САЙФЕР

Сайфер БІС, ТОВ
04107, Київ, вул. Нагірна 25/27, 3-ій поверх

Тел.: +38 (044) 484-4612
Факс: +38 (044) 483-0322
E-mail: info@cipher.com.ua
Web: www.cipher.com.ua

Дата модифікації: 20/08/2020

Єдиний Криптографічний Центр

Настанова з установки та експлуатації Агенту ЄКЦ (Java)

ЗМІСТ

Вступ

В цьому документі описано порядок дій користувача для використання програмного комплексу «Єдиного Криптографічного Центру», а саме Агенту ЄКЦ (Java) його функціональні можливості та необхідні відомості для роботи з ним.

Системні вимоги

Перед початком встановлення та роботи з програмним застосуванням необхідно переконатися, що програмне та апаратне забезпечення відповідає рекомендаціям розробника.

Мінімальні вимоги до апаратного забезпечення:

- Оперативна пам'ять: 512 МБ та вище;
- Процесор – 1,2 ГГц;
- LAN: 10 Мбіт/с.

Мінімальні вимоги до програмного забезпечення:

- Вимоги до ОС:
  - ОС Windows (Windows XP і вище, Windows Server 2008 R2 з SP1 і вище)
  - ОС Linux (Ubuntu Linux 12.04 і вище, CentOS 6 і вище та ін.)
  - ОС MacOS X (10.7.3 і вище)
- Браузери, що підтримуються:
  - Internet Explorer 11;
  - Mozilla Firefox;
  - Google Chrome.
- Java:
  - ОС Windows XP (лише 8u111).
  - ОС Windows 7/8/10 (8u152 і вище).
  - ОС Linux (8u25 вище та ін.)

Підготовка робочого місця для роботи з сервісом

Введення

Програмний комплекс «Агент Єдиного Криптографічного Центру» реалізований мовою програмування Java, що дозволяє виконувати запуск на таких платформах:

- ОС Linux.
- ОС Windows.
- ОС MacOS.

Основною умовою для користування «Агентом Єдиного Криптографічного Центру» є встановлена Java машина. Для того щоб перевірити, чи середовище Java встановлено на комп'ютері і чи коректно працює, потрібно запустити тестовий аплет http://java.com/ru/download/installed.jsp?detect=jre.

За відсутності на комп’ютері користувача Java-машини – запуск програмного комплексу неможливий, тому необхідно інсталювати її. Для початку потрібно завантажити дистрибутив відповідної компоненти (JRE) з офіційного сайту Java за посиланням java.com та слідувати відповідним інструкціям.

Якщо встановлена операційна система Windows XP, то з останніми версіями Java, «Агент Єдиного Криптографічного Центру» працює некоректно, тому слід завантажити за посиланням jre-8u111-windows-i586.exe (розрядність даної версії Java x32) та встановити саме цю версію.

Підтримка захищених носіїв

Агент Єдиного криптографічного центру підтримує роботу із захищеними носіями.

Захищений апаратний носій у пасивному режимі – підтримує збереження особистого ключа у захищеному ключовому контейнері. Доступ до ключа здійснюється за допомогою інтерфейсу PKCS#11. До таких носіїв відносяться:

- Avest Avest-Key.
- Efit Key.
- Author Secure Token-337 Series, Author Smart Card-337 Series (обов’язкове розміщення бібліотеки у залежності від розрядності Java).
- Gemalto IDPrime.
- Gemalto eToken, SafeNet eToken, Aladdin eToken.
- jaCarta.
- eAladdin eToken.
- G&D StarSign Token, G&D StarSign Card.
- ІІТ Алмаз (обов’язкове встановлення ПЗ: EKAlmaz1CInstall.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- ІІТ Кристал (обов’язкове встановлення ПЗ: EKeyCrystal1Install.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).

Захищений апаратний носій у активному режимі – самостійно здійснює створення ЕП за допомогою особистого ключа у захищеному контейнері. Виконання операції з ЕП здійснюється за допомогою PKCS#11 інтерфейсу. До таких носіїв відносяться:

- Avest Avest-Key.
- Efit Key.
- Author Secure Token-337 Series, Author Smart Card-337 Series (обов’язкове розміщення бібліотеки у залежності від розрядності Java).
- ІІТ Алмаз (обов’язкове встановлення ПЗ: EKAlmaz1CInstall.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- ІІТ Кристал (обов’язкове встановлення ПЗ: EKeyCrystal1Install.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- Plasticard TEllipse (обов’язкове встановлення ПЗ та розміщення бібліотеки у залежності від розрядності Java).

Avtor Secure Token – 337

Для роботи із захищеними носіями Avtor Secure Token у Агенті Єдиного криптографічного центру, необхідні додаткові бібліотеки **Av337CryptokiD.dll** (x32/x64 у залежності від розрядності Вашої операційної системи та розрядності Java).

Додатковий .dll файл можна отримати у розробника захищеного носія, компанії Автор, або завантажити за посиланням, вказані нижче, та розмістити за шляхом:

1. Для ОС Windows x86 та Java RE x32 **Av337CryptokiD.dll**. Бібліотеку слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: ***C:\Program Files (x86)\Java\jre1.8.0_181\bin.***

   Завантажити архів можна за посиланням - x86_Av337CryptokiD.rar

2. Для ОС Windows x64 та для Java RE x64 **Av337CryptokiD.dll**. Бібліотеку слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: ***C:\Program Files\Java\jre1.8.0_181\bin.***

   Завантажити архів можна за посиланням - x64_Av337CryptokiD.rar

Для продовження роботи, необхідно повернутися до «Агенту Єдиного криптографічного центру» та заповнити всі поля:

- Завантажити **Агент ЄКЦ**.
- Вказати **АЦСК/КНЕДП**.
- Вказати **Активний** чи **Пасивний режим**.
- Обрати захищений носій, натиснувши «**...**».
- Вказати **PIN-код** до носія.
- Натиснути кнопку **Розпочати роботу з ключем**.

Якщо захищений носій не виявлено, зверніться до:

- Постачальника захищених носіїв.
- Розробника захищених носіїв.
- Розробника «Єдиного криптографічного центру».

Подальша робота «Єдиного криптографічного центру» з PKCS#11 пристроями можлива тільки після повного усунення питань, пов'язаних з правильною роботою захищених носіїв.

Після встановлення програмного забезпечення для роботи із захищеними носіями, слід переконатися, що операційна система виявила їх та відображає в «Диспетчере устройств». Для перевірки необхідно перейти «Пуск»->«Панель управления»->«Диспетчер устройств»-> «SmartCard Reader».

Робота з Агентом Єдиного Криптографічного Центру

Запуск

У веб-браузері перейти за посиланням - https://cryptocenter.kredobank.com.ua/ до Клієнту Єдиного Криптографічного Центру.

Відеоінструкція знаходиться за посиланням.

