**Інструкція з завантаження сертифікатів з вебсайту КНЕДП ДПС та отримання даних для заповнення графи 3 «Ідентифікатор ключа суб’єкта» Повідомлення про надання інформації щодо кваліфікованого сертифіката відкритого ключа (для повідомлень щодо сертифікатів відкритих ключів, які застосовуються в ПРРО)**

1. **Інструкція з завантаження сертифікатів з вебсайту КНЕДП ДПС**

**1.1.** На прикладі КНЕДП ДПС продемонстровано яким чином можливо завантажити два власні сертифікати (сертифікати публікуються на вебсайті КНЕДП ДПС за умови згоди клієнта), які відповідають особистому ключу (наприклад key6.dat):

* ЕЦП, Неспростовність **(містить «Ідентифікатор ключа суб’єкта»);**
* Протоколи розподілу ключів.

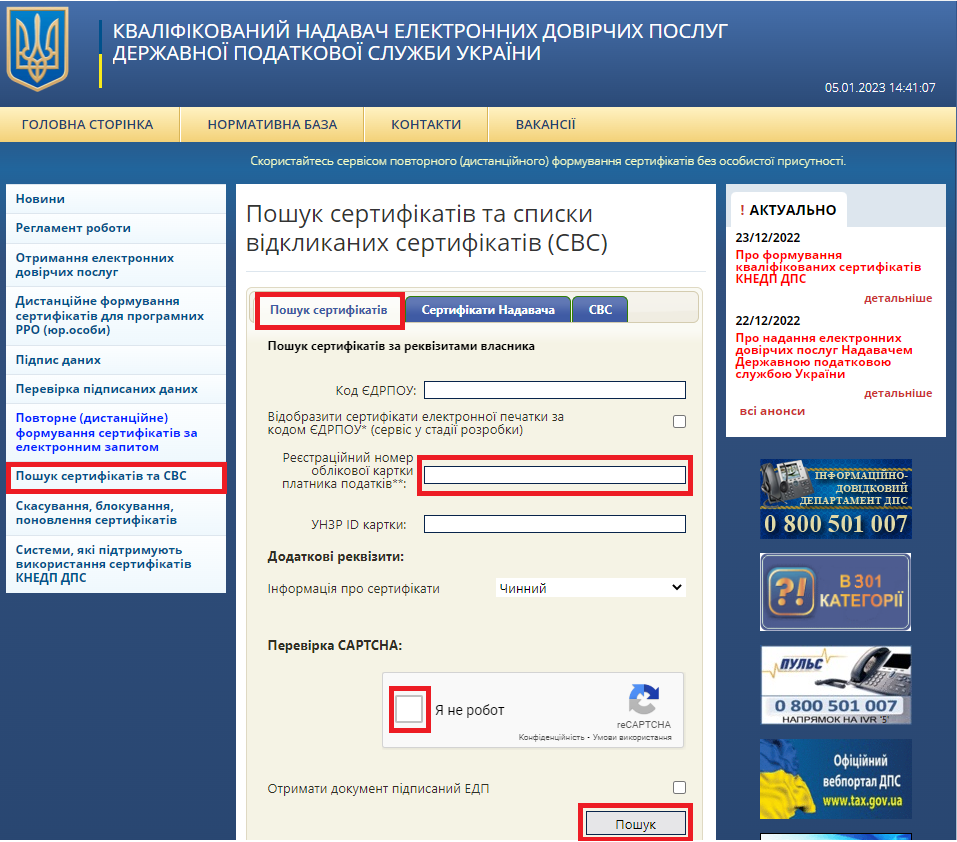
**1.2.** Для цього потрібно зайти на вебсайт https://ca.tax.gov.ua (рис. 1)



