Інструкція встановлення, налаштування та генерації ключів Електронного Цифрового Підпису в Клієнт Банк “Style”

Менеджер відділення надасть підтримку з питань:

- тарифів, послуг, укладання договорів, таке інше;
- **порядку підключення** до послуги Клієнт-Банк та додаткових сервісів;
- **функціональних можливостей** комплексу Клієнт-Банк та його використання при створенні платіжних доручень та заявок;
- **актуального стану** виконання платіжних доручень та заявок;
- **порядку сертифікації** ключів уповноважених представників та їх статусу після генерації.

Ім’я Менеджера

_____

Стаціонарний телефон

_____

Мобільний телефон

_____

УВАГА! Номер телефону відділення можна знайти за наступним посиланням: www.credit-agricole.ua/branches/otdelenija-i-bankomaty/

Служба технічної підтримки надасть допомогу при:

- **технічних помилках** системи;
- **інсталяції системи** Клієнт-Банк на комп’ютер;
- **генерації ключів** уповноважених представників.

Стаціонарний телефон

0-800-30-30-28

ВСТАНОВЛЕННЯ СИСТЕМИ STYLE ТА ПІДГОТОВКА ДО ЇЇ ПЕРШОГО ЗАПУСКУ

Для успішного встановлення та функціонування системи клієнт-банк “Style”, необхідно виконати наступні дії:

1. Створити папку, наприклад **Agricole_CB** на диску **C:**, або в будь-якому місці, або на флеш-носіїї (Flashdrive). У випадку використання декількох клієнт-банків Style для різних організацій на одному комп’ютері необхідно створити папки з іменами **Agricole_CB1, Agricole_CB2,** і т.п. Для кожної організації повинна бути створена **своя** папка.
2. Отриманий в Банку заархівований файл, що містить ПЗ клієнт-банк “Style”, необхідно скопіювати в створену папку, та розархівувати його.
3. Створити ярлик для файла **Upp_4.exe** (**Agricole_CB – Client - BIN Upp_4.exe)** для запуску клієнт-банку та помістити його на робочий стіл комп’ютера. У випадку використання лише одного клієнт-банку на комп’ютері, назву ярлика можна залишити без змін. У випадку використання декількох клієнт-банків для різних організацій на одному комп’ютері ярлик повинен бути створений, перейменований та поміщений на робочий стіл **для кожної організації окремо**.

Якщо при виконанні дій, що наведені вище, у Вас виникли питання, зверніться до свого системного адміністратора.

1. ПЕРШИЙ ЗАПУСК СИСТЕМИ

Запустити клієнт-банк шляхом подвійного натискання на ярлик для файла **Upp_4.exe**. При першому, після встановлення, запуску слід вибрати мову інтерфейсу. Після вибору бажаної мови з’явиться вікно входу в систему (Рис. 1).

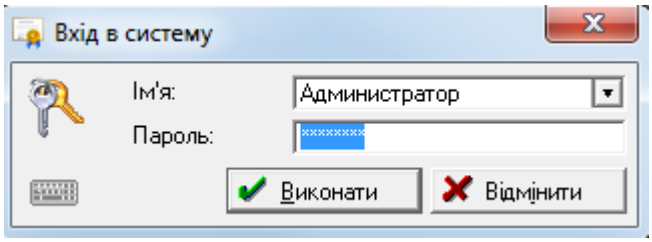

Рисунок 1 - Вхід в систему клієнт-банк

Для входу необхідно використовувати такі дані:
Ім’я: Администратор **Пароль: 11111111**

Далі необхідно налаштувати анкету. Для цього необхідно увійти в меню **Сервіс – Настроювання ini-Файлу,** вкладка **Реєстрація**. Заповнюються дані наступним чином:
Count Banks – не заповнюється;
Bank Name – найменування обслуговуючого банку (ПАТ “КРЕДІ АГРІКОЛЬ БАНК”);
Bank Mfo – МФО обслуговуючого банку (300614);
Kart OKPO – ЄДРПОУ організації клієнта;
Kart Name – найменування організації клієнта; для юридичних осіб зазначається скорочена назва відповідно до установчого документу; для фізичних осіб – підприємців - абревіатура ФОП та ПІБ повністю (наприклад, «ФОП Іванова Катерина Михайлівна»).
IDENT – DOCPOST клієнта (дана інформація надається у відділенні банку);
SERIAL – серійний номер (дана інформація надається у відділенні банку);
PROGNOSIS – On;

OWN_NAME – найменування організації клієнта (тільки для системи SWIFT);
OWN_ADDRESS – юридична адреса організації клієнта (тільки для системи SWIFT);
BANK_NAME – найменування обслуговуючого банку (ПАТ “КРЕДІ АГРІКОЛЬ БАНК”) (тільки для системи SWIFT);
BANK_ADRESS – юридична адреса обслуговуючого банку (Україна, м. Київ, вул. Пушкінська, 42/4) (тільки для системи SWIFT);
Pay Systems – залишається без змін (SWIFT|БИК);

ЗВЕРНІТЬ УВАГУ: Поля, що містять інформацію щодо клієнта (Kart OKPO, Kart Name, IDENT, SERIAL) мають бути заповнені **обов’язково**.

Приклад заповнення анкети клієнта наведено на рисунку 2.

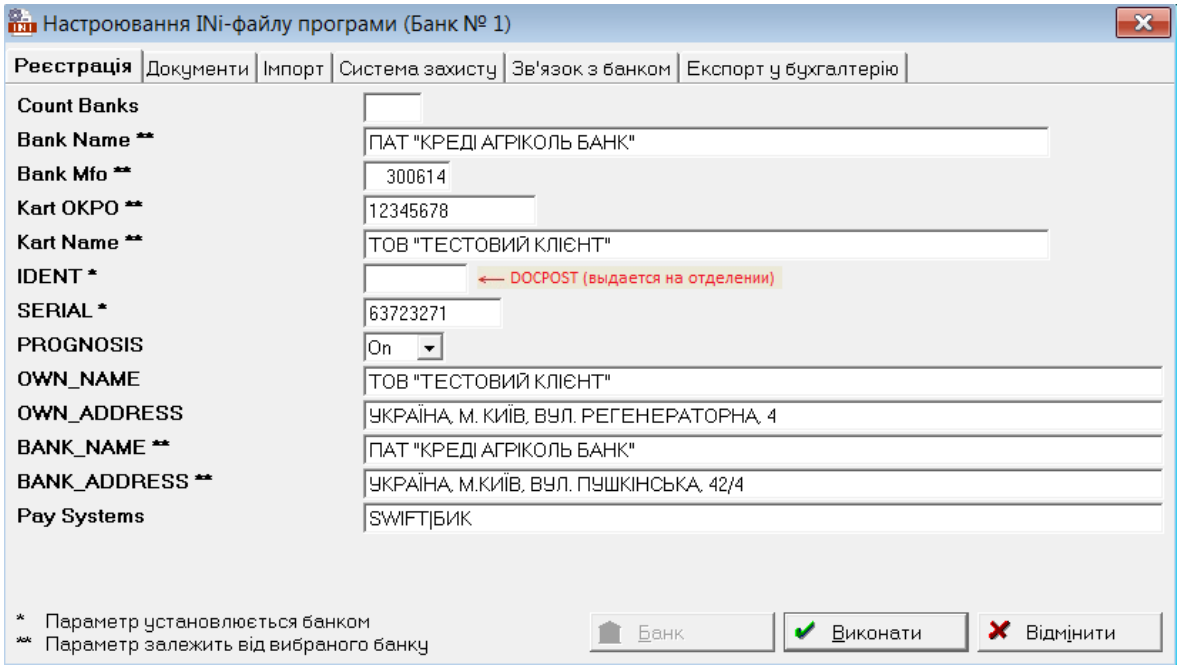

Рисунок 2 - Реєстрація в системі клієнт-банк

Після заповнення необхідно натиснути кнопку **Виконати**.