Покрокова інструкція та ознайомлення з інтерфейсом програмного комплексу:

1. Стартове вікно Клієнту Єдиного Криптографічного Центру у веб-браузері показано на Рис. 1.

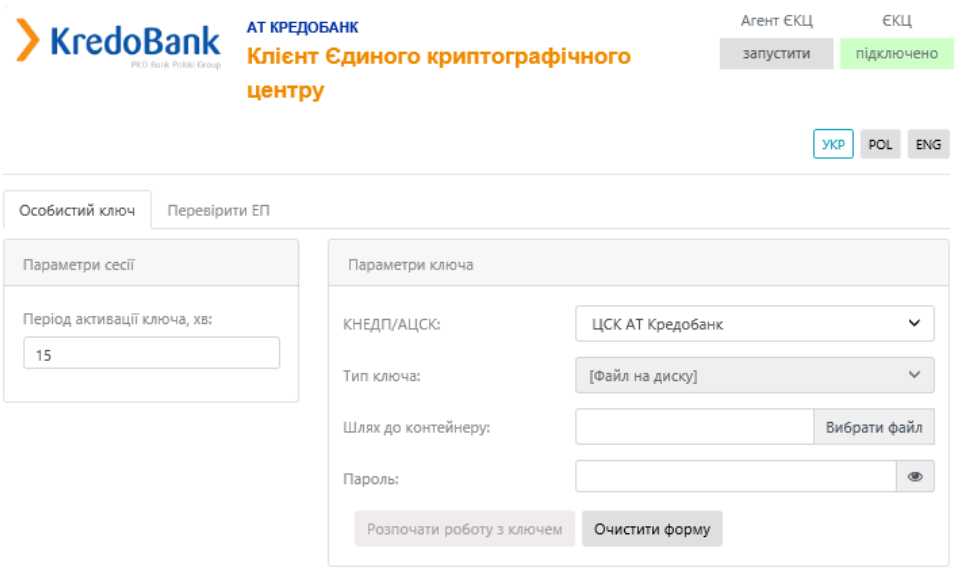

Рис. 1. Стартове вікно ЄКЦ

2. Наступним кроком слід відкрити Агент ЄКЦ, натиснувши у правому верхньому куті під написом Агент ЄКЦ кнопку «запустити», Рис. 2.

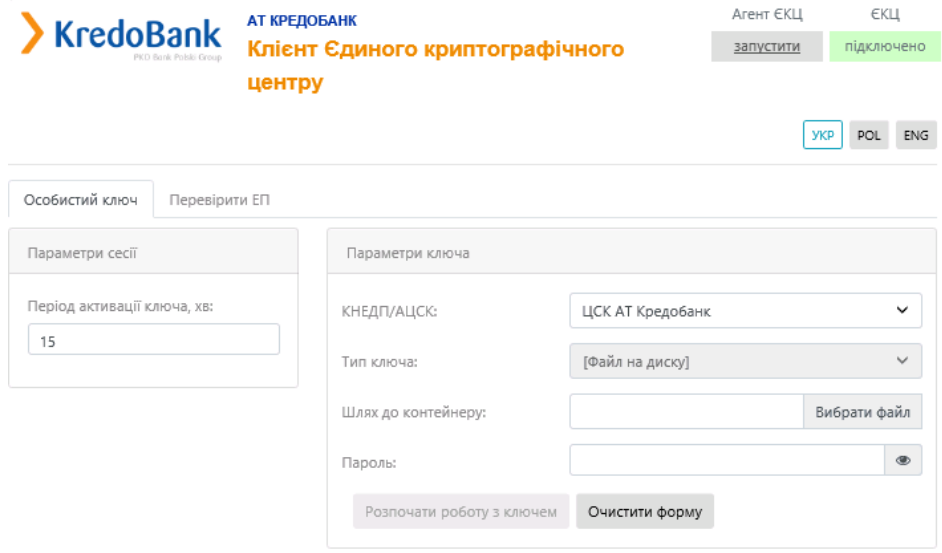

Рис. 2. Запуск Агенту ЄКЦ

3. Далі відкривається вікно Агенту єдиного криптографічного центру, Це означає що Агент запущено, все працює коректно, його слід згорнути та повернутися до веб-браузера, Рис. 3.

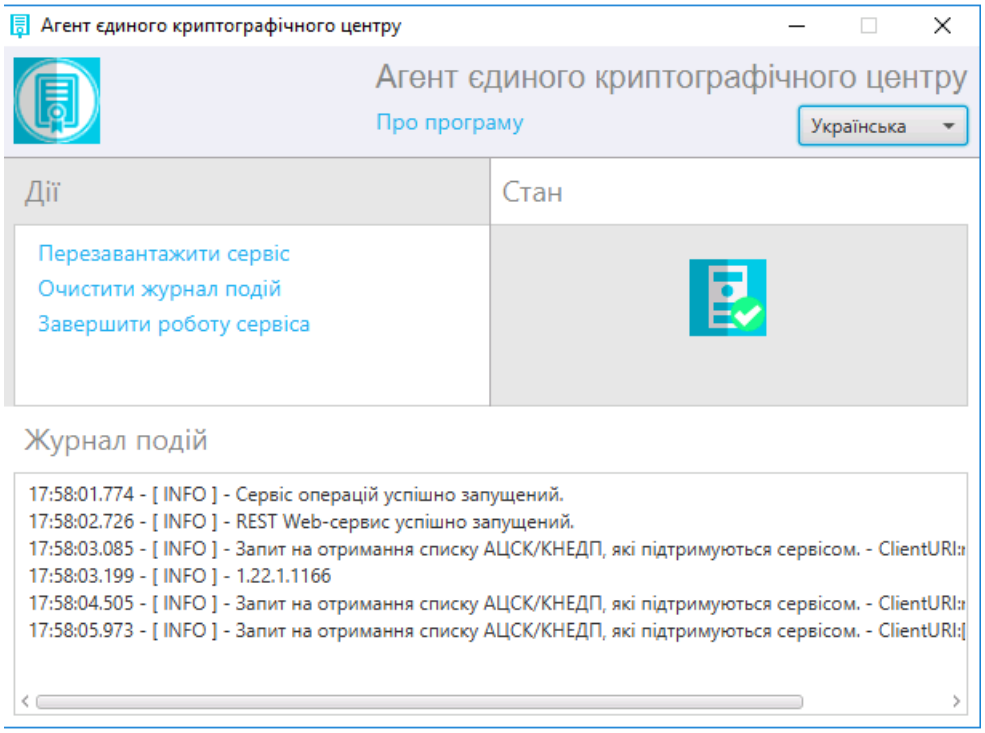

Рис. 3. Вікно «Агенту єдиного криптографічного центру»

4. У веб-сторінці одразу помітні зміни. Статус Агенту ЄКЦ змінено на «підключено» та став доступний для змін пункт «Тип ключа», Рис. 4.

