ІНСТРУКЦІЯ КОРИСТУВАЧА
З ГЕНЕРАЦІЇ КЛЮЧА ТА ЙОГО СЕРТИФІКАЦІЇ В ЦЕНТРІ СЕРТИФІКАЦІЇ КЛЮЧІВ (ЦСК) БАНКУ (варіант генерації через SOFT GenKeyCtx)

Генерація ключа

1. Встановити програмне забезпечення (ПЗ) «`Генератор ключів v1`» за посиланням на сайті ЦСК «АТ Укрексімбанк» (https://ca.eximb.com): https://ca.eximb.com/storage/app/media/Software/x86/setup_CiX509_CTXCreator.zip

2. Запустити (ПЗ) «`Генератор ключів v1`» (Рис. 1.).

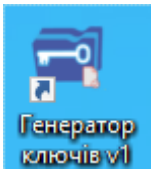

Рис. 1.

3. У вікні, що з’явиться, обрати тип власника ключа (підписувача), та натиснути кнопку «`Прийняти`» (Рис. 2.).

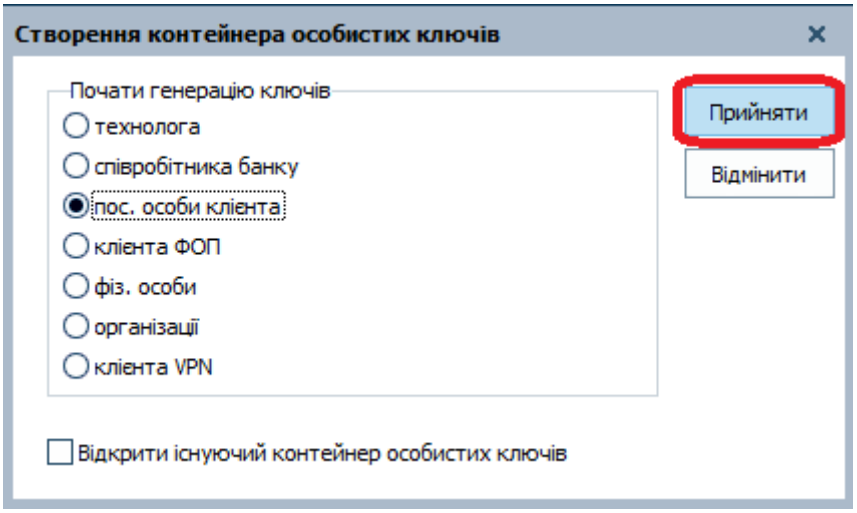

Рис. 2.

4. У наступному вікні заповнити анкету підписувача.

Примітки:
1. Обов’язково заповнюються:
ПІБ, назва організації, посада підписувача, країна, адреса, e-mail, код ЄДРПОУ організації, ІПН (ідентифікаційний код фізичної особи) підписувача (або серія та номер паспорту), телефон, фраза для блокування сертифіката.

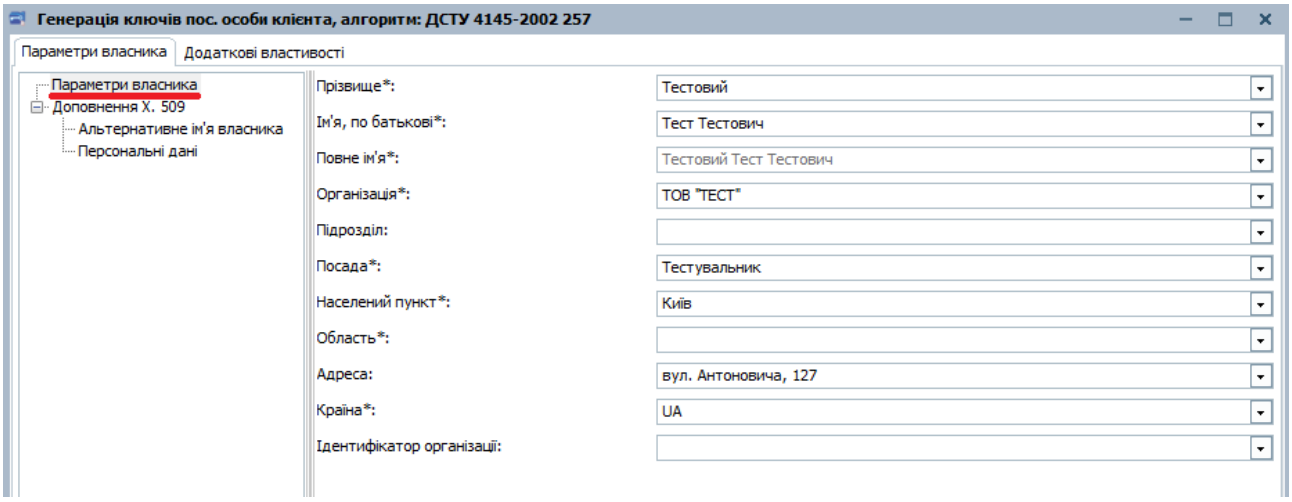

Рис. 3.

