Державне підприємство «Національні інформаційні системи»

Акредитований центр сертифікації ключів органів юстиції України

Надійний засіб електронного цифрового підпису
«ІІТ Користувач ЦСК-1»

НАСТАНОВА ОПЕРАТОРА

Генерація особистого ключа

Київ 2016

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ЕЦП	-	Електронний цифровий підпис;
АЦСК	-	Акредитований центр сертифікації ключів органів юстиції України;

1. Генерація особистого ключа

Для генерації особистого ключа необхідно обрати підпункт «Згенерувати ключі» в пункті меню «Особистий ключ» (рис 1.1 – 1.2).

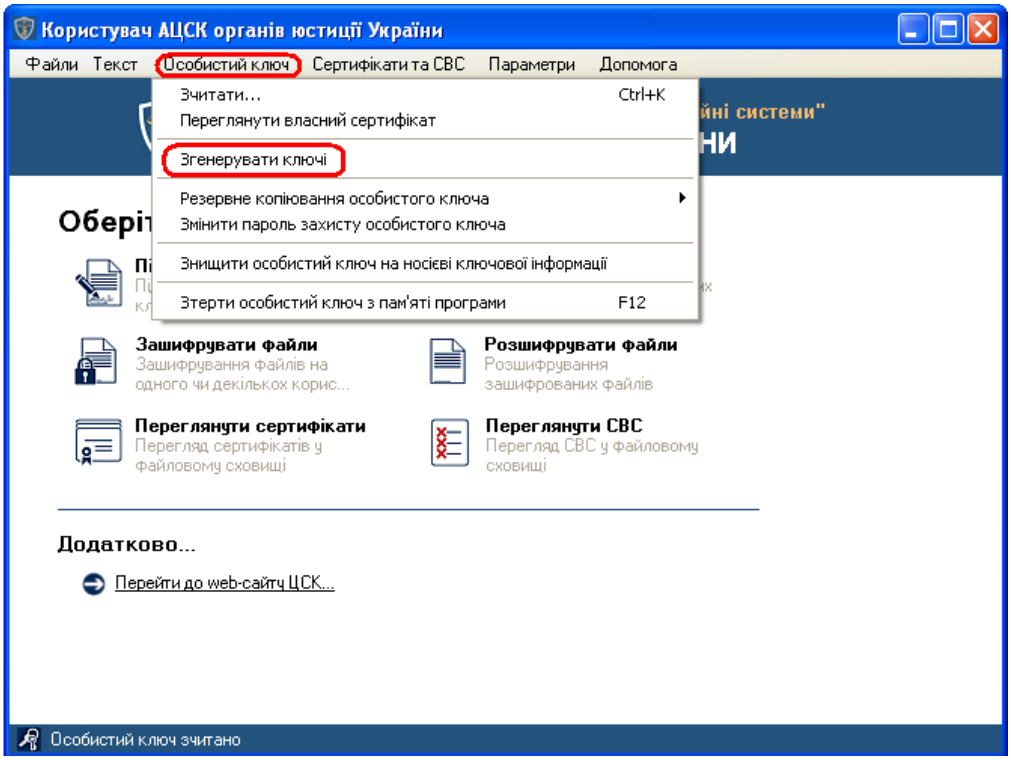

Рисунок 1.1

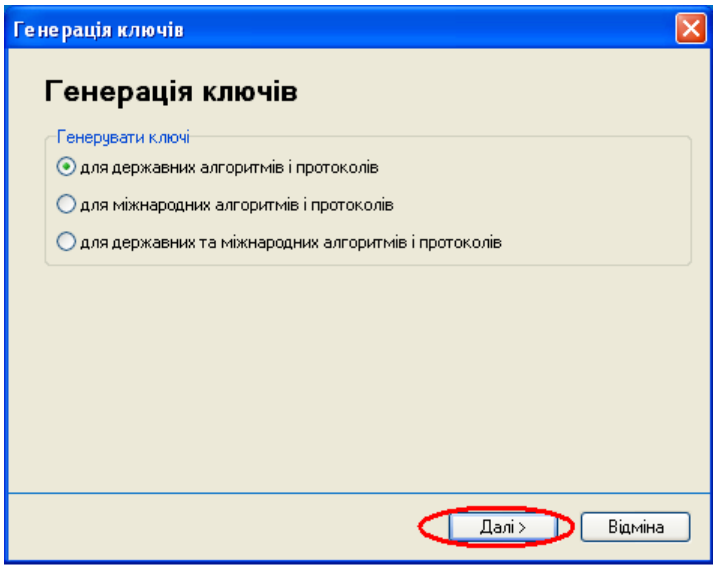

Рисунок 1.2