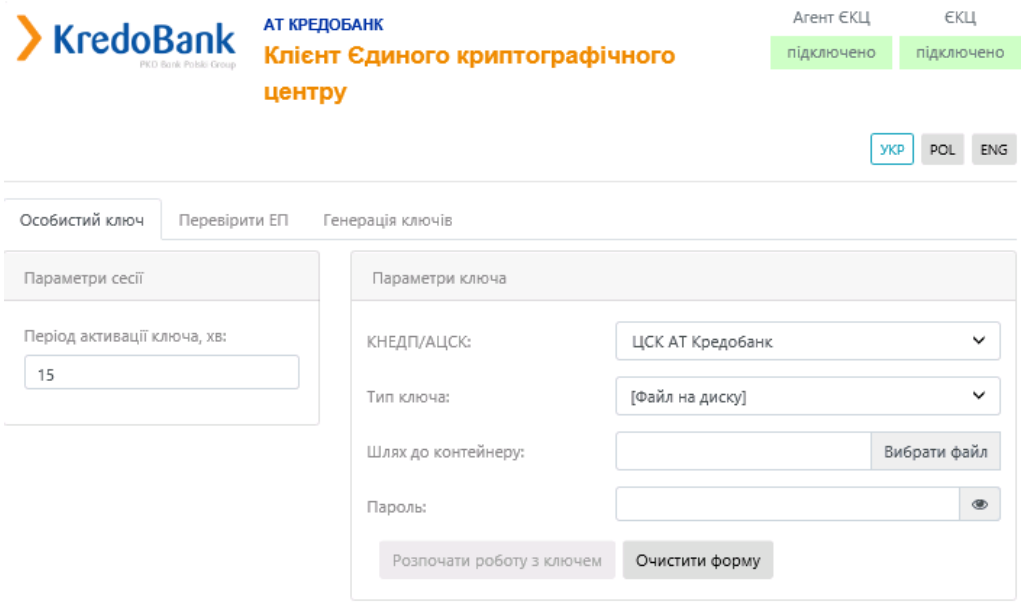

Рис. 4. Стартове вікно Агент ЄКЦ

5. На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвилинах період активації ключа, за замовчуванням 15 хв.
6. На вкладці «Особистий ключ» у розділі «Параметри ключа» слід вказати:
   1. ***КНЕДП/АЦСК***, у якому було отримано ключ;

Перелік КНЕДП/АЦСК, які підтримуються «Агентом Єдиного Криптографічного Центру»:

- ЦСК АТ Кредобанк;
- АЦСК/КНЕДП Національного банку України;
- КНЕДП ІДД ДПС;
- КНЕДП «ДІЯ»;
- АЦСК/КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
- АЦСК/КНЕДП АТ «КБ «Приватбанк»;
- АЦСК/КНЕДП ПАТ «УкрСиббанк»;
- АЦСК/КНЕДП «Masterkey» ТОВ «Арт-мастер»;
- АЦСК/КНЕДП Збройних Сил;
- АЦСК/КНЕДП Міністерства внутрішніх справ України;
- КНЕДП Державної прикордонної служби;
- АЦСК/КНЕДП Укрзалізниці;
- КНЕДП «АЦСК ринку електричної енергії»;
- АЦСК/КНЕДП ПАТ «Національний депозитарій України»;
- АЦСК/КНЕДП ТОВ «Ключові системи»;
- КНЕДП ДП «Українські спеціальні системи»;
- АЦСК/КНЕДП Генеральної прокуратури України;
- АЦСК/КНЕДП АТ «Ощадбанк»;
- КНЕДП Казначейства (з ключами, які отримано після 31.01.2020);
- КНЕДП ТОВ «Депозит Сайн».

2. ***Тип ключа***:
   - файл на диску;
   - PKCS#11 пристрої – активний режим;
   - PKCS#11 пристрої – пасивний режим.
3. ***Шлях до контейнеру***;
4. ***Пароль*** до ключа чи PIN до захищеного носія, Рис. 5.

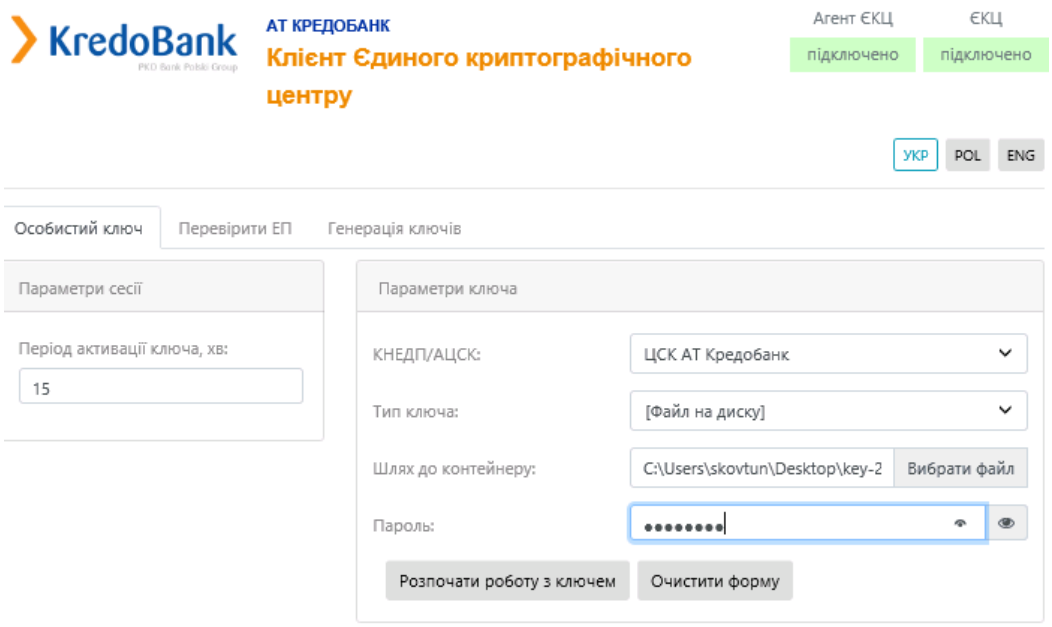

Рис. 5. Заповнення розділу «Параметри ключа»

7. Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем» та одразу створюється криптографічний контекст, де відкривається робоча область, де стають доступні всі функції та операції в Агенту ЄКЦ, Рис. 6.