Рис. 4.

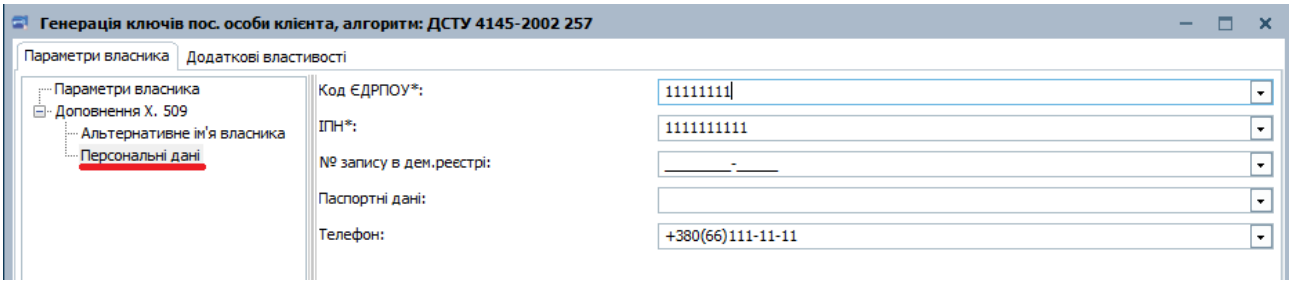

Рис. 5.

Рис. 6.

В залежності від типу носія ключової інформації (файловий ключовий контейнер або USB-токен – «SafeNet», SC-337 «Автор»):

4.1. У випадку файлового носія:

- обрати «Тип» носія – «Файл на диску»,
- придумати та ввести «Пароль» до файлу ключа і підтвердити пароль («Підтвердження»),

- натиснути кнопку «...», і у вікні, що з’явиться, обрати каталог для зберігання ключа та натиснути «Открыть» (Рис. 8.).

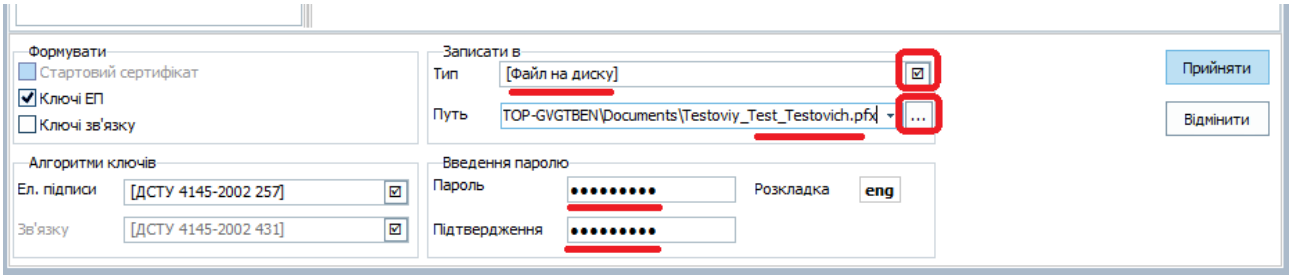

Рис. 7.