У вікні генерації ключів необхідно встановити параметр «Використовувати окремий ключ для протоколу розподілу», при цьому буде згенеровано дві ключові пари, одна з яких буде використовуватись для підписання даних, а друга (ключ протоколу розподілу) буде використовуватись для шифрування даних.

Для продовження генерації ключа необхідно натиснути кнопку «Далі» (рис 1.3).

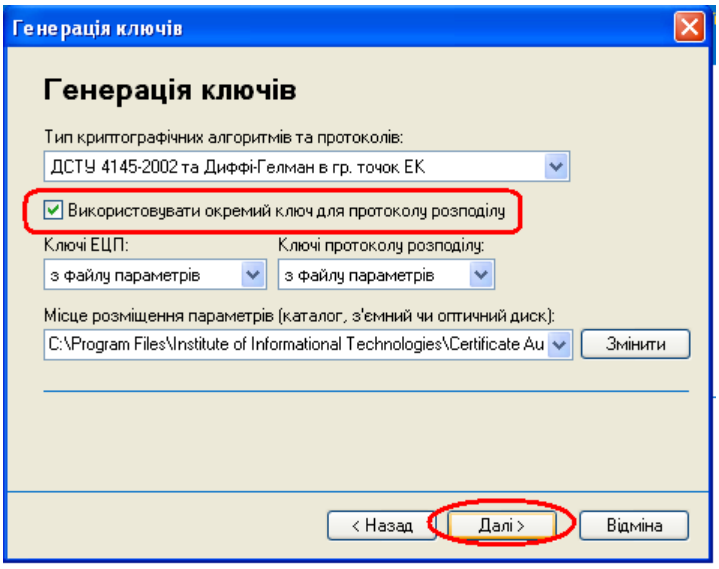

Рисунок 1.3

Після появи вікна запису особистого ключа, необхідно обрати з'ємний носій, на який буде записано особистий ключ, ввести пароль захисту до нього та натиснути кнопку «Записати» (рис.1.4).

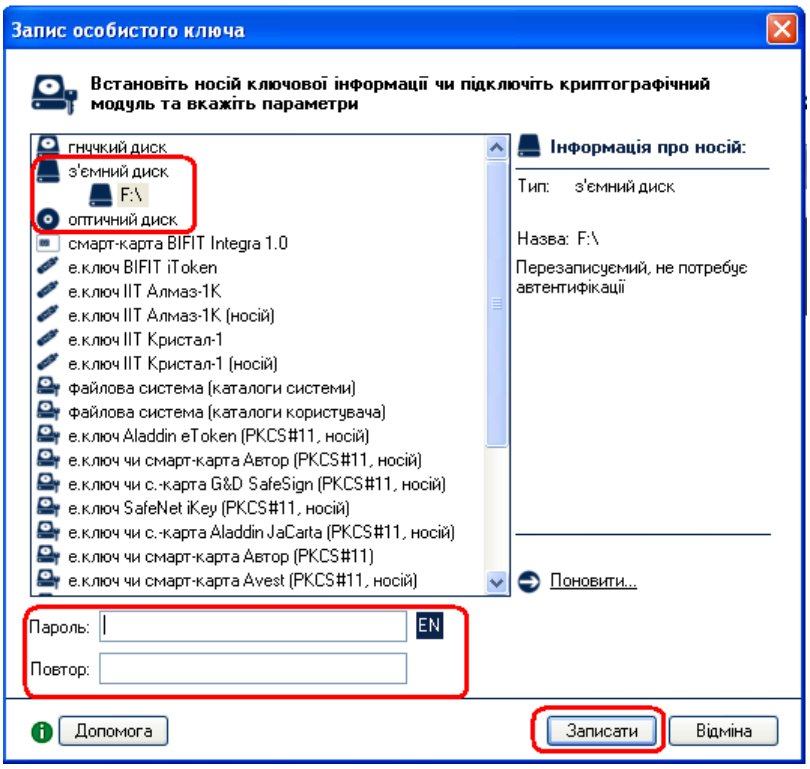

Рисунок 1.4

Обидва особистих ключа (для підпису та шифрування) будуть записані у вигляді одного файлу особистого ключа – Key-6.dat.