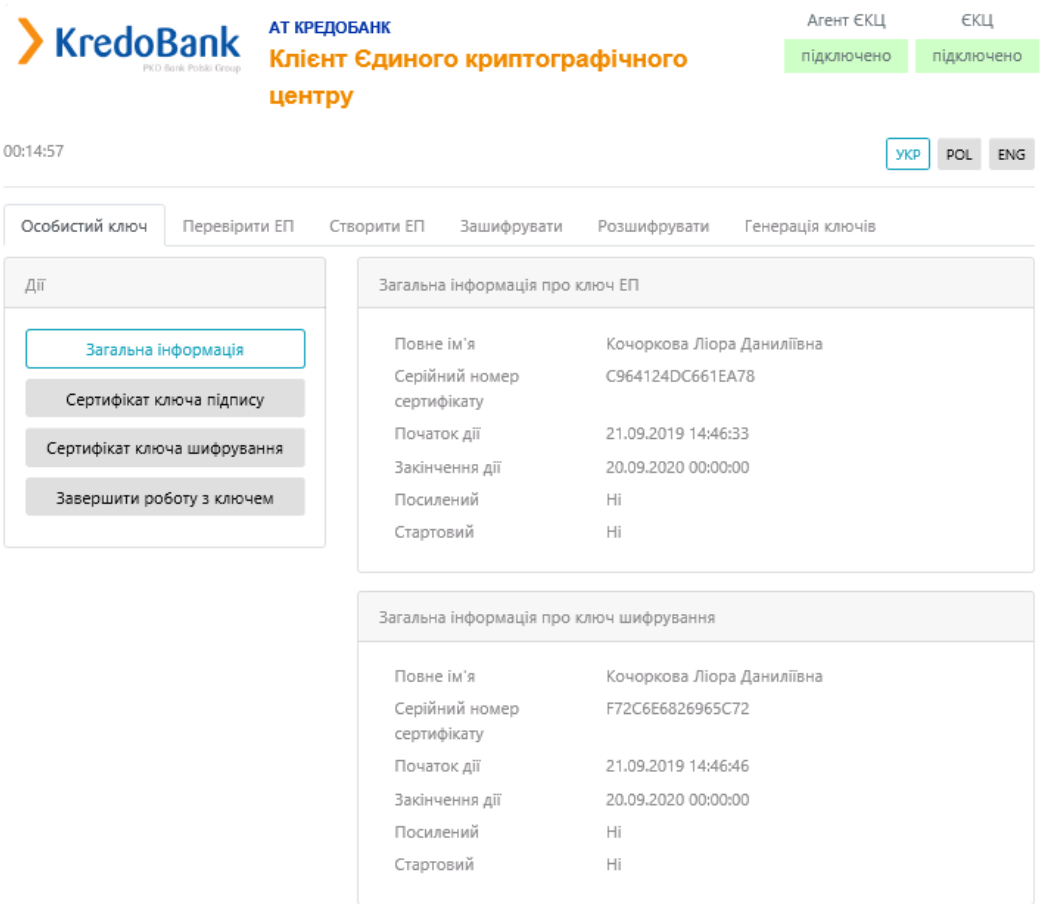

Рис. 6. Робоча область Агенту ЄКЦ

Службові функції та опції ЄКЦ

Після завантаження даних ключового контейнеру у вікні «Клієнту Єдиного Криптографічного Центру» з'являються такі поля та відповідні опції, Рис. 7:

1. Вкладка «Особистий ключ», яка містить кнопки:
   - «Загальна інформація» - коротка інформація про ключі.
   - «Сертифікат ключа ЕП» - повна інформація про сертифікат ключа ЕП. За наявності.
   - «Сертифікат ключа шифрування» - повна інформація про сертифікат ключа шифрування, за наявності.
   - «Завершити роботу з ключем» - завершується сесія.
2. Вкладка «Перевірити ЕП».

На даній вкладці є можливість здійснити перевірку ЕП, доступні такі розділи:

- «Параметри перевірки ЕП» включає в себе:
  - Можна вказати Тип ЕП (Вбудована чи Відкріплена).
  - Режим перевірки електронної позначки часу для ЕП (Ігнорувати електронну позначку часу чи перевіряти електронну позначку часу, якщо вона присутня чи повертати помилку, якщо вона відсутня).
  - Режим перевірки електронну позначки часу для даних (Ігнорувати електронну позначку часу чи перевіряти електронну позначку часу, якщо вона присутня чи повертати помилку, якщо вона відсутня).
- Розширення ЕП.
- «Файл» включає в себе 2 поля, якщо:

    - Тип ЕП - Відкріплена: файл для перевірки (файл на який було створено підпис) та файл з підписом (файл, який містить підпис).
    - Тип ЕП – Вбудована: файл з підписом (файл який містить підпис).
- «Текстові дані» включає в себе 2 поля, якщо:
    - Кодування UTF-16LE та UTF-8.
    - Тип ЕП - Відкріплена: текстові дані для перевірки (текст на який було створено підпис) та підпис у кодуванні Base64 (текст, який містить підпис).
    - Тип ЕП – Вбудована: підпис у кодуванні Base64 (текст, який містить підпис) та дані з електронного підпису (виведення даних без підпису).