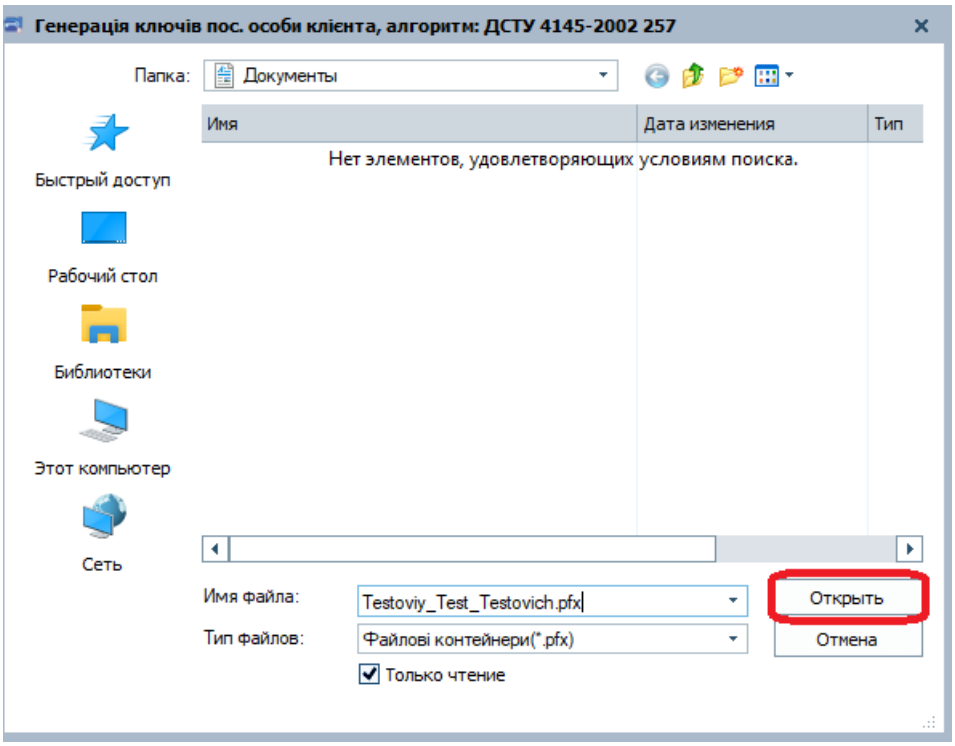

Рис. 8.

Натиснути кнопку «Прийняти».

4.2. У випадку USB-токена:

- обрати «Тип» носія – «Пасивні PKCS#11-носії»,
- ввести діючий «Пароль» до USB-токена,
- натиснути кнопку «...», і у вікні, що з’явиться, обрати ім’я USB-токена та натиснути «Вибрати» (Рис. 10.).

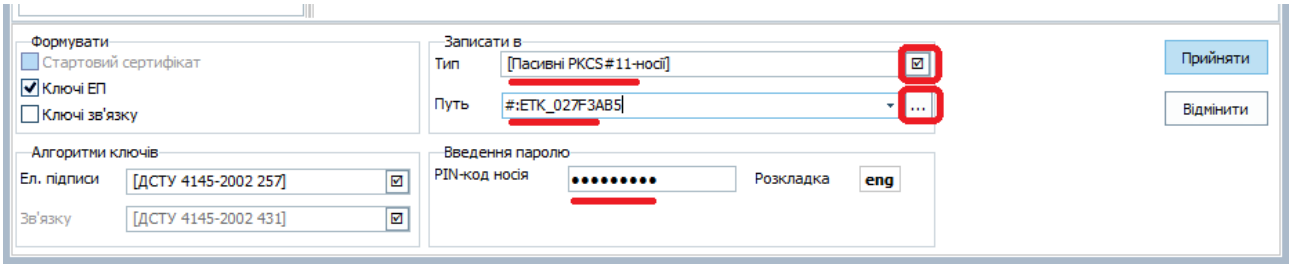

Рис. 9.

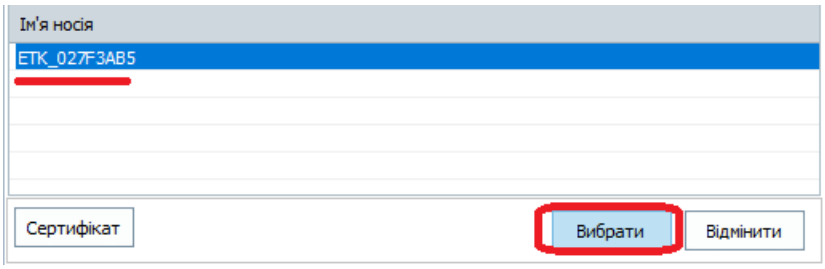

Рис. 10.

Натиснути кнопку «Прийняти».

Примітки:

1. Може з'явитись вікно, як на рис. Рис. 11. (якщо на USB-токені наявні попередні ключі), в такому разі потрібно натиснути кнопку «Прийняти».

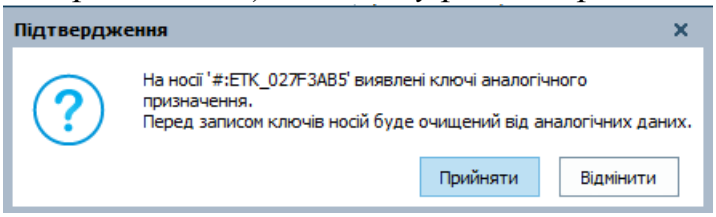

Рис. 11.

5. У вікні, що з'явиться, обрати каталог для збереження запиту на сертифікацію та натиснути кнопку «Сохранить» (Рис. 12.).