Після запису особистого ключа на з'ємний носій буде виведено вміст запиту на формування сертифіката з відкритим ключем ЕЦП та запиту на формування сертифіката з відкритим ключем протоколу розподілу. Для продовження генерації натискаємо кнопку «ОК» (рис. 1.5, 1.6).

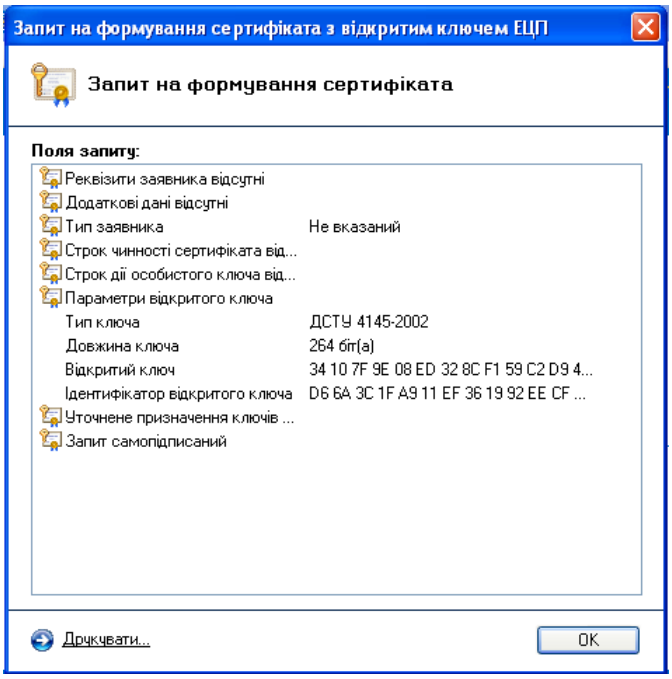

Рисунок 1.5

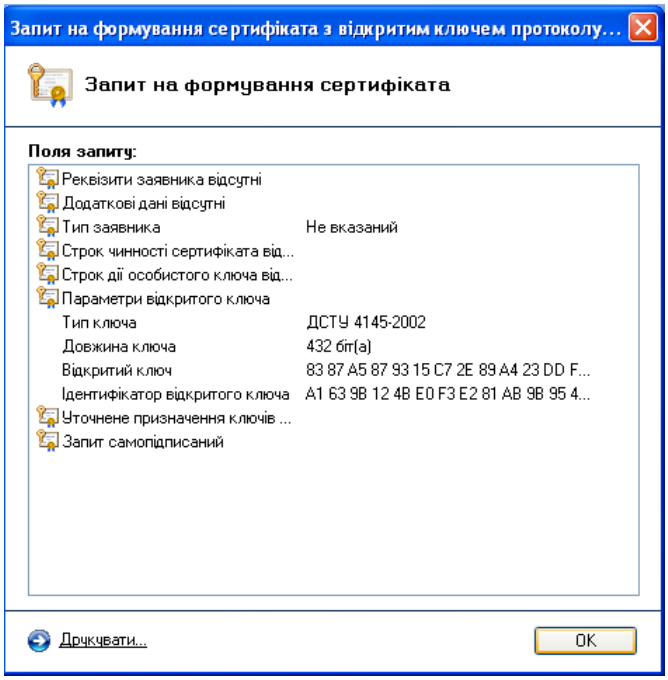

Рисунок 1.6

Для передачі запитів на формування посилених сертифікатів до АЦСК необхідно зберегти їх у файл (рис. 1.7). Для цього встановити параметр «Зберегти у файл» та натиснути кнопку «Далі».