2. ЗАПОВНЕННЯ ПАРАМЕТРІВ ЗВ’ЯЗКУ

Необхідно обрати тип зв’язку, який буде використовуватись – Інтернет або модемне з’єднання. Це можна зробити зайшовши в меню **Обробка – Зв'язок з банком.**
Якщо Ви використовуєте з’єднання через Інтернет, натискаємо на кнопку **«Локальна мережа»**, як зображено на рис. 3, далі натискаємо кнопку **Настроїти зв'язок з банком (Ctrl+T),** як зображено на Рис. 4.

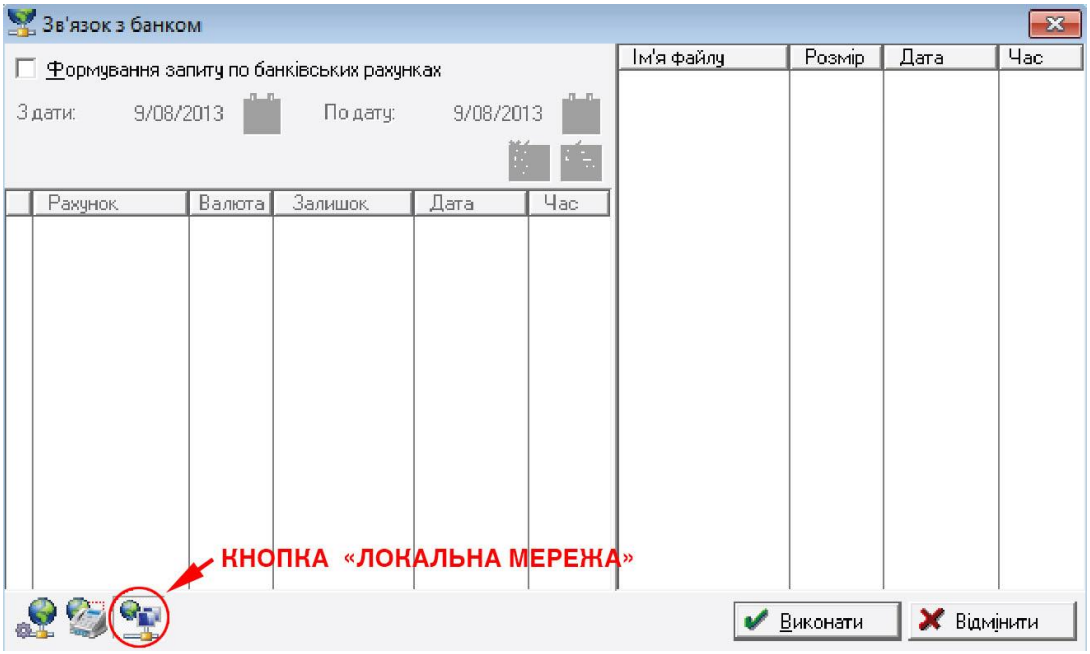

Рисунок 3 - Настроювання параметрів зв’язку з банком

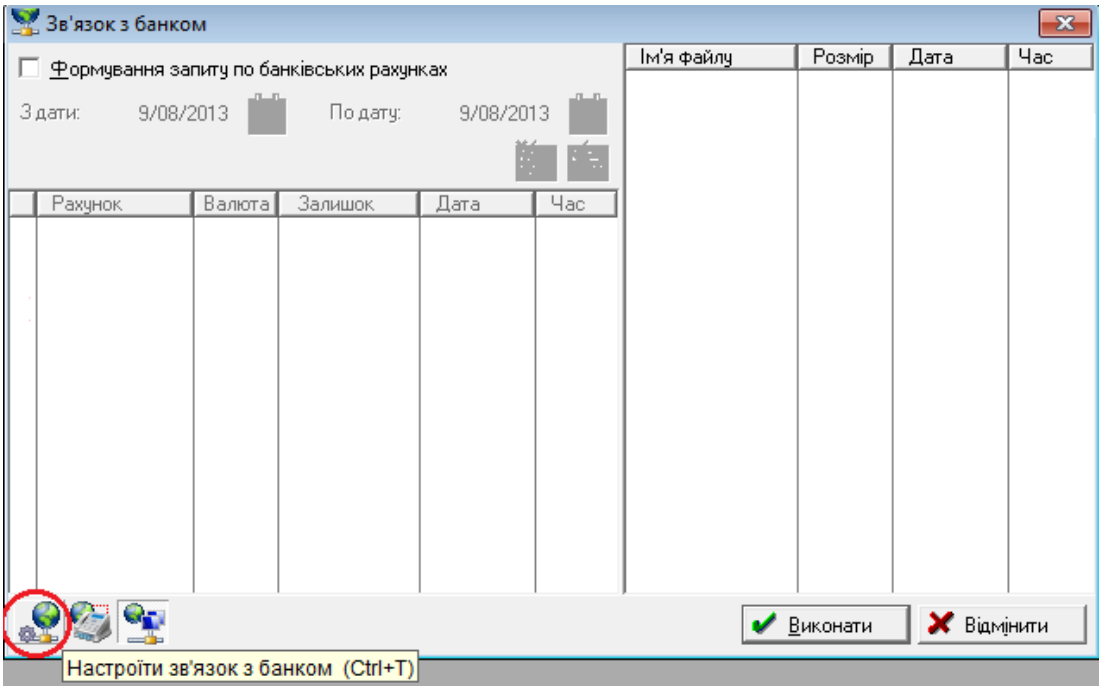

Рисунок 4 - Настроювання параметрів зв’язку з банком

У вікні **Параметри зв’язку (див. Рисунок 5)** на вкладці **Загальні,** необхідно заповнити параметри користувача:
Ім’я (Логін) – дана інформація надається у відділенні банку;
Пароль – дана інформація надається у відділенні банку;
Якщо у Вашій організації для виходу в Інтернет використовується Проксі-сервер, в параметрах проксі необхідно ввести адресу, порт та облікові дані для авторизації.

ЗВЕРНІТЬ УВАГУ: Всі **інші** налаштування даної вкладки **не повинні бути змінені**.

Приклад заповнення вкладки **Загальні**, наведено на рисунку 5.

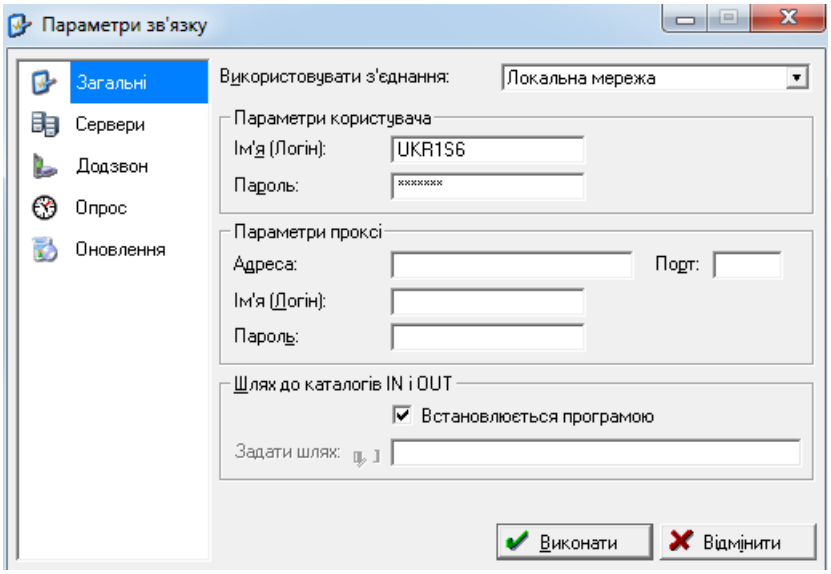

Рисунок 5 - Налаштування параметрів зв’язку.