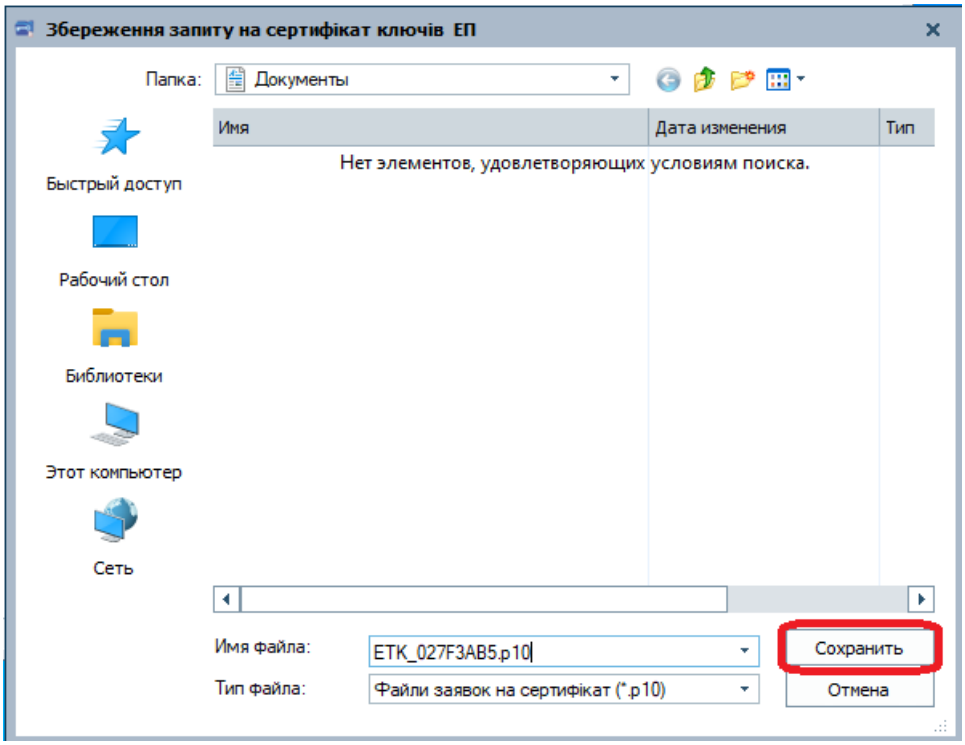

Рис. 12.

6. У вікні, що з’явиться, з результатами виконання операції, натиснути кнопку «Ok» (приклад, Рис. 13.).

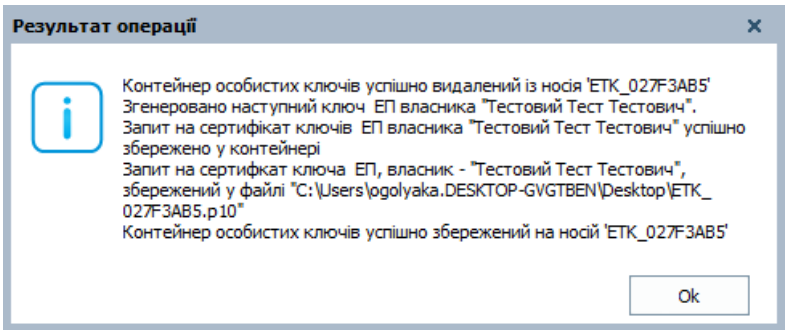

Рис. 13.

Таким чином буде згенерована пара ключів (особистий та відкритий), які збережені на носії ключової інформації, і в обраному каталозі збережено запит на сертифікацію (з відкритим ключем).

7. Відправити збережений файл запиту на сертифікацію, з розширенням *.p10 (в даному прикладі «ETK_027F3AB5.p10»), Адміністратору реєстрації НЕДП Банку. Для цього відправити на поштову адресу ca@eximb.com лист (пустий) із темою: «*Адміністратору реєстрації відправлено запит на сертифікацію ключа (Клієнт банку)*».

8. Після завершення процесу реєстрації запиту та сертифікації ключа (виконують Адміністратор реєстрації НЕДП та Адміністратор сертифікації

НЕДП), отримати лист від Адміністратору реєстрації НЕДП з сертифікатом ключа підписувача.

9. Отриманий сертифікат ключа необхідно зберегти (до ключового контейнера з особистим ключем) на власний носій ключової інформації (файл або USB-токен). Для цього в меню «Генератор ключів v1», натиснути кнопку «Отримати сертифікат» (Рис. 14.).

