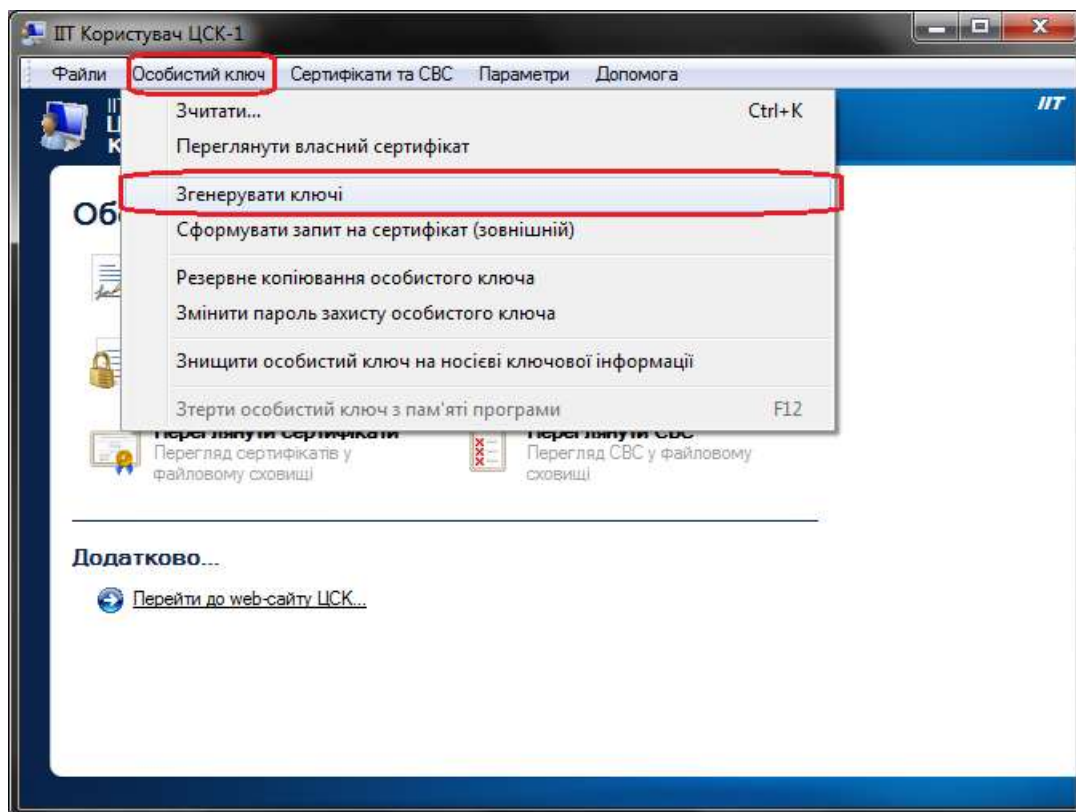


Інструкція по генерації особистого ключа користувача

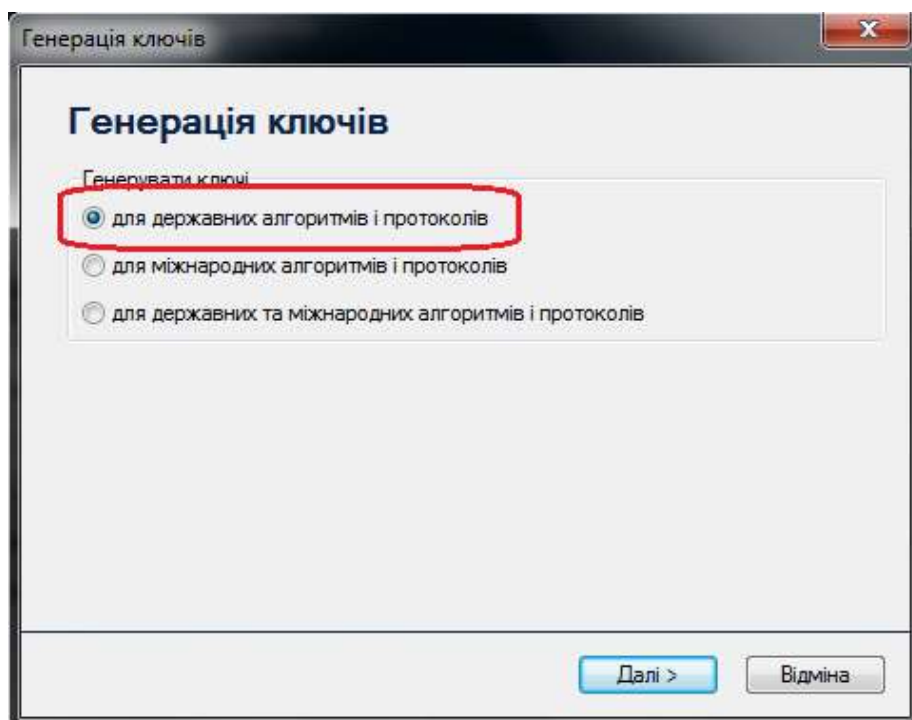
Крок 1

Запустіть програму «ІТ Користувач ЦСК» і виберіть пункт меню «Особистий ключ» / «Згенерувати ключі».



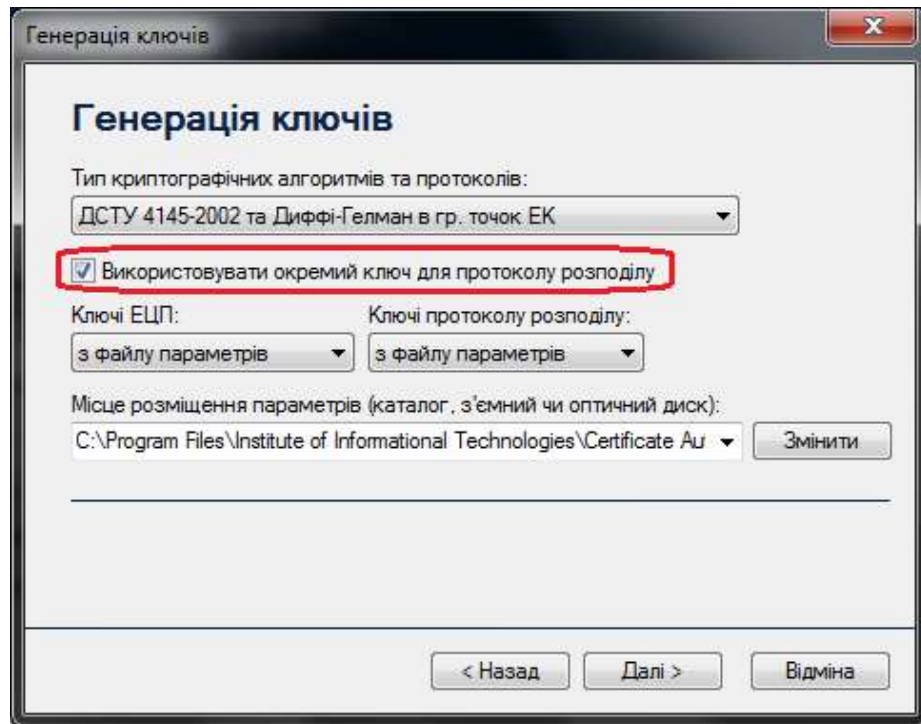
Крок 2

В цьому вікні залиште вибраним перемикач «для державних алгоритмів і протоколів» і натисніть кнопку «Далі».