Після заповнення необхідно натиснути кнопку **Виконати.**

ЗВЕРНІТЬ УВАГУ: При наявності в організації обмежень доступу в інтернет для роботи клієнт-банк, необхідно дозволити доступ до IP адреси 193.17.217.18, весь трафік на порт 7000. Якщо у Вас виникли питання, зверніться до свого системного адміністратора.

Якщо Ви використовуєте для зв’язку з’єднання через модем – необхідно натиснути кнопку **«Телефонне підключення»**, як зображено на Рис. 6.

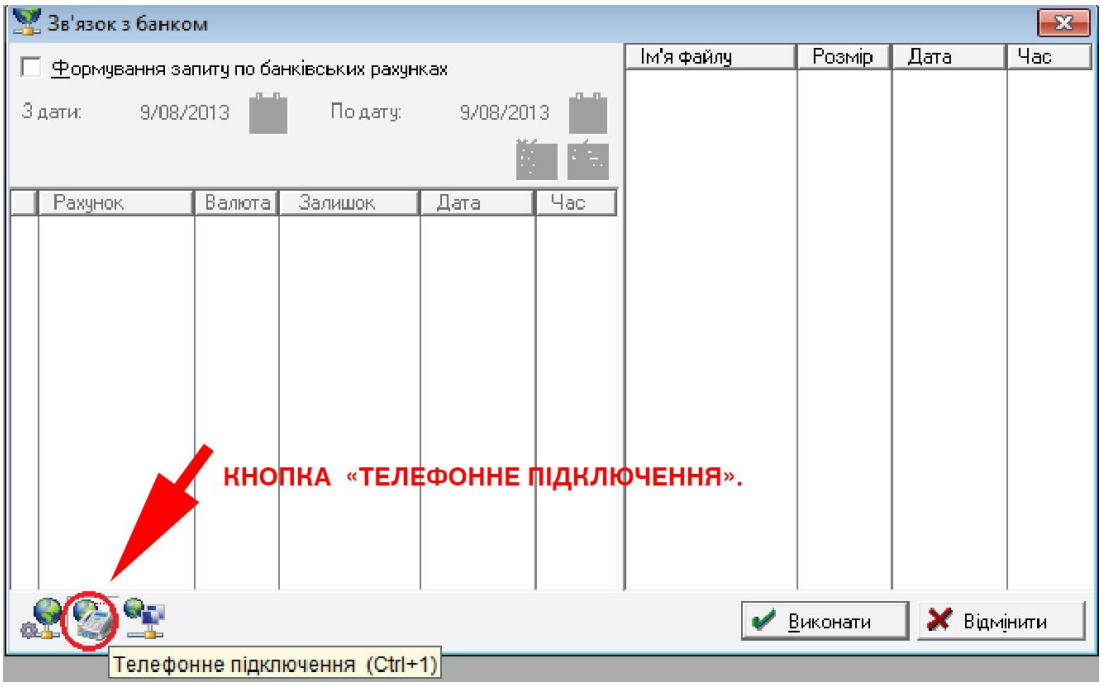

Рисунок 6 - Вибір та налаштування телефонного підключення

Далі **натискаємо кнопку Настроїти зв'язок з банком - Дозвін (див Рисунок 7),** та заповнюємо параметри користувача:
Ім’я користувача (Логін) – дана інформація надається у відділенні банку;
Пароль користувача – дана інформація надається у відділенні банку.
Після заповнення необхідно натиснути кнопку **Виконати.** **Приклад наведено на рисунку 7.**

ЗВЕРНІТЬ УВАГУ: Всі інші налаштування даної вкладки не повинні бути змінені.

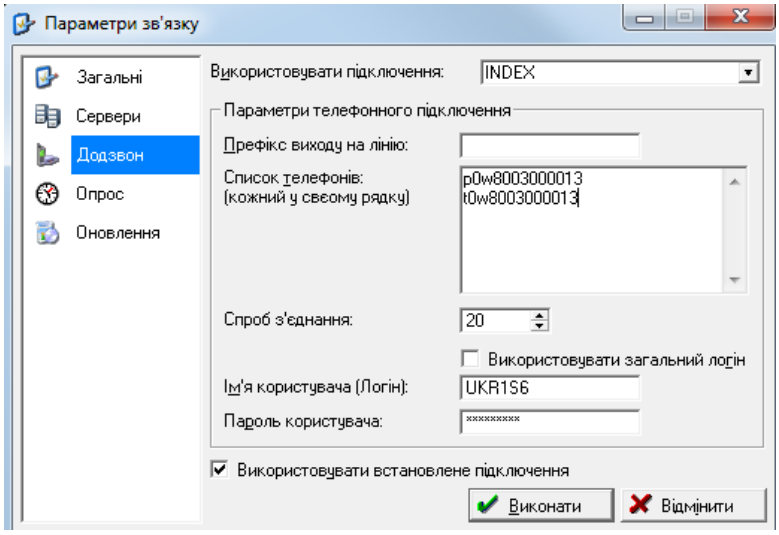

Рисунок 7 - Заповнення параметрів зв’язку телефонного підключення

ЗВЕРНІТЬ УВАГУ: Для роботи клієнт-банку за допомогою модему, необхідно створити телефонне з’єднання з іменем “INDEX”. Якщо у Вас виникли питання, зверніться до свого системного адміністратора.

3. НАЛАШТУВАННЯ ЗАХИСТУ

Необхідно зайти в меню **“Настроювання – Система захисту X.509”**. У вікні **“Центр управління системи захисту X.509”** (Рис. 8).

! Кожен новий користувач (посадова особа) особисто виконує генерацію ключів, за встановленим порядком (*див.п. 4.1- 4.4 цієї інструкції*).

