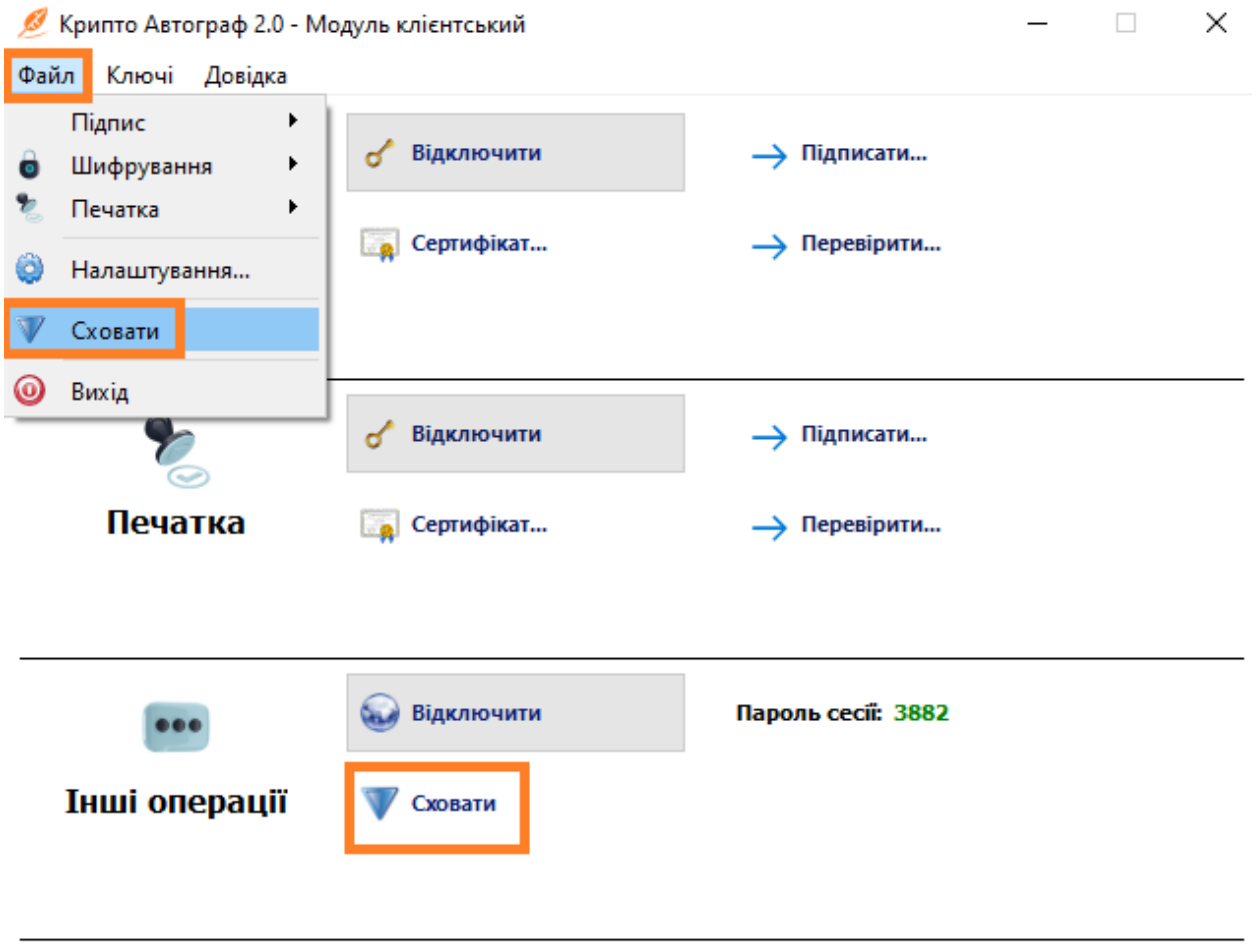
ЗАВЕРШЕННЯ РОБОТИ

Для завершення роботи в Засобі натисніть «Х» в правому верхньому куті вікна або в горизонтальному меню оберіть пункт «Файл», далі натисніть «Вихід».

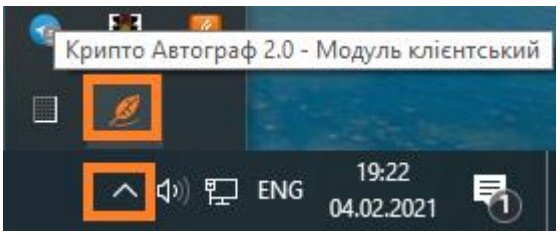


Для того щоб згорнути Засіб в системний трей натисніть «Сховати» в нижній частині графічного інтерфейсу Засобу.

Або в горизонтальному меню оберіть пункт «Файл», далі натисніть «Сховати».



Для того щоб відновити вікно Засобу, в правому нижньому куті екрану натисніть на стрілку, щоб розгорнути список згорнутих програм. Далі в списку знайдіть ярлик Крипто-Автограф і розгорніть його подвійним натисканням лівої клавіші миші.



Або натисніть на ярлик Засобу правою клавішею миші та оберіть пункт «Показати».