Крок 3

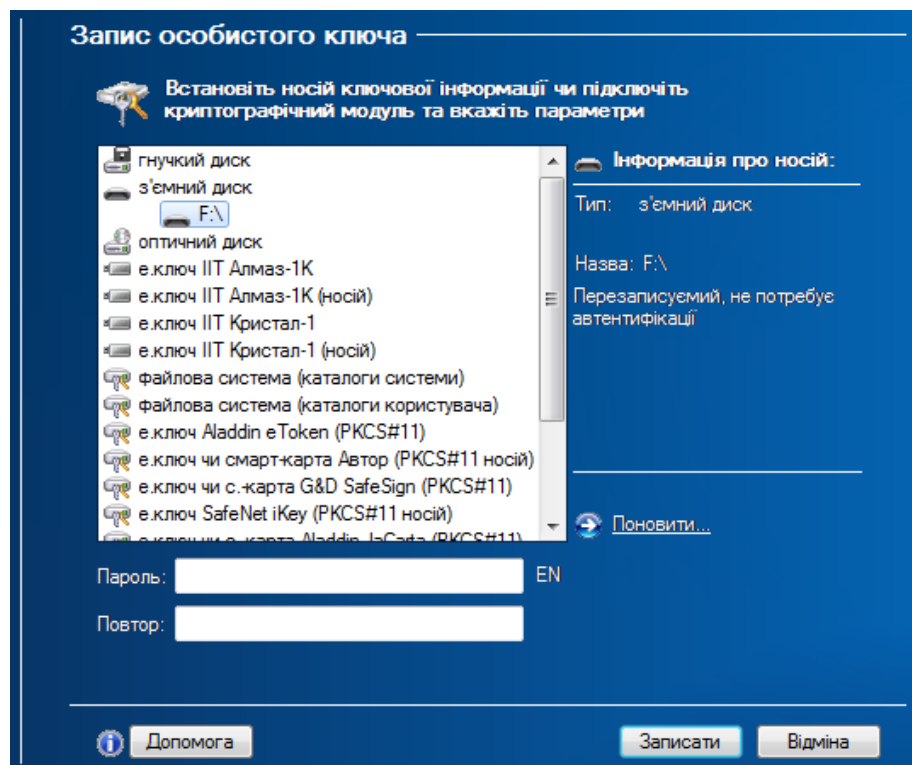
В цьому вікні обов'язково переконайтесь, що **відмічено** «Використовувати окремий ключ для протоколу розподілу» і натисніть кнопку «Далі».



Крок 4

У вікні «Запис особистого ключа»:

1. Виберіть тип носія, який буде використовуватися як носій ключової інформації (з'ємний диск, оптичний диск і т. д.). Наприклад, якщо особистий ключ планується зберігати на USB флеш-диску, то вибирається тип «з'ємний диск».
2. Виберіть назву носія (літеру). Наприклад, якщо в комп'ютер вставлено два USB флеш-диска, і вони мають літерні позначення «G:\» і «H:\», то необхідно вказати той, на який потрібно записати ключ.



3. В полі «Пароль» введіть пароль для захисту особистого ключа. Пароль повинен задовольняти наступним вимогам:

- довжина пароля повинна бути не менше ніж 8 символів;
- символи повторюватися не повинні;
- не можна використовувати поспіль більше двох символів з розкладки клавіатури (по горизонталі);
- дозволені символи: «а» - «z», «А» - «Z», «0» - «9», «+», «-».

Наприклад, пароль «**werobhfz8**» не задовольняє вищевказаним вимогам.