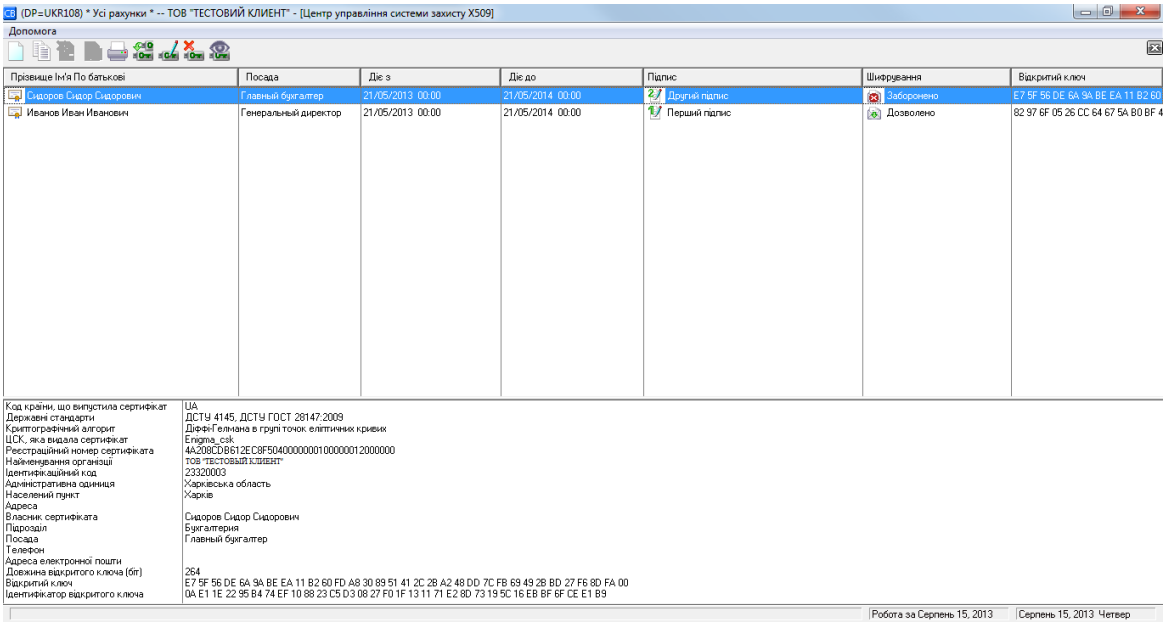

Рисунок 8 - Вікно “Центр управління системи захисту X.509”

УВАГА! Якщо форма організації клієнта Приватне Підприємство (ПП), Суб’єкт Підприємницької Діяльності (СПД), Фізична Особа Підприємець (ФОП) та клієнт не має в картці підписів організації бухгалтера, для повноцінної роботи з Клієнт-Банком достатньо створення лише ключа єдиного підпису (п. 4.4 даної Інструкції).
Якщо в картці підписів організації клієнта присутні директор та бухгалтер, для роботи з Клієнт-Банком необхідно обов’язково створити ключі першого та другого підпису. (п. 4.1 – 4.3 даної Інструкції).

4.1. ГЕНЕРАЦІЯ КЛЮЧА ЕЦП ПЕРШОГО ПІДПИСУ

Необхідно увійти до вікна центру управління системи захисту X.509 (меню **«Настроювання – Система захисту X.509»)**, натиснути **«Додати ключ посадової особи»** або **«Insert»** (щоб скопіювати і відредагувати існуючий ключ). Уважно заповнити всі поля вікна «Генерація ключа» (Рис. 9).

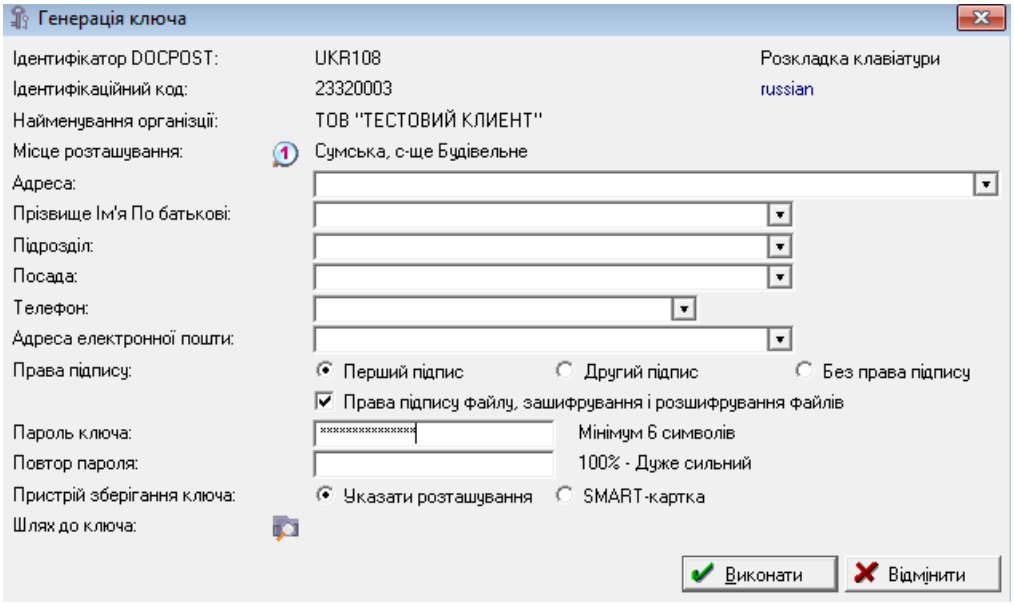

Рисунок 9 - Генерація ключа першої особи

УВАГА! Всі поля при генерації ключа заповнюються **українською мовою**, у відповідності до картки підписів клієнта.

у поле **«Прізвище Ім`я та по Батькові»** повністю вводиться П.І.Б. працівника, що **буде здійснювати підпис документів клієнт-банку**.
У поле **Посада** вводиться фактична посада даного працівника.
У поле **Підрозділ** вводиться назва фактичного підрозділу в організації даного працівника (якщо поділ на підрозділи відсутній – вводиться найменування організації).
У полі **Пароль ключа** та **Повтор паролю** вводиться пароль, яким буде зашифрований особистий (секретний) ключ. **Вимоги до паролю:** не менше 6 символів.
Поля **«Місце розташування»** та **«Шлях до ключа»** заповнюються за допомогою спеціальних кнопок меню (Рис. 9а та 9б).

УВАГА! Обираючи шлях до ключа доцільно буде відразу зберегти ключ на зовнішньому носії (flash cd, смарт-карта) з міркувань інформаційної безпеки**. Якщо в якості носія використовується токен, необхідно обрати опцію Smart-картка та вказуючи шлях до ключа в розділі е.ключ IIT Алмаз-1К обрати серійний номер токена.**

У рядку «Права підпису» слід вибрати **«Перший підпис»**.
Обов’язкові для заповнення: «ПІБ», «Підрозділ», «Посада», пароль, місце розташування та шлях до ключа.
Детальні пояснення по кожному полю наведені у файлі допомоги програми. Цей файл доступний з вікна **“Генерація ключа”** або по натисканню клавіші **“F1”**.

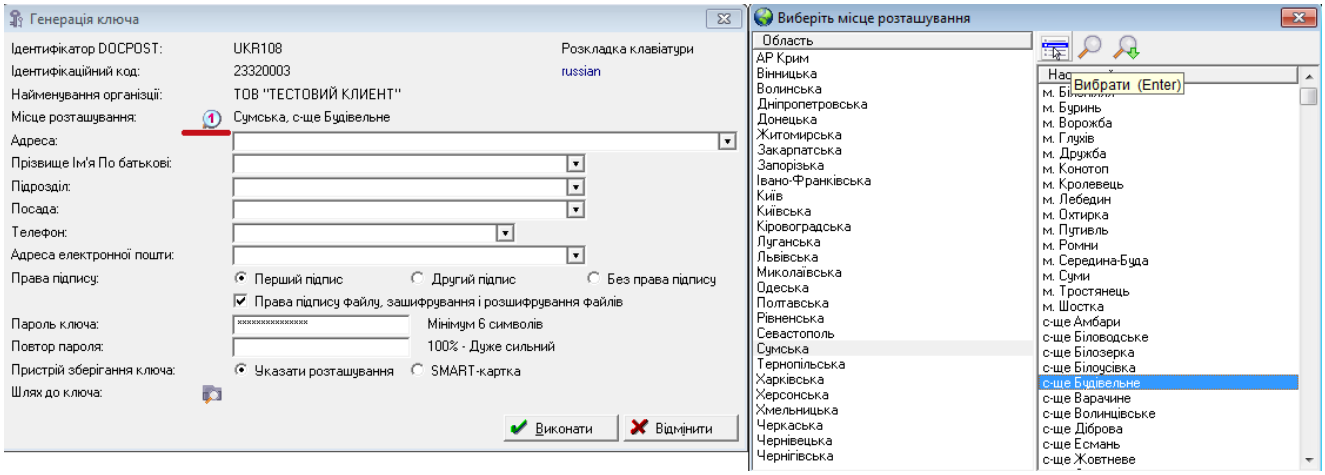

Рисунок 9а - Генерація ключа першої особи, вибір місцезнаходження.