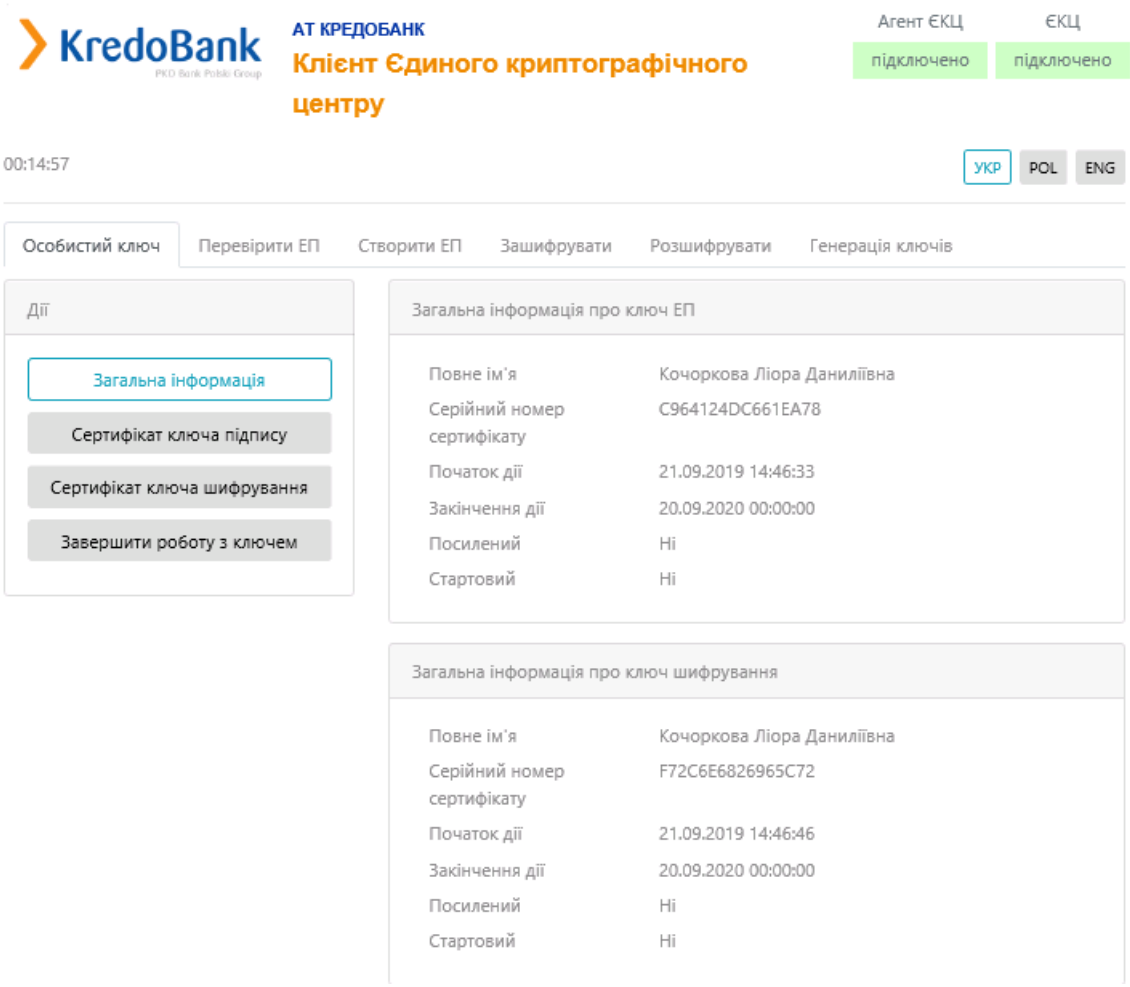

Рис. 7. Робоча область Агенту ЄКЦ

3. Вкладка «Створити ЕП».

На даній вкладці є можливість здійснити створення ЕП, доступні такі розділи:

- «Параметри створення ЕП» включає в себе:
    - Тип ЕП (Вбудована чи Відкріплена), за необхідності вказати позначку «Додати підпис до вже існуючого» (таким чином, можуть підписувати один файл кілька осіб).
    - Формат ЕП (CAdES-X Long).
- «Файл». Включає в себе 2 поля:
    - Файл/файли для підпису (файл, який необхідно підписати).
- «Текстові дані». Включає в себе поля:
    - Кодування UTF-16LE та UTF-8.

- Текстові дані для підпису (текст, який необхідно підписати).
- Додатковий опис (назва тексу підпису).
- Підпис у кодуванні Base64.

4. Вкладка «Зашифрувати».

На даній вкладці є можливість здійснити зашифрування даних, доступні такі розділи:

- «Параметри зашифрування». Слід визначитися з параметром, який слід додати при зашифруванні:
  - Сертифікат відправника та сертифікати видавців.
  - Сертифікат відправника.
  - Не додавати сертифікат відправника та сертифікати видавців.
- «Сертифікат отримувача». Поле, де слід вказати сертифікат отримувача зашифрованих даних.
- «Файл». Поле, де слід вказати файл/файли для зашифрування.
- «Текстові дані».
  - Кодування UTF-16LE та UTF-8.
  - «Текст для зашифрування». Поле, де слід вказати текст для зашифрування.
  - «Зашифровані дані у кодування Base64». Виведення зашифрованої інформації.

5. Вкладка «Розшифрувати».

На даній вкладці є можливість здійснити розшифрування даних, доступний такий розділ:

- «Файл». Слід вказати файл, який необхідно розшифрувати.
- «Текстові дані»:
  - Кодування UTF-16LE та UTF-8.
  - «Зашифровані дані у кодування Base64». Поле, де слід вказати зашифрований текст.
  - «Розшифрований текст». Виведення розшифрованої інформації.

6. Вкладка «Генерація ключів».

На даній вкладці є можливість здійснити генерацію ключів попередньо обравши відповідний профіль генерації ключів.

Профілі генерації ключів:

- Посадова особа клієнта Онлайн банкінгу.
- Клієнт Онлайн банкінгу (ФОП).

Генерація ключів відбувається як файл на диску так і на захищений носій.

7. Час до кінця сесії – відлік у реальному часі до закінчення сесії (знаходиться у лівому верхньому куті).
8. Статус роботи програмного комплексу «Агенту ЄКЦ» - знаходиться у правій верхній частині вікна. За допомогою «Агент ЄКЦ» є можливість працювати не лише із файлами на диску, але із захищеними носіями.

Можливі статуси «Агенту ЄКЦ»:

- «Запустити». Для початку роботи із «Агентом ЄКЦ», необхідно натиснути дану кнопку та для подальшої роботи слід відкрити іншу інструкцію «Агент Єдиного Криптографічного Центру. Настанова з установки та експлуатації».
- «Підключено». Працює у звичайному режимі.
- «Відключено». Слід звернутися до системного адміністратора.

9. Статус роботи програмного комплексу «ЄКЦ» - знаходиться у правій верхній частині вікна.

Можливі статуси ЄКЦ:

- «Підключено». Працює у звичайному режимі.
- «Відключено». Слід звернутися до системного адміністратора.

10. Зміна мови - знаходиться у правій верхній частині вікна можна змінити мову веб-інтерфейсу ЄКЦ. Доступні мови: українська, польська та англійська.
11. Версія Єдиного Криптографічного Центру знаходиться у правому нижньому куті.

Основна форма «Агенту Єдиного Криптографічного Центру» містить такі поля та відповідні опції, Рис. 8.

1. Даний розділ містить:
   - назву Програмного комплексу.
   - гіперпосилання «Про програму», яке відкриває нове вікно з інформацією про розробників, версію продукту, Рис. 9.
   - Випадаючий список зі зміною мови, доступні мови: Українська, Англійська, Польська.
2. Розділ «Дії» містить гіперпосилання:
   - «Перезавантажити сервіс».
   - «Очистити журнал подій».
   - «Завершити роботу сервісу».
3. Розділ «Стан» містить інформацію про стан роботи сервісу, що він працює.
4. Розділ «Журнал подій» містить повну інформацію про дії, які виконуються у веб-браузері, під час роботи з Агентом ЄКЦ.