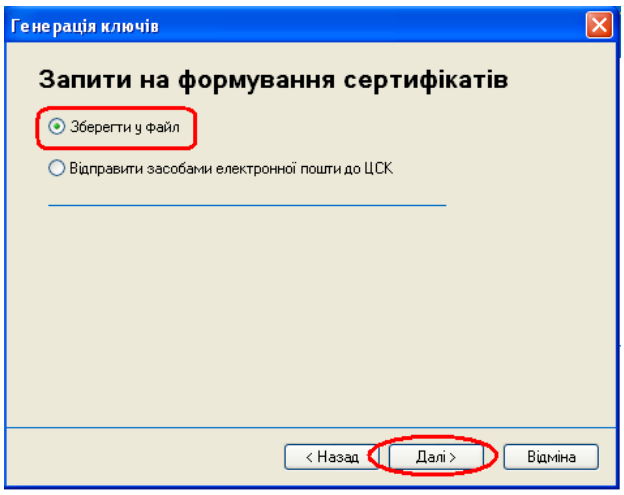

Рисунок 1.7

Запити повинні бути записані на носій інформації чи на жорсткий диск. Для цього необхідно натиснути кнопку «Змінити» (рис. 1.8) та вказати необхідний носій інформації та ім’я запитів на формування сертифікатів у файл.

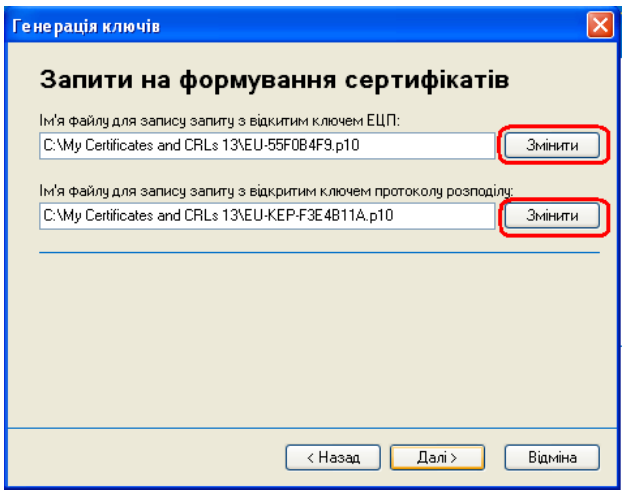

Рисунок 1.8

Увага! Для коректної ідентифікації запитів з відкритим ключем ЕЦП та протоколом розподілу користувача файл запиту на формування сертифіката повинен обов’язково зберігатись з ім’ям у наступному форматі:

«EU-XXXXXXXX-Прізвище.p10» та

«EU-KEP-XXXXXXXX-Прізвище.p10»,

де: Прізвище – прізвище підписувача;

EU-XXXXXXXX.p10 та EU-KEP-XXXXXXXX.p10 – унікальне ім’я файлу запиту, що формується програмним забезпеченням за замовчуванням та повинно залишатись без змін.

Наприклад:

EU-69PH0S9W-Іванов.p10; EU-KEP-KB50S67Z-Іванов.p10.

Для завершення генерації необхідно натиснути кнопку «Завершити» (рис. 1.9).

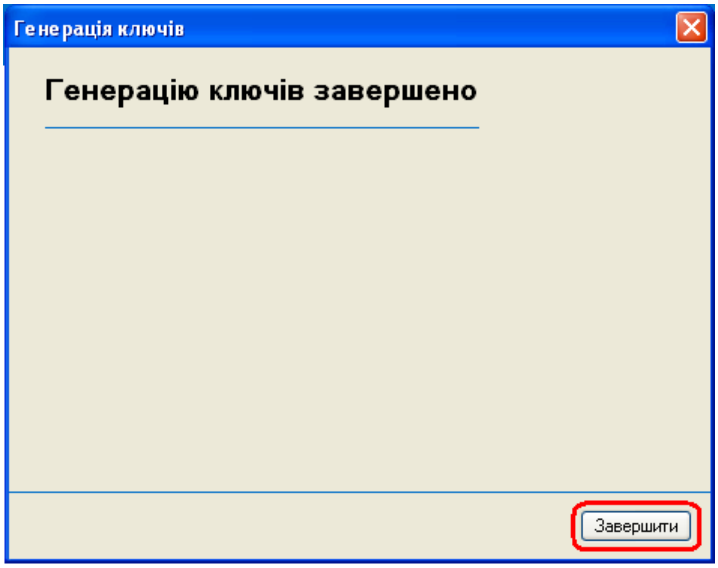

Рисунок 1.9

Після цього, запити разом з комплектом реєстраційних документів можуть бути передані до пункту реєстрації користувачів АЦСК для формування посилених сертифікатів.