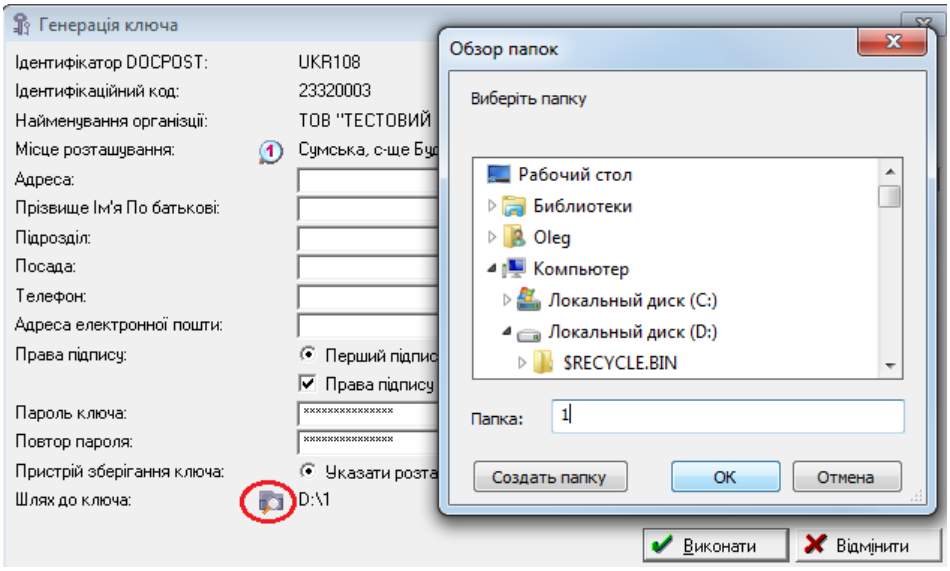

Рисунок 9б - Генерація ключа першої особи,вибір шляху до ключа

Після внесення та перевірки усіх параметрів натиснути **«Виконати».**

4.2. ГЕНЕРАЦІЯ КЛЮЧА ЕЦП ДРУГОГО ПІДПИСУ, ТА КЛЮЧА БЕЗ ПРАВА ПІДПИСУ

У вікні центру управління системи захисту X.509 (меню **«Настроювання – Система захисту X.509»)** натиснути **«Додати ключ посадової особи»** або **«Insert».** Уважно заповнити всі поля форми «Генерація ключа» (Рис. 10).
Вибрати права **«Другий підпис»,** або у випадку якщо працівник Вашої організації наділений повноваженнями **лише** прийому та відправки документів в Банк **– «Без права підпису»**. Для генерації ключа БЕЗ права підпису обов’язково оберіть (поставте «галочку») для опції «Права підпису файлу, шифрування і розшифрування файлів».

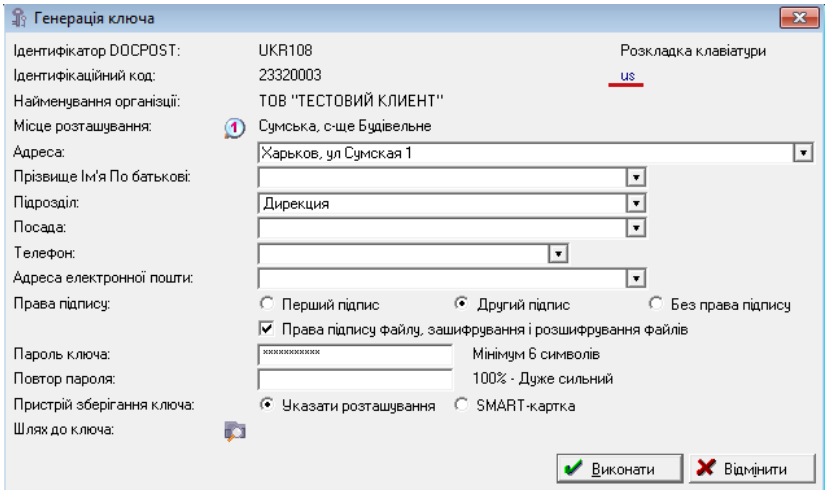

Рисунок 10 - Генерація ключа другої особи

ЗВЕРНІТЬ УВАГУ: Всі вимоги щодо створення ключа ЕЦП другого підпису аналогічні вимогам, що стосуються створення ключа ЕЦП першого підпису (наведені в пункті 4.1 даної Інструкції).
Після внесення та перевірки усіх параметрів натиснути **«Виконати»**.

4.3. ГЕНЕРАЦІЯ КЛЮЧА ЄДИНОГО ПІДПИСУ

Якщо форма організації клієнта Приватне Підприємство (ПП), Суб’єкт Підприємницької Діяльності (СПД), Фізична Особа Підприємець (ФОП), та клієнт не має в картці підписів організації бухгалтера, генерація ключів першого та другого підпису не обов’язкова.
У такому випадку, достатньо виконати генерацію ключа єдиного підпису. Для налаштування можливості генерації ключа єдиного підпису, необхідно увійти в меню **Сервіс – Настроювання ini-Файлу,** вкладка **Система захисту**. Встановити значення поля **“Single signature”** в **“On”**, натиснути **«Виконати»**.

ЗВЕРНІТЬ УВАГУ: Всі інші налаштування даної вкладки не повинні бути змінені.
Приклад налаштування на єдиний підпис наведено на рисунку 11.

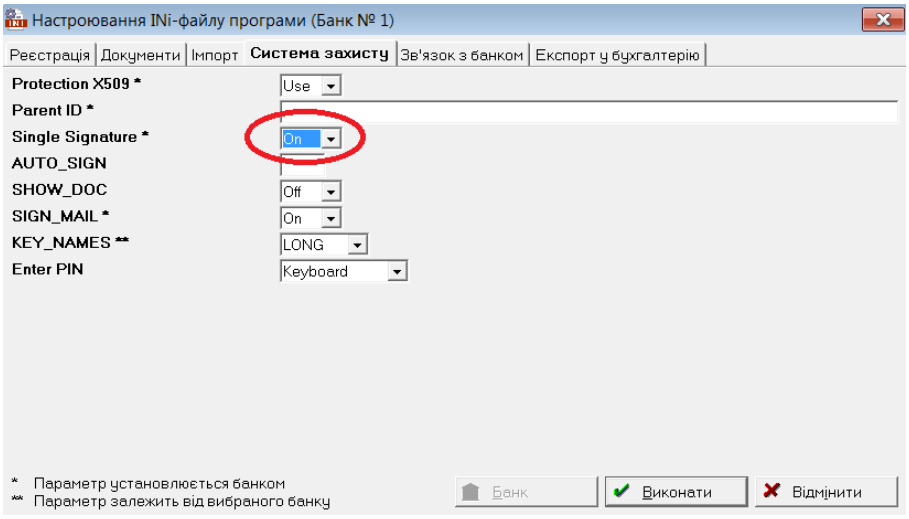

Рисунок 11 – Налаштування для генерації єдиного підпису

Далі, у центрі управління системи захисту X.509 натиснути **«Додати ключ посадової особи»** або **«Insert».** Уважно заповнити всі поля форми «Генерація ключа» (Рис. 12). Вибрати права підпису **«Підпис документа»**.