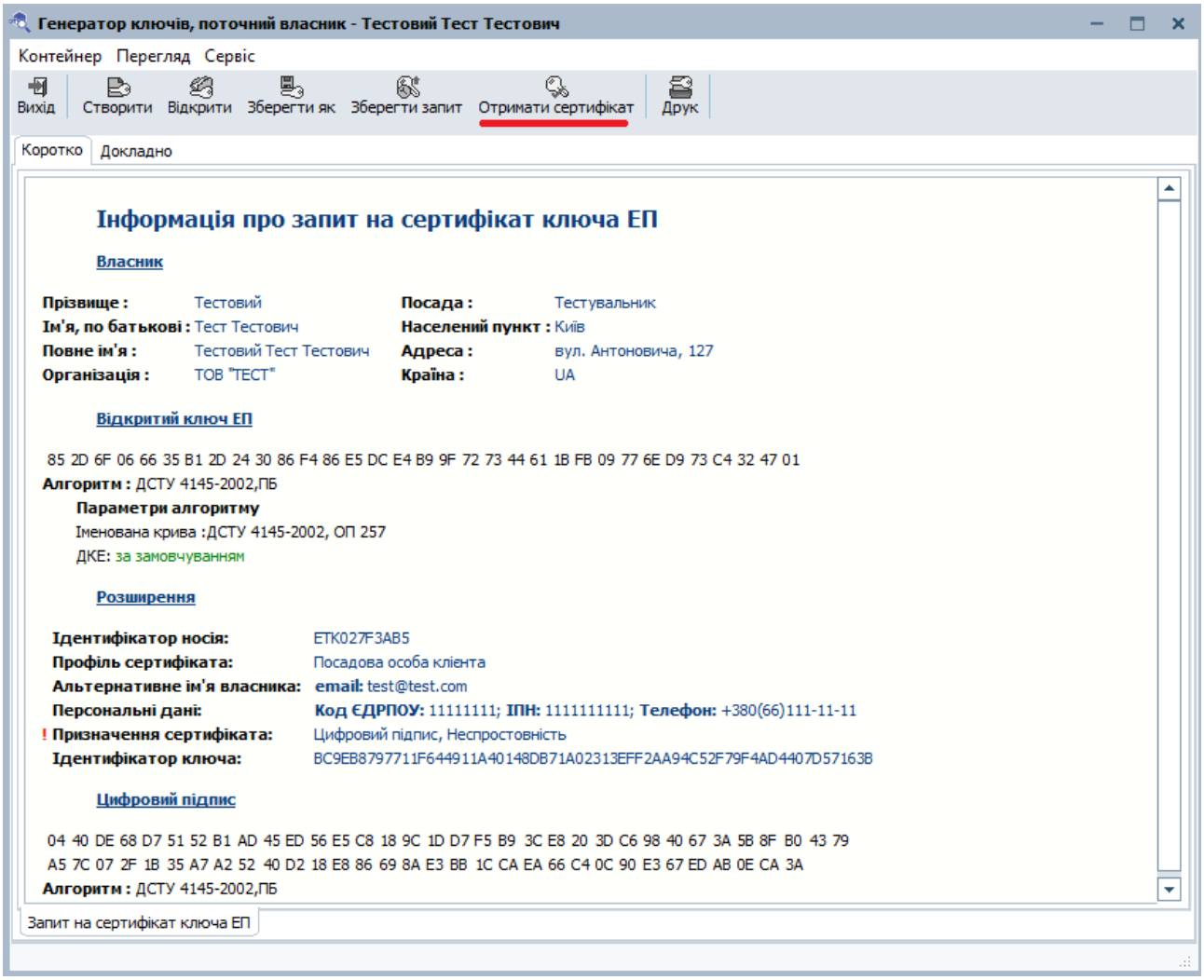

Рис. 14.

10. У вікні, що з’явиться, обрати у «тип файлов» - «Файли ланцюжків сертифікатів (p7b)», обрати файл отриманого ланцюжку сертифікатів (сертифікати підписувача та видавця) і натиснути кнопку «Открыть» (Рис. 15.).