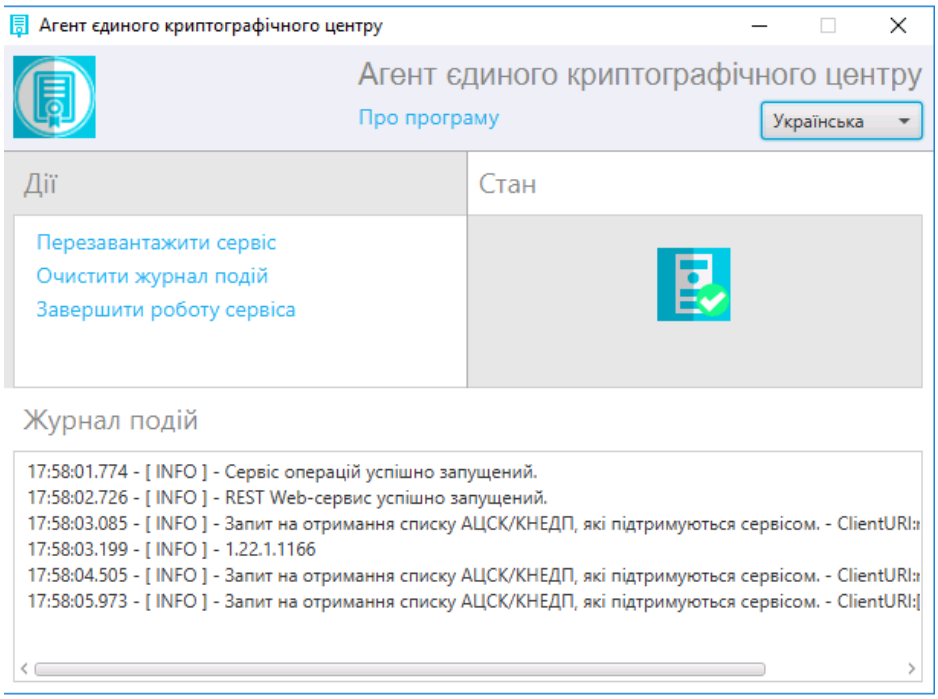

Рис. 8. Агент єдиного криптографічного центру

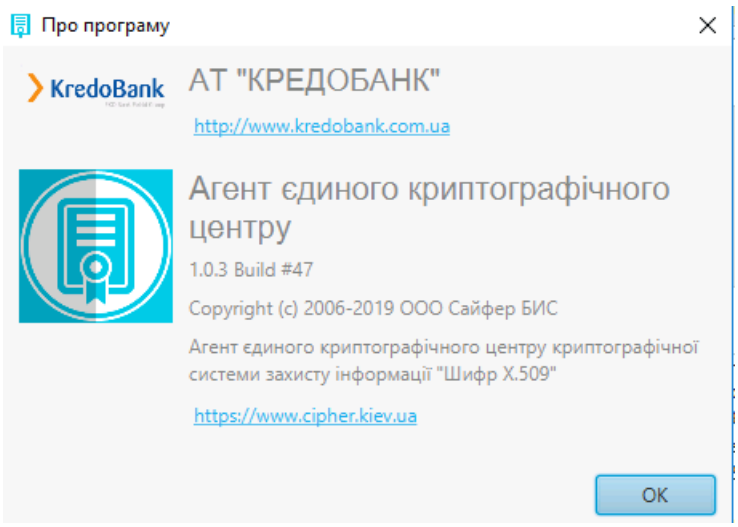

Рис. 9. Вікно «Про програму»

Вибір ключа ЕП – файл

1. Стартове вікно Клієнту Єдиного Криптографічного Центру у веб-браузері показано на Рис. 10.

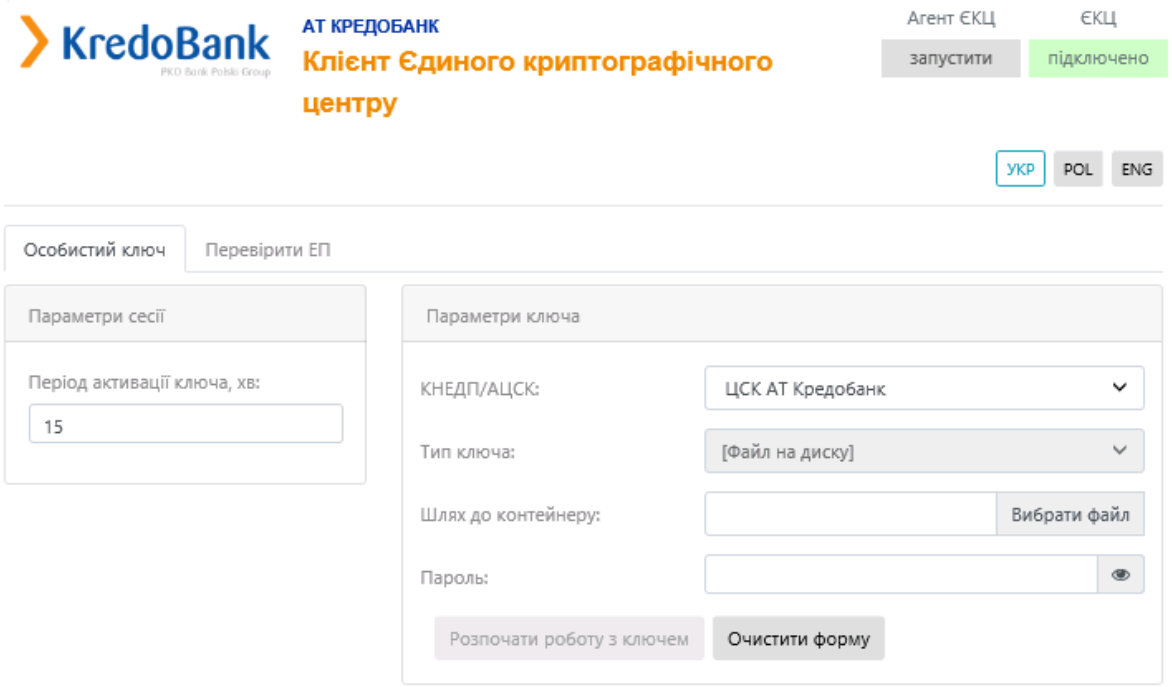

Рис. 10. Стартове вікно ЄКЦ

2. Наступним кроком слід відкрити Агент ЄКЦ, натиснувши у правому верхньому куті під написом Агент ЄКЦ кнопку «запустити», Рис. 11.