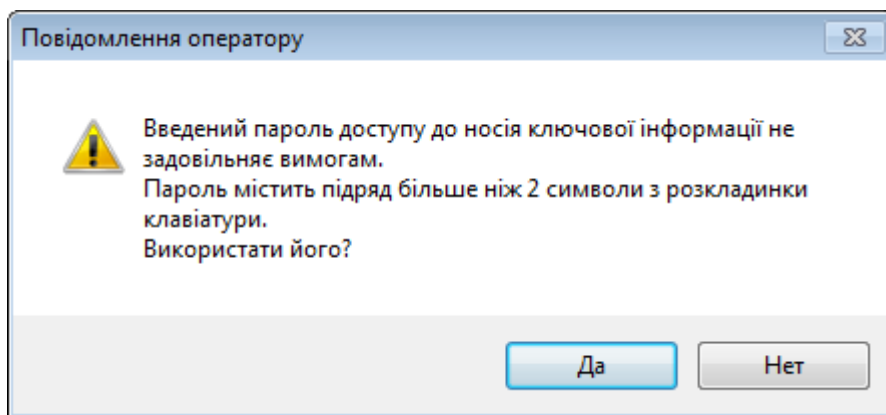
4. В полі «Повтор» повторіть введений пароль для перевірки правильності попереднього введення.

5. Натисніть кнопку «Записати». Далі буде сгенеровано особистий ключ і записано його на носій. У разі виникнення будь-яких проблем, перевірте правильність вибору типу носія, його назви, пароля захисту особистого ключа.

Крок 5

Якщо складність пароля захисту особистого ключа не задовольняє вимогам, буде виданого відповідне попередження.

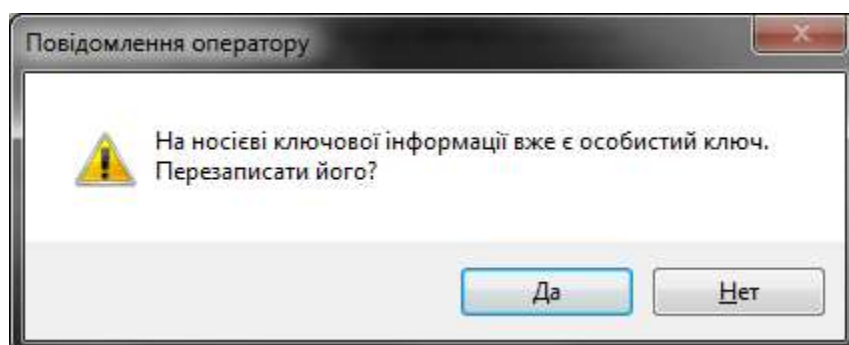
Щоб змінити пароль на складніший натисніть на кнопку «Ні», щоб використовувати введений пароль, натисніть на кнопку «Так».



Крок 6

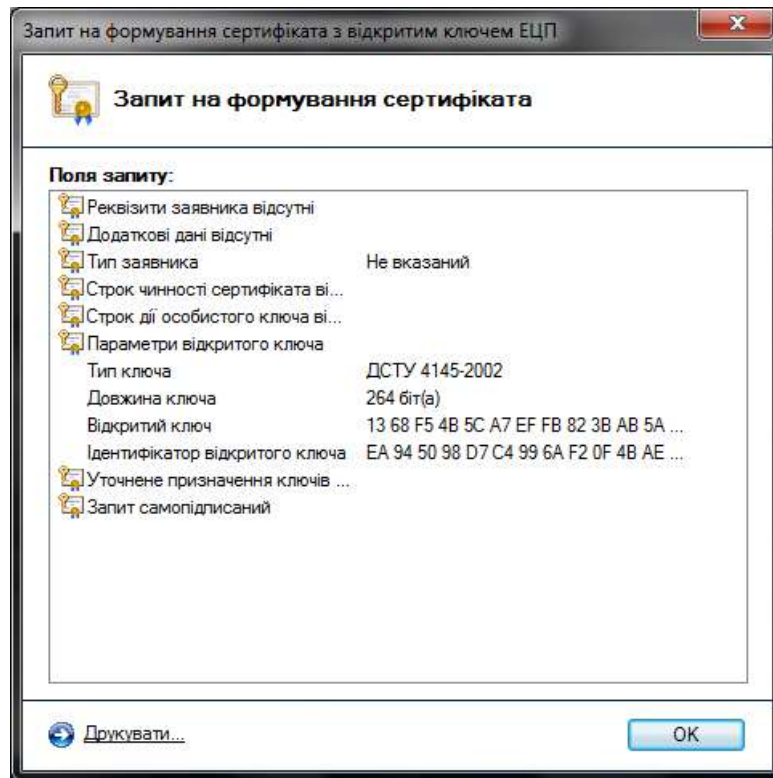
Якщо на вибраному носії вже є записаний особистий ключ (файли Key-6.dat та Key-11.dat) то буде показано вікно з попередженням.