*Рис. 1*

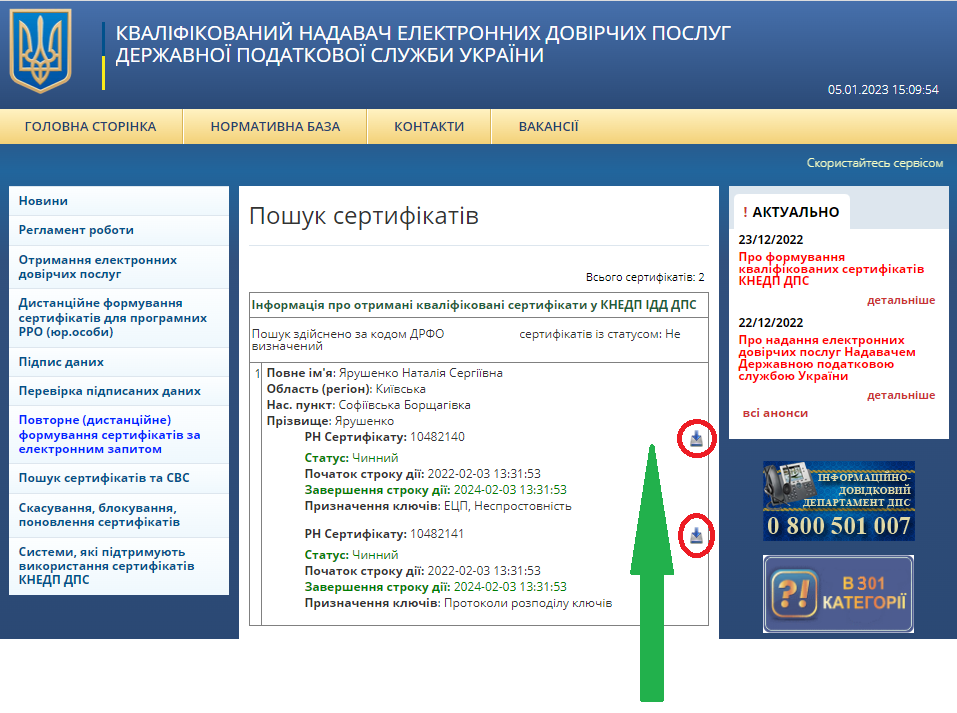
* 1. Для пошуку власних сертифікатів потрібно перейти до розділу   
     [«Пошук сертифікатів та СВС»](http://acskidd.gov.ua/certificates-search), вкладка «Пошук сертифікатів» використовуючи поле «Реєстраційний номер облікової картки платника податків»\*, поставити галочку в полі «Я не робот» та натиснути кнопку «Пошук» (рис. 1.1).

\* У разі відмови від реєстраційного номеру облікової картки платника податків пошук здійснюється за серією та номером паспорта (для паспорта громадянина України у формі книжечки) або за номером (для паспорта громадянина України у вигляді ID –картки).



*Рис. 1.1*

**1.4**. Якщо ви знайшли кваліфікований сертифікат відповідного підписувача – завантажте його на свій комп’ютер натиснувши кнопки – D:\РОБОТА\Роботи картинки\photoshop\Arrow\b_sm_export.png (рис. 1.2).

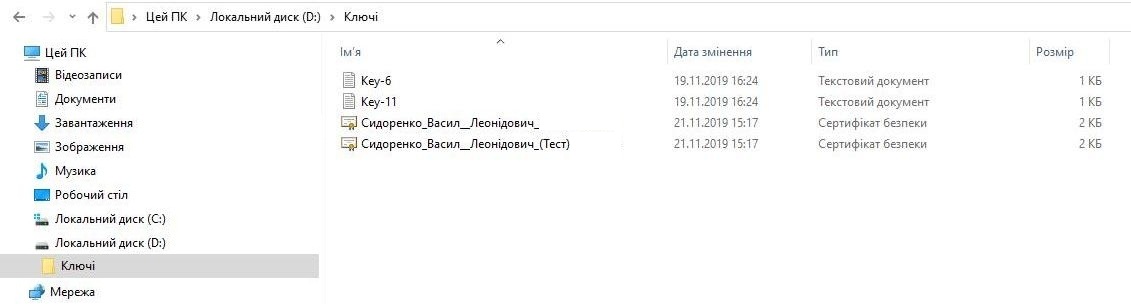


**Cертифікат, який містить «Ідентифікатор ключа суб’єкта»**

*Рис. 1.2*

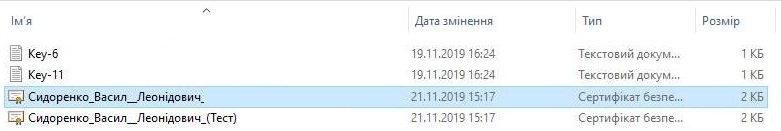
1. **Отримання даних для заповнення графи 3 «Ідентифікатор ключа суб’єкта» Повідомлення про надання інформації щодо кваліфікованого сертифіката відкритого ключа (для повідомлень щодо сертифікатів відкритих ключів, які застосовуються в ПРРО)**

**2.1.** Обираємо носїй інформації та переходимо за місцем розташування файлів типу «Сертифікат безпеки» із розширенням \*.cer. (рис. 2)