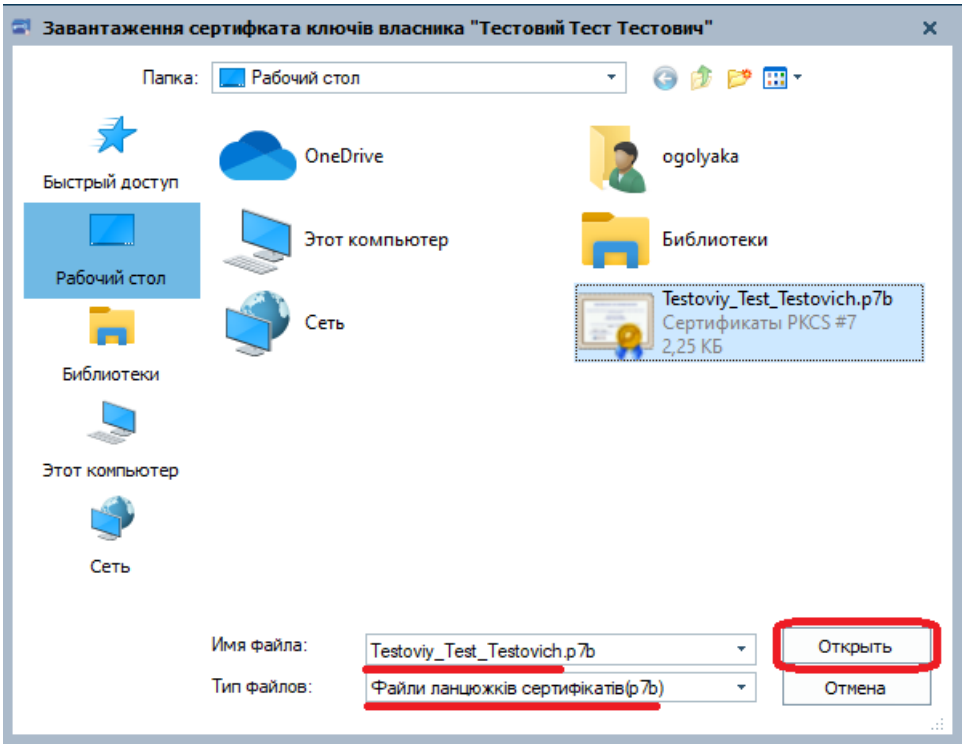

Рис. 15.

11. У вікні, що з’явиться, натиснути галочку (Рис. 16.).

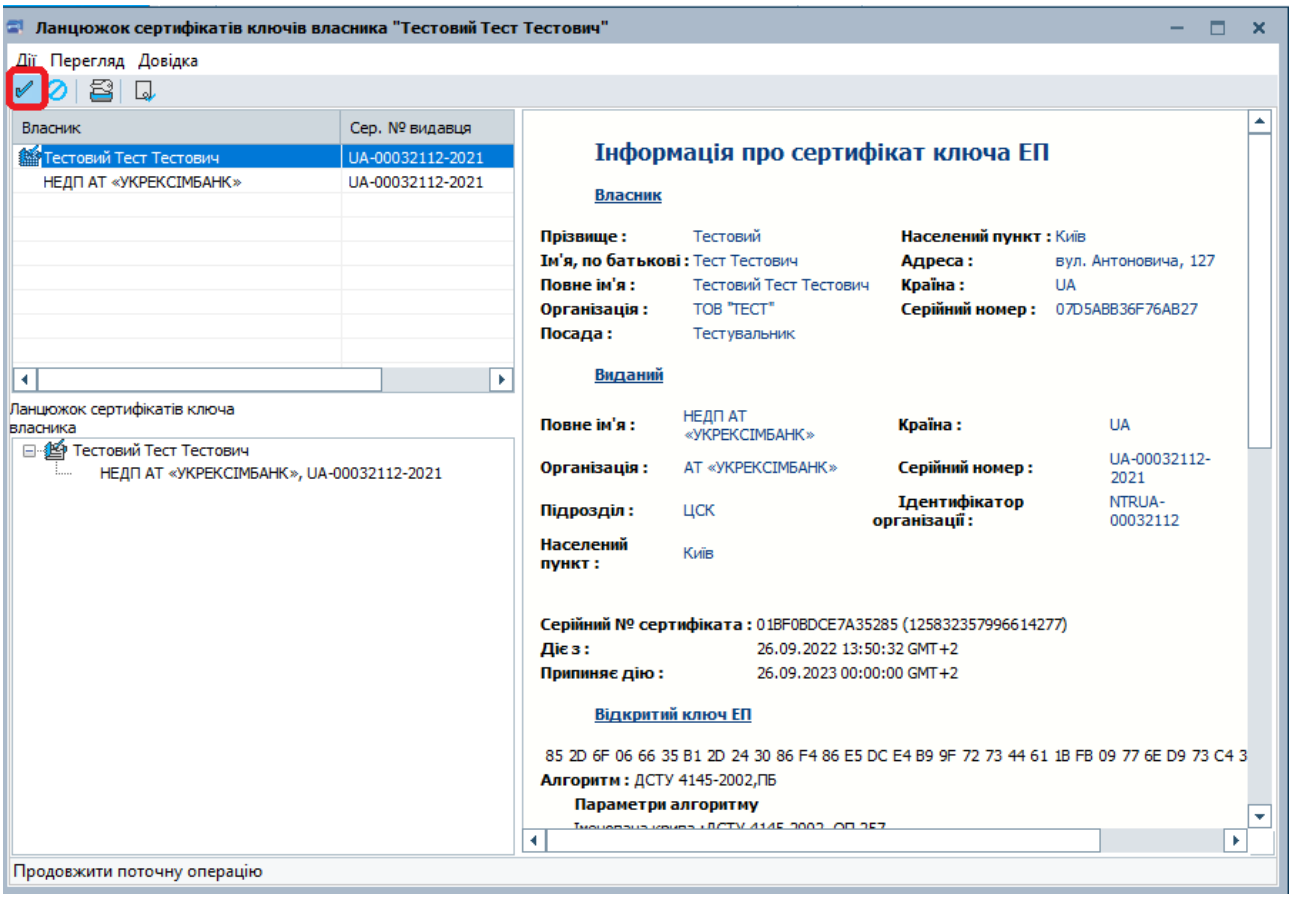

Рис. 16.