Вставте інший носій або скопіюйте існуючі файли ключа і натисніть кнопку «Так».



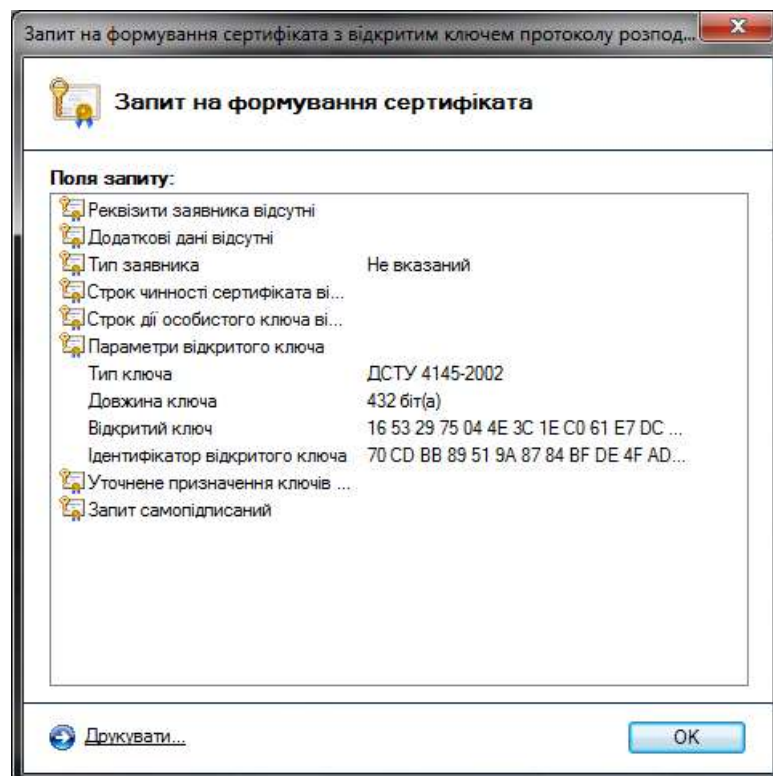
Крок 7

У вікні «Запитів на формування сертифіката з відкритим ключем ЕЦП» відображається інформацію, що міститься у файлі-запиті на сертифікат ЕЦП (електронної печатки).