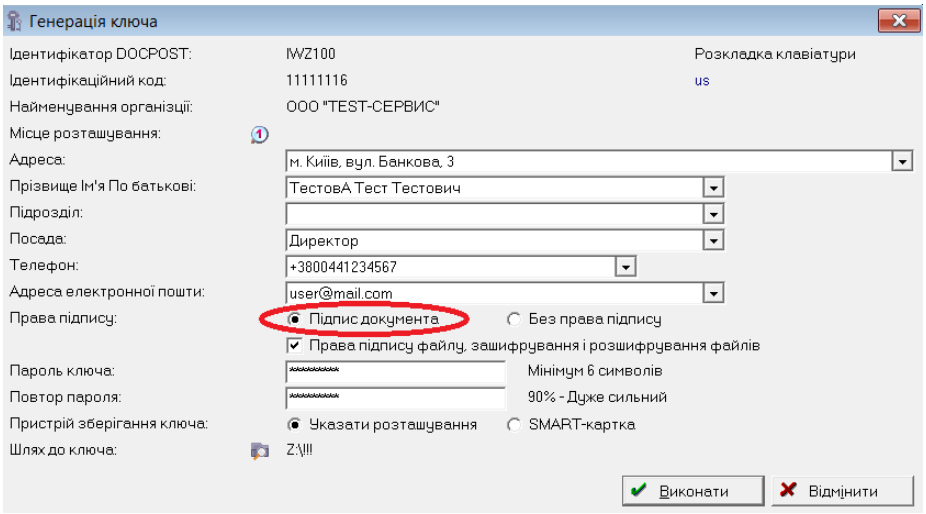

Рисунок 12 – Генерація ключа єдиного підпису

У випадку, коли клієнту з єдиною особою в картці підписів в організації, необхідно лише отримувати виписки по рахункам з Банку, без права відправляти до Банку платіжні документи, необхідно виконати генерацію ключа без права підпису. Для цього, натиснути **«Додати ключ посадової особи»** або **«Insert».** Уважно заповнити всі поля форми «Генерація ключа» (Рис. 12а). Вибрати права підпису **«Без права підпису»** та **обов’язково** вибрати опцію «**Права підпису файлу, шифрування і розшифрування файлів**».

ЗВЕРНІТЬ УВАГУ: Всі вимоги щодо створення ключа ЕЦП єдиного підпису аналогічні вимогам, що стосуються створення ключів ЕЦП першого та другого підпису (наведені в пункті 4.1, 4.2 даної Інструкції).

Після внесення та перевірки усіх параметрів натиснути **«Виконати»**.

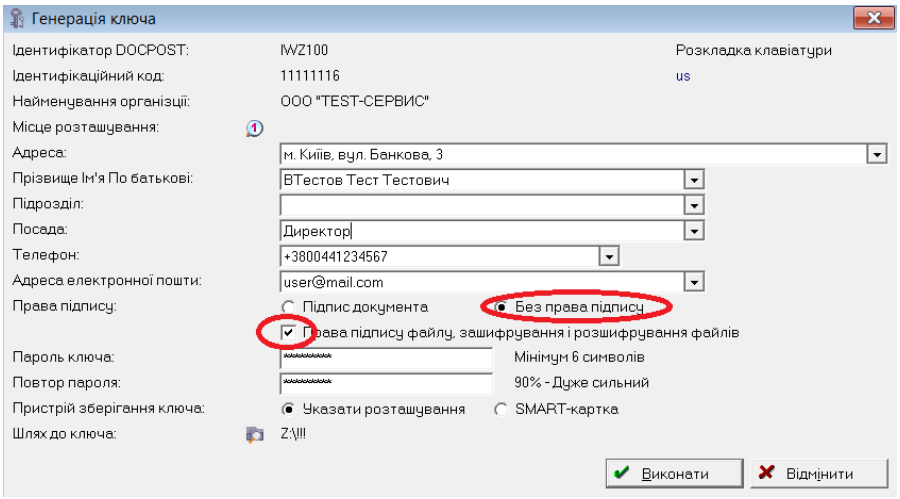

Рисунок 12а – Генерація ключа без права підпису для отримання виписок з Банку

4.4. ДРУК ЗАПИТІВ НА СЕРТИФІКАЦІЮ ТА ЗБЕРЕЖЕННЯ ЇХ В ФАЙЛ

Наступним кроком в банк необхідно надати зразки відкритого ключа посадової особи в **електронному вигляді** та на **паперовому носієві в одному** екземплярі.
Щоб передати запити в електронному вигляді: «Головне меню-Обробка –зв'язок з банком – Виконати» *(файли запитів на сертифікацію створюються автоматично)*
Переконайтеся, що запити було успішно відправлено до банку, для цього: «Головне меню - Обробка – Зв'язок з банком - **перегляд FTP-протоколу**», файли запитів були успішно відправлені.
У разі необхідності, запити можна сформувати знову (меню “Настроювання – Система захисту X.509”), встановити курсор на необхідний запит та натиснути  (**“Повторно зберегти запит на сертифікат” або “Ctrl+S”).**
Далі необхідно надрукувати **паперовий зразок** відкритого ключа за кнопкою **“Надрукувати запит на сертифікат (Ctrl+P)”**  у вікні “Центр управління системи захисту X.509” (меню “Настроювання – Система захисту X.509”).
Для цього у списку шаблонів звітних форм оберіть “Запит на сертифікат” (Рис.12б) та натисніть “Enter”.

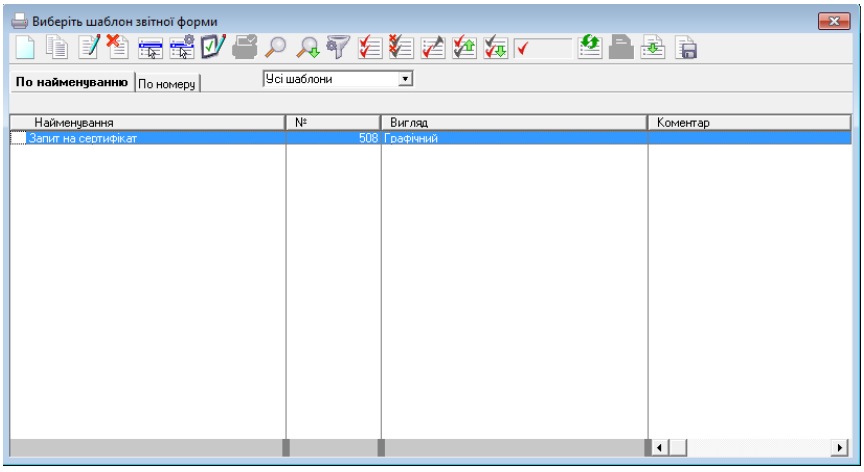

Рисунок 12б - Вибір запиту на сертифікат для друку.