12. У вікні, що з’явиться, натиснути кнопку «Ok» (Рис. 17.).

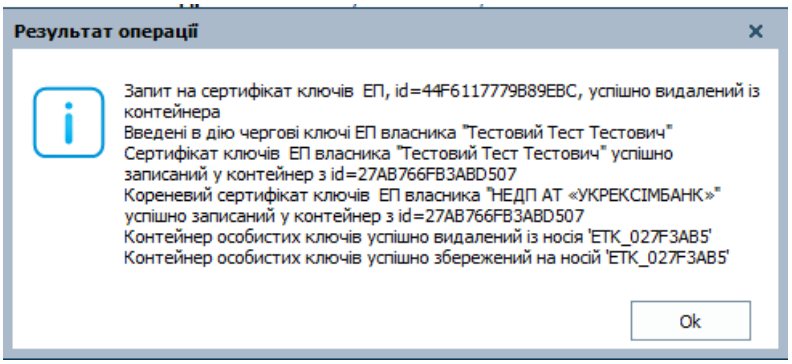

Рис. 17.

13. На цьому процедура завершена, переглянути оновлену ключову інформацію на носії можна на вкладці «Докладно» (Рис. 18.).

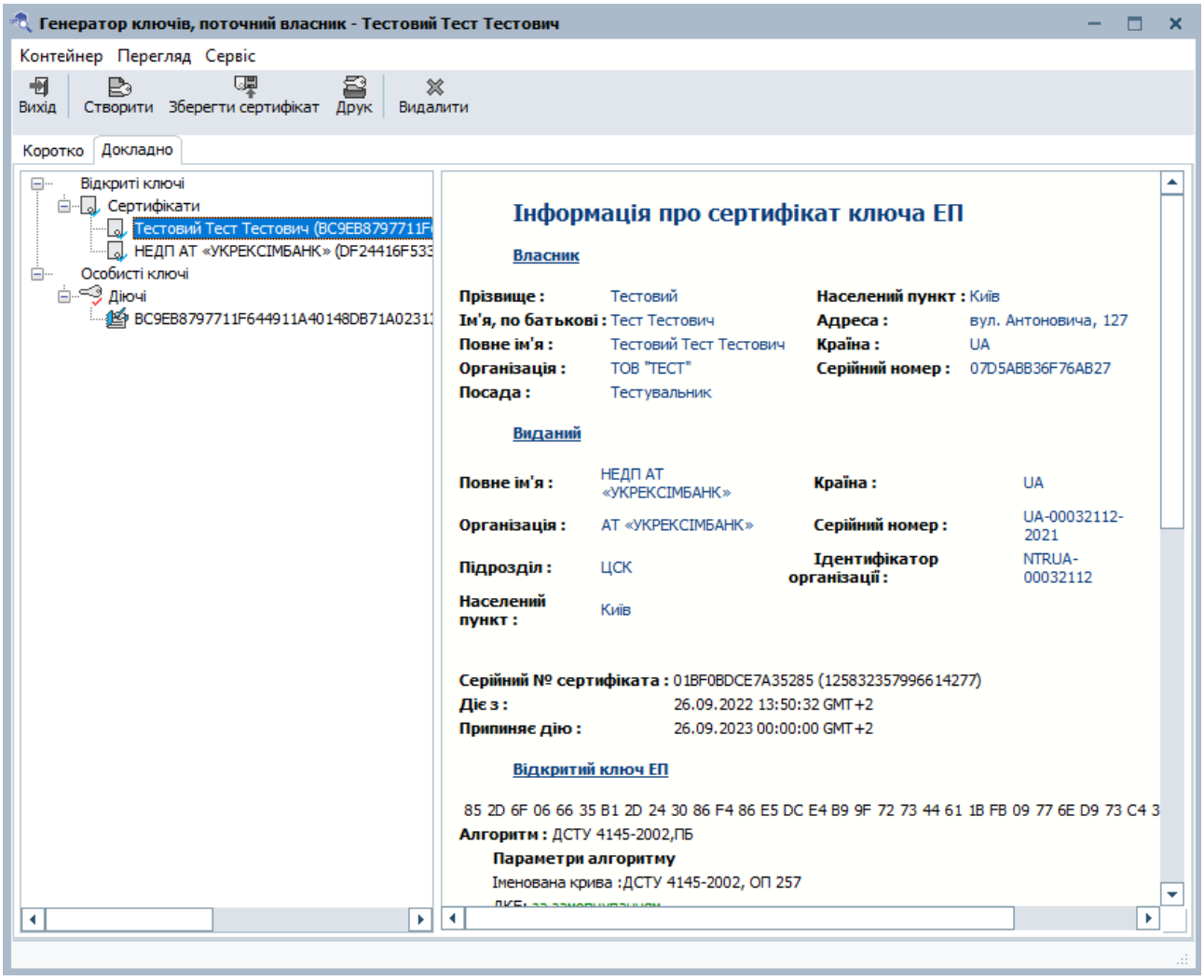

Рис. 18.