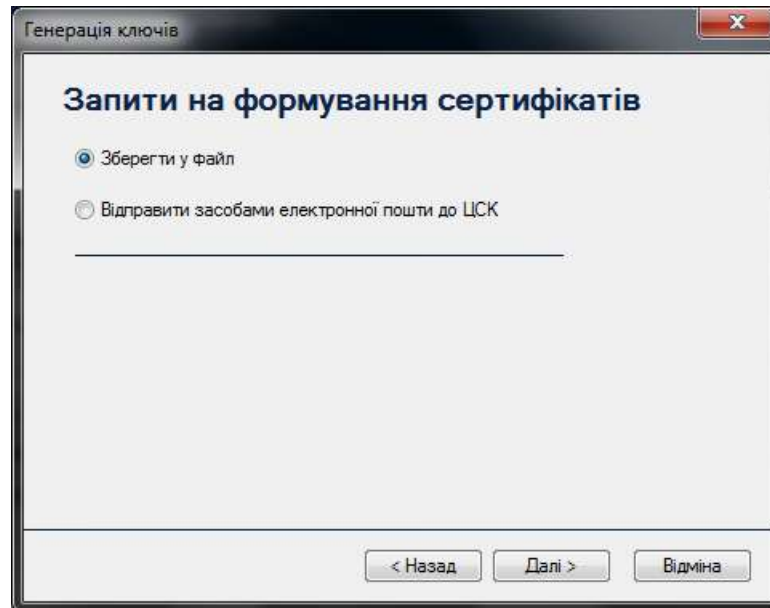
Крок 8

У вікні «Запитів на формування сертифіката з відкритим ключем протоколу розподілу» відображається інформацію, що міститься у файлі-запиті на сертифікат шифрування.



Крок 9

Виберіть опцію «Зберегти у файл» і натисніть кнопку «Далі».

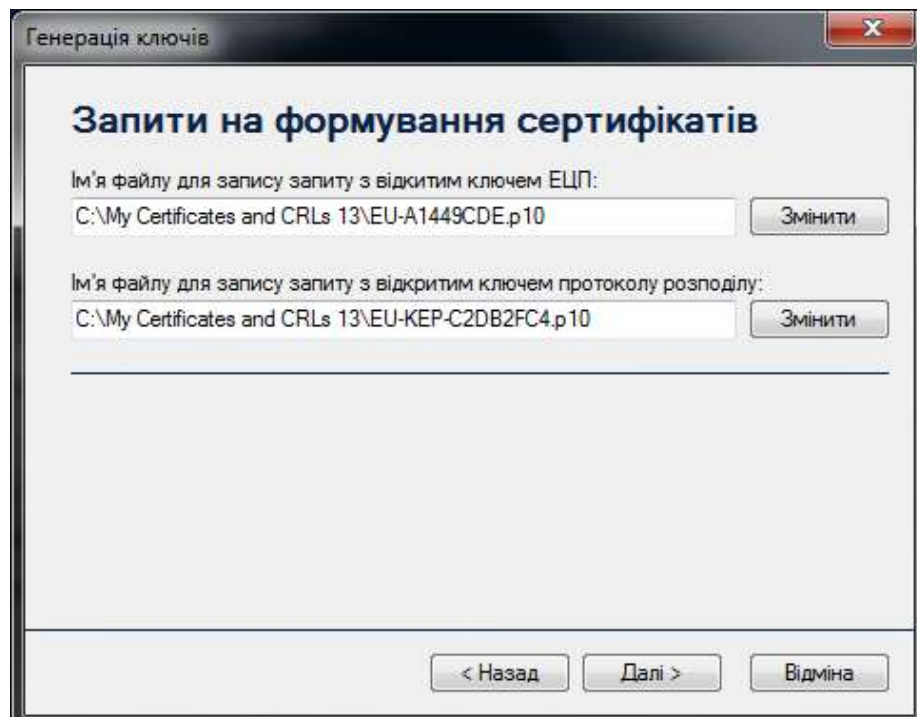


Крок 10

Далі необхідно вказати каталог для збереження і назви файлів запитів на формування сертифікатів.

Файли запитів мають розширення p10.

Щоб змінити каталог для запису файлу натисніть кнопку «Змінити».



Ім'я для файлу-запиту бажано задавати наступним чином:

- для запиту з відкритим ключем ЕЦП у форматі

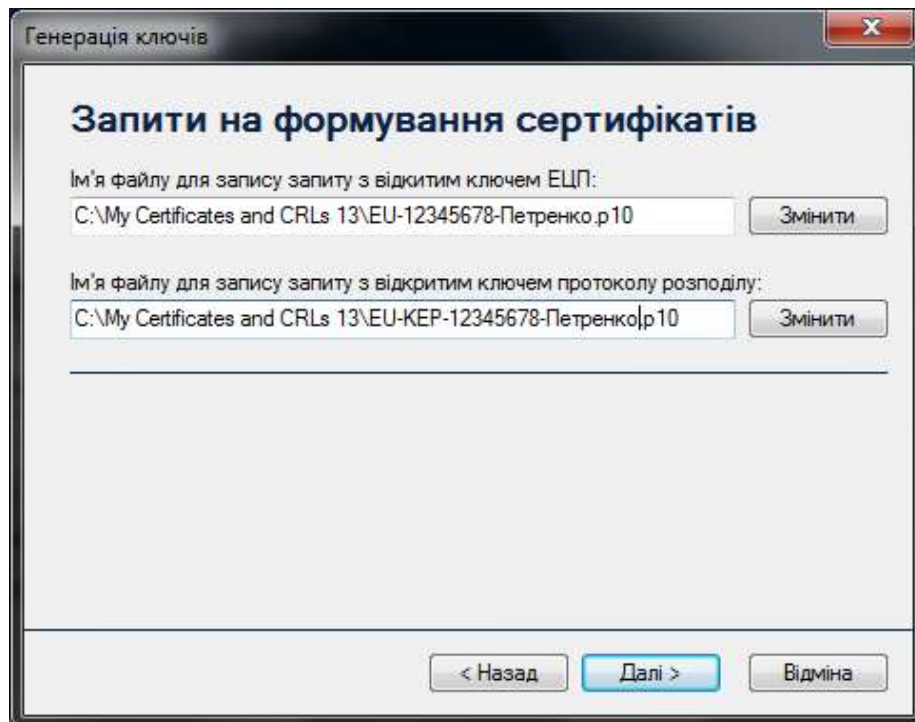
EU-ЄДРПОУ-Прізвище.p10, наприклад:

EU-12345678-Петренко.p10

- для запиту з відкритим ключем протоколу розподілу у форматі

EU-KEP-ЄДРПОУ-Прізвище.p10, наприклад:

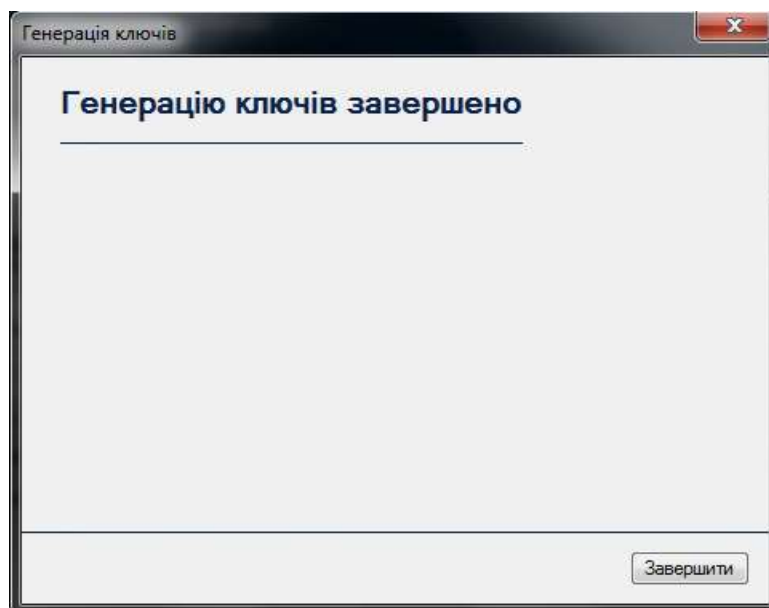
EU-KEP-12345678-Петренко.p10



Після того, як ви вказали каталог та імена файлів, натисніть кнопку «Далі».

Крок 11.

Щоб завершити процес генерації нового ключа, натисніть кнопку «Завершити».



Отримані файли-запити на формування сертифікатів збережіть на окремий з'ємний носій (USB флеш-диск, оптичний диск) для передачі до ЦСК ТОВ «КС» (в найближчий до Вас пункт реєстрації).