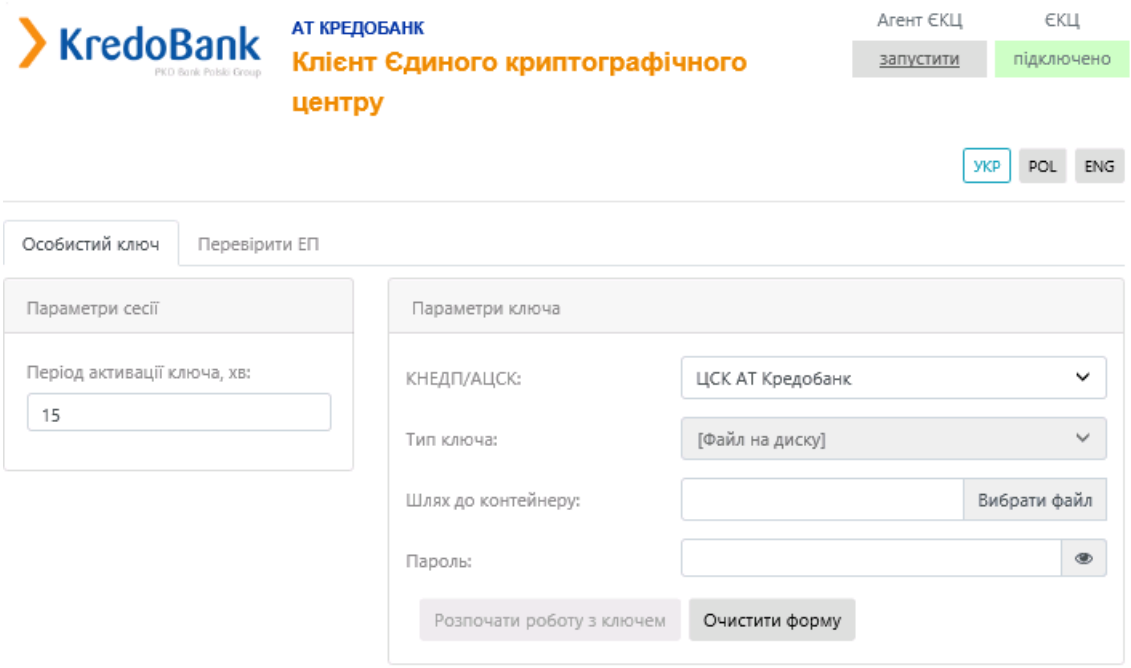

Рис. 11. Запуск Агенту ЄКЦ

3. Далі відкривається вікно Агенту Єдиного Криптографічного Центру, його слід згорнути та повернутися до веб-браузера, Рис. 12.

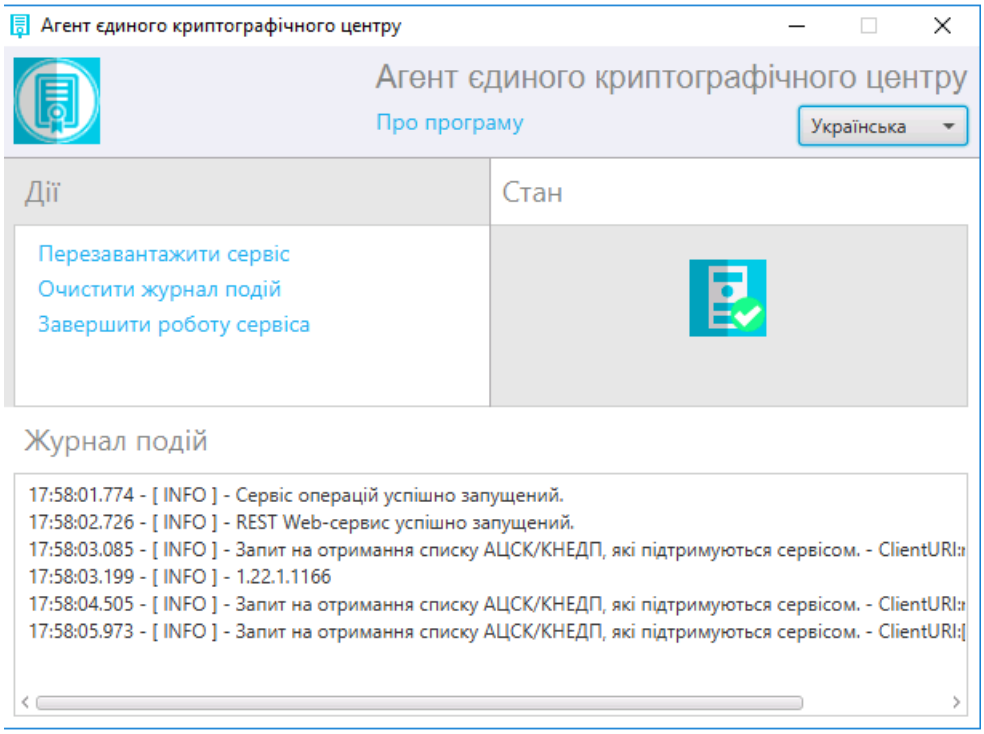

Рис. 12. Агент Єдиного Криптографічного Центру

4. У веб-сторінці одразу помітні зміни. Статус Агенту ЄКЦ змінено на «підключено» та став доступний для змін пункт «Тип ключа», Рис. 13.

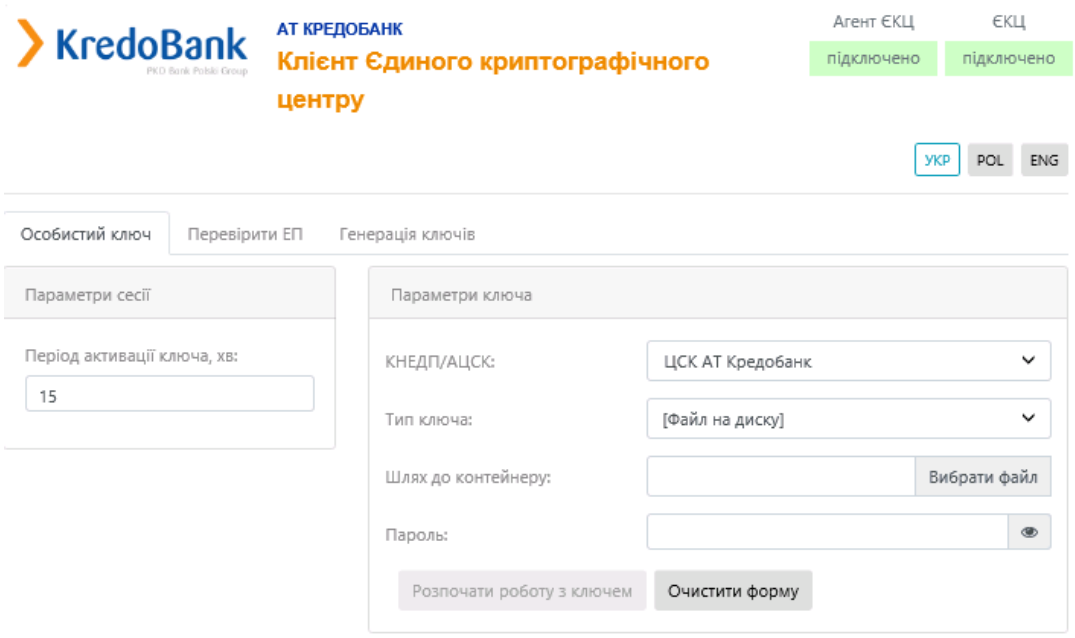

Рис. 13. Стартове вікно Агент ЄКЦ

5. На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвилинах період активації ключа, за замовчуванням 15 хв.
6. На вкладці «Особистий ключ» у розділі «Параметри ключа» слід вказати:
   1. ***КНЕДП/АЦСК***, у якому було отримано ключ;

Перелік КНЕДП/АЦСК, які підтримуються «Агентом Єдиного Криптографічного Центру»:

- ЦСК АТ Кредобанк;
- АЦСК/КНЕДП Національного банку України;
- КНЕДП ІДД ДПС;
- КНЕДП «ДІЯ»;
- АЦСК/КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
- АЦСК/КНЕДП АТ «КБ «Приватбанк»;
- АЦСК/КНЕДП ПАТ «УкрСиббанк»;
- АЦСК/КНЕДП «Masterkey» ТОВ «Арт-мастер»;
- АЦСК/КНЕДП Збройних Сил;
- АЦСК/КНЕДП Міністерства внутрішніх справ України;
- КНЕДП Державної прикордонної служби;
- АЦСК/КНЕДП Укрзалізниці;
- КНЕДП «АЦСК ринку електричної енергії»;
- АЦСК/КНЕДП ПАТ «Національний депозитарій України»;
- АЦСК/КНЕДП ТОВ «Ключові системи»;
- КНЕДП ДП «Українські спеціальні системи»;
- АЦСК/КНЕДП Генеральної прокуратури України;
- АЦСК/КНЕДП АТ «Ощадбанк»;
- КНЕДП Казначейства (з ключами, які отримано після 31.01.2020);
- КНЕДП ТОВ «Депозит Сайн».