У формі друку зняти опції “Попередній перегляд” та натиснути “Виконати”. (Рис. 13)

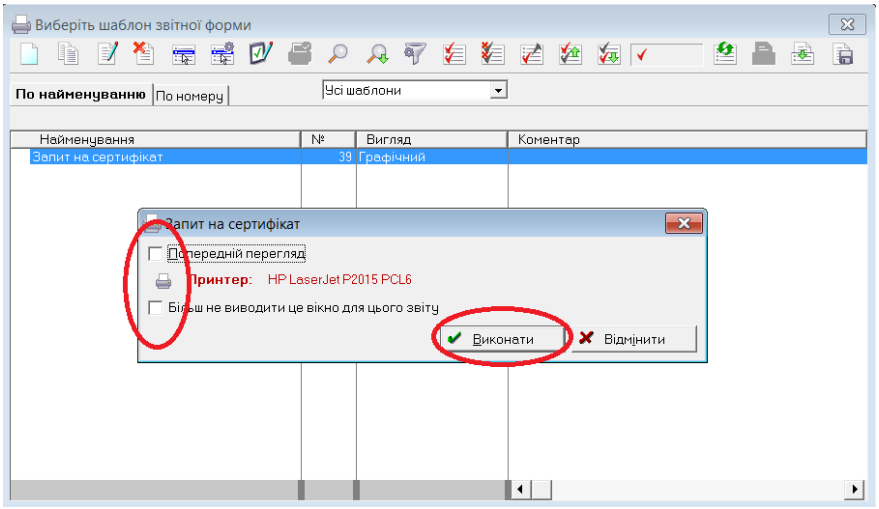

Рисунок 13 - Друк запиту на сертифікат.

УВАГА! Всі роздруковані паперові екземпляри **повинні бути завізовані підписами власників ключів та скріплені печаткою організації.** Поле **Підпис власника підтверджую** заповнюється відповідальною особою клієнта (керівник, директор), що має право підтвердити підпис та повноваження власника ключа. **Паперові екземпляри клієнтом передаються у відділення банку, попередньо переконавшись, що банк отримав електронні запити на сертифікацію.**

Після реєстрації запитів на сертифікацію в Головному офісі банку, на їх основі будуть створені сертифікати, які будуть відправлені на адресу Вашої організації каналами клієнт-банку. Щодо інформації про завершення реєстрації на стороні Банку необхідно звернутися до відділення.

4.5. ОТРИМАННЯ СЕРТИФІКАТУ КЛЮЧА ПОСАДОВОЇ ОСОБИ ОРГАНІЗАЦІЇ

Після підтвердження завершення реєстрації на стороні банку важливо отримати сертифікат (пакету сертифікатів) **на стороні клієнта**. З цією метою необхідно виконати: «**Обробка- Зв'язок с банком» - «Виконати». Перевірка** успішного прийому сертифікату (пакету сертифікатів): «Настроювання-Система захисту X.509».

У вікні замість запитів на сертифікацію (позначення -), з`являться сертифікати (позначення -), з відповідними повноваженнями, датою початку та закінчення терміну дії (Рисунок 14).

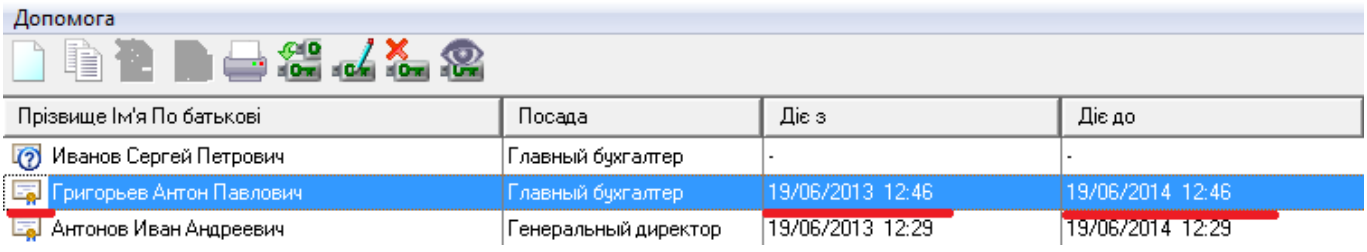

Рисунок 14 - Успішний прийом сертифікаті від банку

Тепер сертифікати успішно отримані і встановлені. Посадові особи можуть починати роботу з фінансовими документами, відповідно повноважень їх ключів.
Ключ дійсний 1 рік з моменту сертифікації ключа банком.

ЗВЕРНІТЬ УВАГУ: Рекомендується зберігати таємний ключ на з’ємних носіях (flash, cd, смарт-карти) з міркувань інформаційної безпеки.

5.1. ЗМІНА ПАРОЛЯ НА КЛЮЧ ЕЦП

Для зміни паролю необхідно у вікні “Центр управління системи захисту X.509” натиснути кнопку “Змінити пароль ключа на носії”.
У формі “Зміна паролю ключа” на носії (Рис. 15) встановити місцезнаходження файлу особистого ключа, ввести старий, та двічі новий пароль. Натиснути “Виконати”. Пароль змінено. До нової парольної фрази застосовуються всі ті ж самі вимоги, як при генерації ключів (Наведені в п. “4.1 Генерація ключа ЕЦП першого підпису ” інструкції).

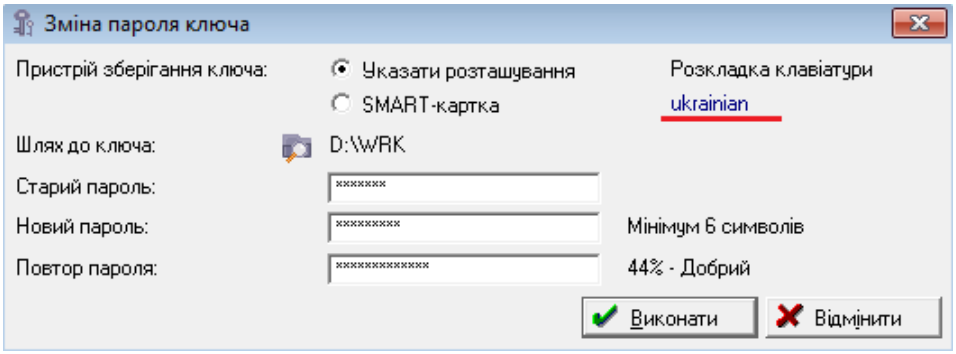

Рисунок 15 - Форма зміни паролю особистого ключа на носієві

У разі помилки, програма надасть повідомлення з текстом причини збою.

ЗВЕРНІТЬ УВАГУ: Зміна паролю **НЕ подовжує** строк дії існуючого ключа. Для планової своєчасної зміни ключів необхідно повторно пройти процедуру генерації ключів, наведену у **розділі 4** інструкції.

5.2. ВІДКЛИКАННЯ СЕРТИФІКАТУ

УВАГА!: У разі компрометації чи втрати особистого ключа сертифікат відкритого ключа посадової особи **повинен бути терміново заблокований/скасований.** Для цього необхідно терміново звернутися в найближче відділення банку особисто або телефоном. Також сертифікат може бути відкликано у результаті рішень зміни посадової особи, припинення діяльності організації, закінчення строку дії особистого ключа тощо.

Для відкликання сертифікату слід надрукувати **1 копію** запиту на відкликання сертифікату, завірити її **печаткою та особистим підписом посадової особи** (керівник, директор), надати примірники **у відділення банку**. Для цього увійти до центру управління системою захисту X.509, встановити курсор на сертифікат, що відкликається, та натиснути кнопку **“Надрукувати запит на відкликання сертифікату Ctrl+P”.** (У списку шаблонів звітних форм оберіть “Запит на відкликання сертифікату X.509” (Рис.16) та натисніть “Enter”).