Примітки:

1. Якщо користувач закрив ПЗ «Генератор ключів v1», то для імпорту сертифіката необхідно повторно відкрити ПЗ «Генератор ключів v1» та

у вікні, що з'явиться обрати «Відкритий існуючий контейнер особистих ключів» (Рис. 19.)

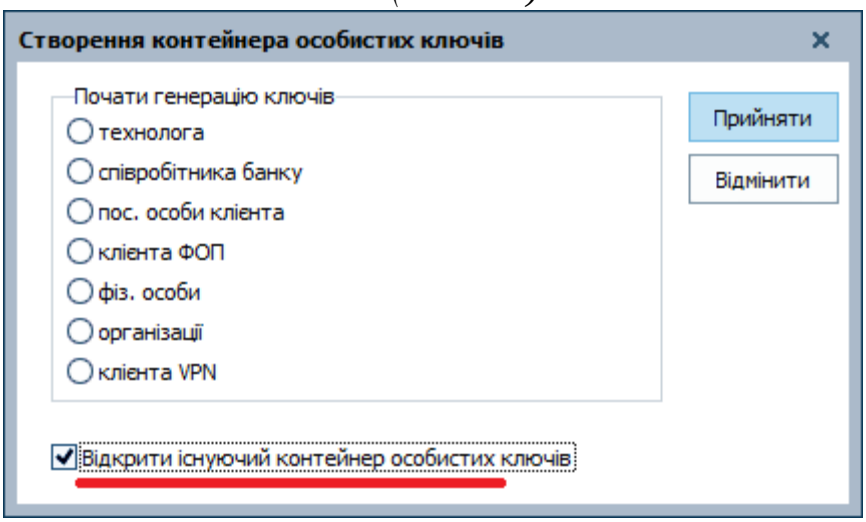

Рис. 19.

У наступному вікні користувач обирає:

- *«Тип» носія (файл або апаратний носій – токен PKCS#11),*
- *«Шлях» до носія ключа (файл на диску або USB-токен),*

вводить «Пароль» до файлу ключа або USB-токена (в залежності від носія ключової інформації),

натискає кнопку «Виконати».

Нижче Рис. 20. – приклад для файлу ключа, Рис. 21.Рис. 21. – для USB-токена (також натиснути кнопку «...», і у вікні, що з'явиться, обрати ім'я USB-токена та натиснути «Вибрати», Рис. 10.).

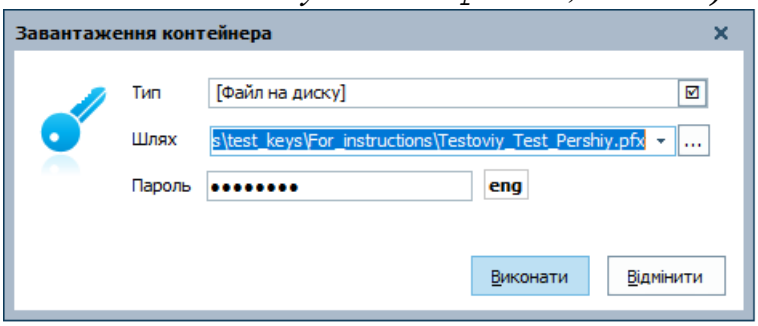

Рис. 20.

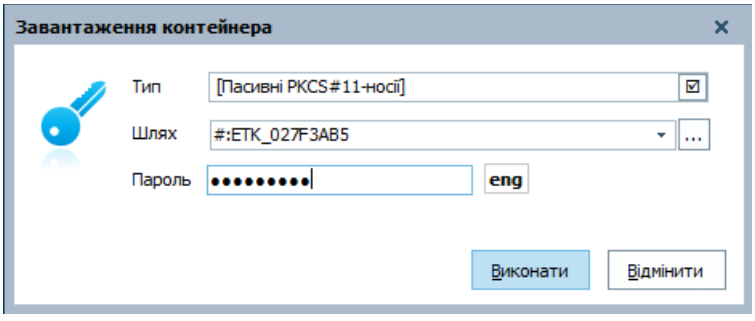

Рис. 21.