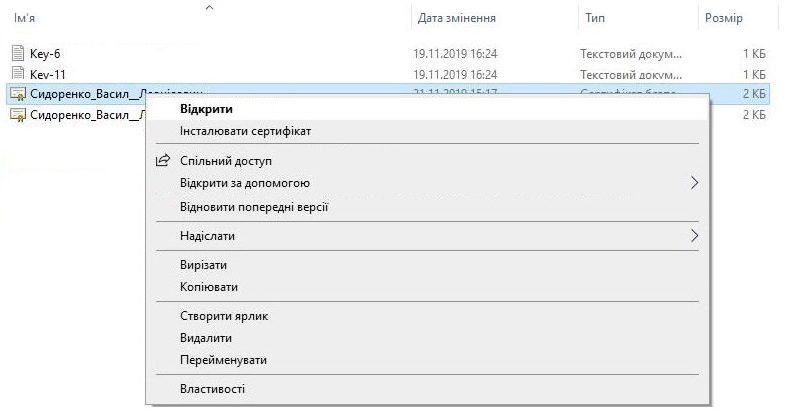
*Вибір місця розташування сертитфікату (рис. 2)*

**2.2.** Виділяємо обраний файл сертифіката (рис. 2.1).



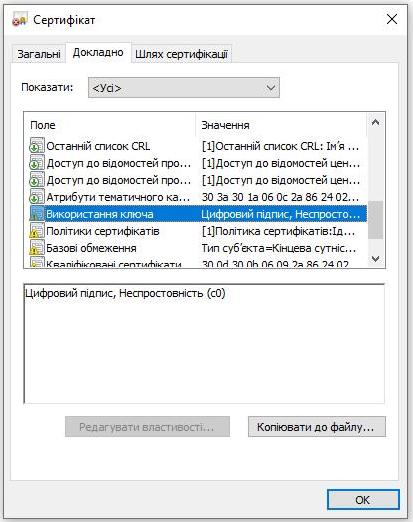
*Вибір сертифіката (рис 2.1)*

**2.3.** Правою клавішею «мишки» переходимо до вибору команди «Відкрити» та підтверджуємо дію (рис. 2.2).

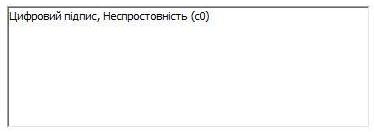


*Відкриття файлу сертифіката (рис.2.2)*

**2.4.** У відкритому файлі сертифіката переходимо у вкладку «Докладно» та знаходимо поле з назвою «Використання ключа» (рис. 2.3) значення якого відповідає «Цифровий підпис, Неспростовність» (рис. 2.4). Якщо значення поля не відповідає зазначеним даним необхідно обрати інший сертифікат.

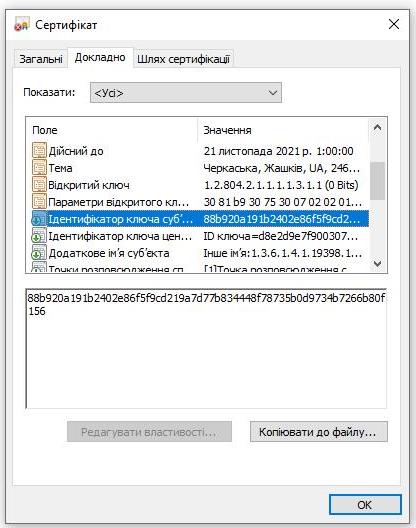
****

*Вибір поля «Використання ключа» (Рис. 2.3)*

**

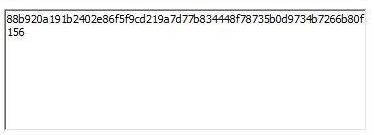
*Значення поля «Використання ключа» (Рис. 2.4)*

**2.5.** У разі відповідності у відкритому файлі сертифіката значення поля «Використання ключа», знаходимо та виділяємо рядок з назвою «Ідентифікатор ключа суб’єкта» (рис. 2.5).



*Вибір поля «Ідентифікатор ключа суб’єкта» (рис. 2.5)*

**2.6.** При виборі поля «Ідентифікатор ключа суб’єкта» у нижчому віконці відображається набір букв та цифр (рис. 2.6), який і потрібно вказати у даних графи 3 «Ідентифікатор ключа суб’єкта» при заповненні Повідомлення про надання інформації щодо кваліфікованого сертифіката відкритого ключа (для повідомлень щодо сертифікатів відкритих ключів, які застосовуються в ПРРО) за формою J/F1391801. У разі відображення ключа у вигляді парних наборів символів (як приклад: 88 b9 20 a1 91 b2 40 2e 86 f5 f9 cd 21 9a 7d 77 b8 34 44 8f 78 73 5b 0d 97 34 b7 26 6b 80 f1 56) необхідно при заповненні графи 3 «Ідентифікатор ключа суб’єкта» прибрати пробіли.



*Значення поля «Ідентифікатор ключа суб’єкта» (рис. 2.6)*