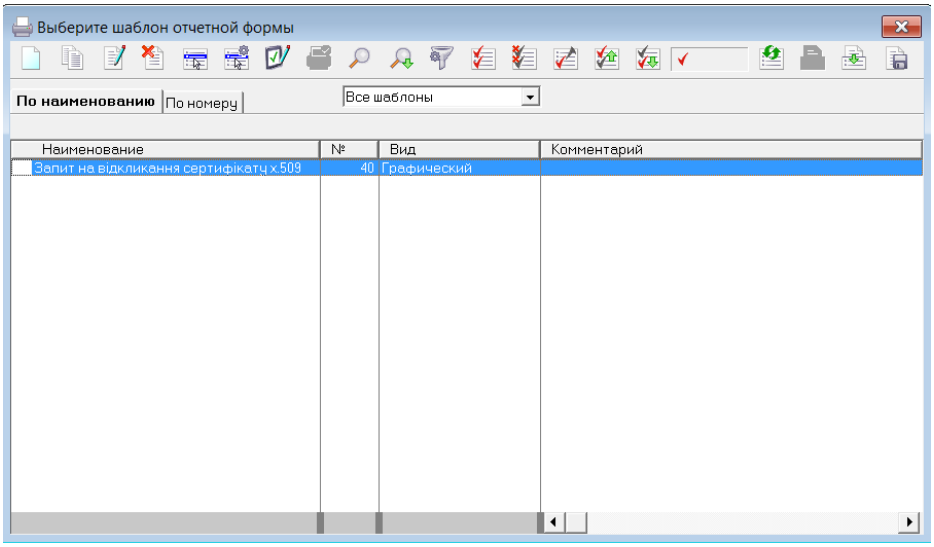

Рисунок 16 - Вибір Запит на відкликання сертифікату X.509.

У формі друку зняти опції “Попередній перегляд” та натиснути “Виконати”. (Рис. 17).

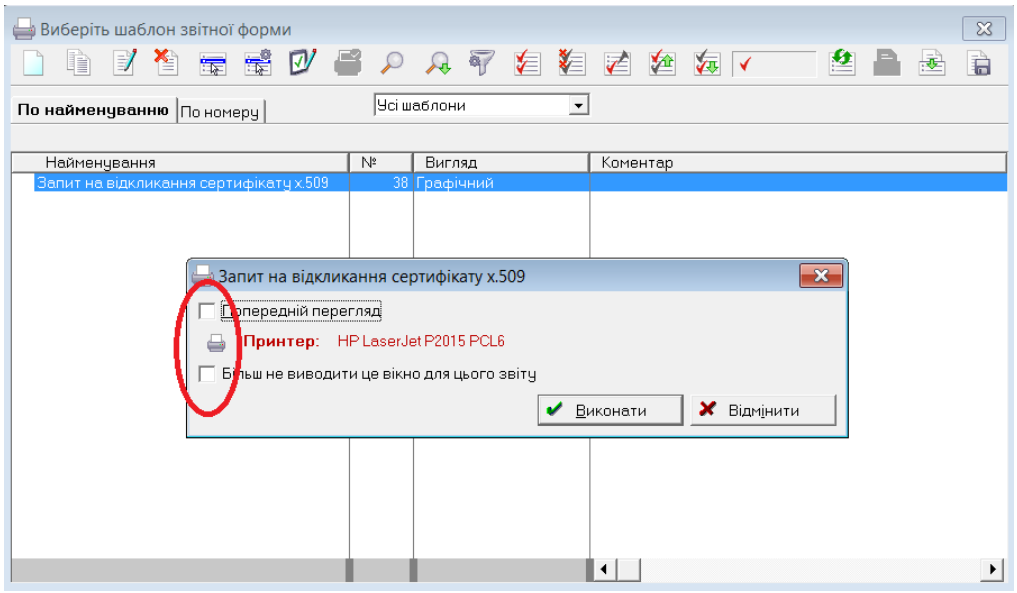

Рисунок 17 - Друк запиту на відкликання сертифікату X.509.

УВАГА! Після завірення примірників запитів печаткою та особистим підписом посадової особи, запити необхідно, обов’язково, передати адміністратору реєстрації банку. *Для прискорення виконання блокування, спочатку, можливо надіслати відсканований примірник запиту адміністратору Банку засобами електронної пошти.*
Після обробки банком запитів, з наступним сеансом зв’язку, статус сертифікату буде оновлено. У списку сертифікатів вікна «Система захисту X.509» зміниться індикація сертифікату з  на  , як не діючого.

5.3. ПЕРЕГЛЯД КОНТЕКСТУ ТАЄМНИХ КЛЮЧІВ

Для перегляду контексту таємних ключів ЕЦП на різних носіях увійдіть до меню **центру управління системою захисту X.509**.

Натисніть кнопку **“Переглянути контекст секретних ключів”** (Рис. 18).

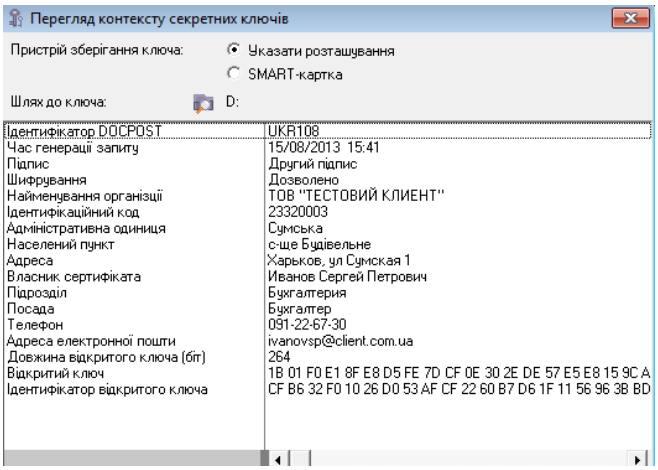

Рисунок 18 - Перегляд контексту секретного ключа

У вікні доступні для перегляду всі реквізити секретного ключа, якщо вони були задані. **Примітка:** можливість роботи режиму зі смарт-картами залежить від типу та фірми-виробника пристрою.

5.4 СТВОРЕННЯ РЕЗЕРВНОЇ КОПІЇ ТА ВИДАЛЕННЯ ОСОБИСТОГО КЛЮЧА

Необхідно увійти до меню **центру управління системою захисту X.509**. Натиснути кнопку “Створити резервну копію ключа (F5)”. (Рис. 19).

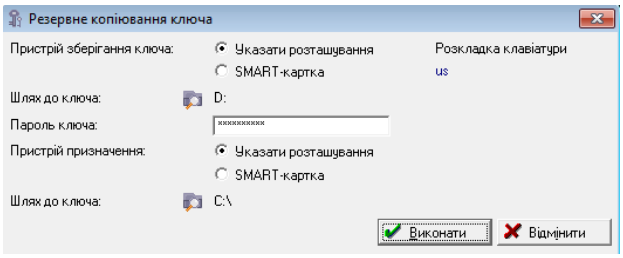

Рисунок 19 - Форма резервного копіювання

Необхідно вказати розташування місця зберігання ключа, пароль та місце зберігання резервної копії. **Видалення ключу здійснюється за допомогою кнопки** “Видалити ключ носія”, у центрі управління системою захисту X.509. У формі видалення ключа необхідно указати розташування та ввести вірний пароль, натиснути «Виконати». Можливість роботи режиму зі смарт-картами залежить від типу та фірми-виробника пристрою.