2. ***Тип ключа***:
   - файл на диску (обрати даний пункт з випадаючого списку);
   - PKCS#11 пристрої – активний режим;
   - PKCS#11 пристрої – пасивний режим.
3. ***Шлях до контейнеру***;
4. ***Пароль*** до ключа, Рис. 14.

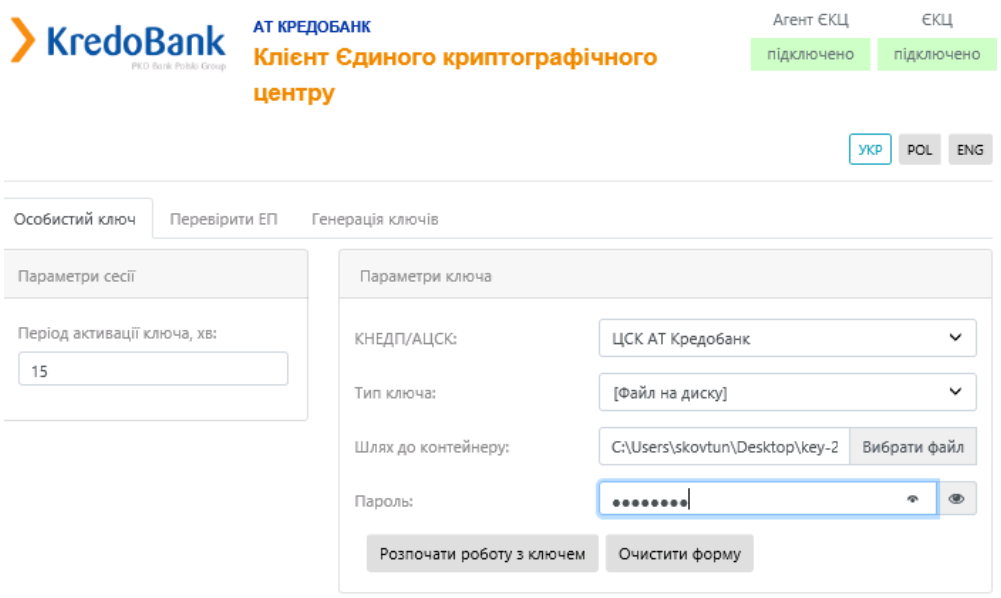

Рис. 14. Заповнення розділу «Параметри ключа»

7. Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем» та одразу створюється криптографічний контекст, де відкривається робоча область, де стають доступні всі функції та операції в Агенту ЄКЦ, Рис. 15.

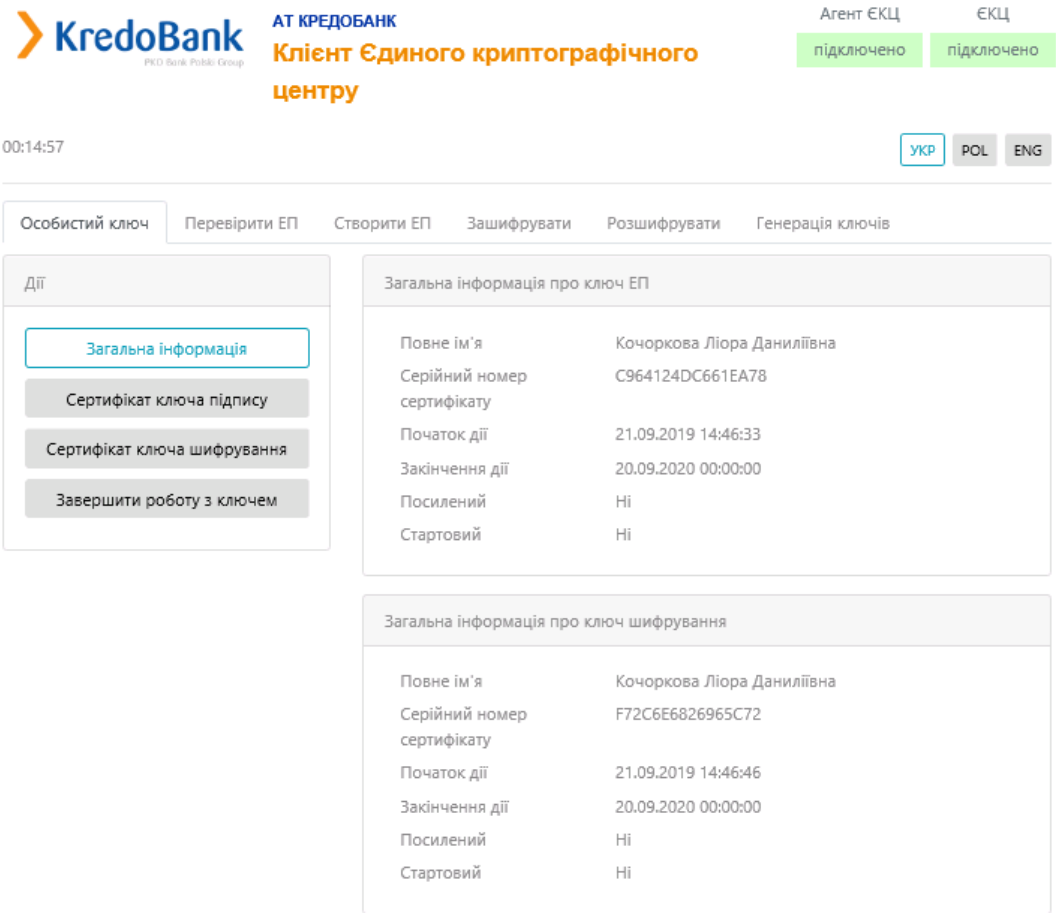

Рис. 15. Робоча область Агенту ЄКЦ

Вибір ключа ЕП – захищений носій

1. Стартове вікно Клієнта Єдиного Криптографічного Центру у веб-браузері показано на Рис. 16.

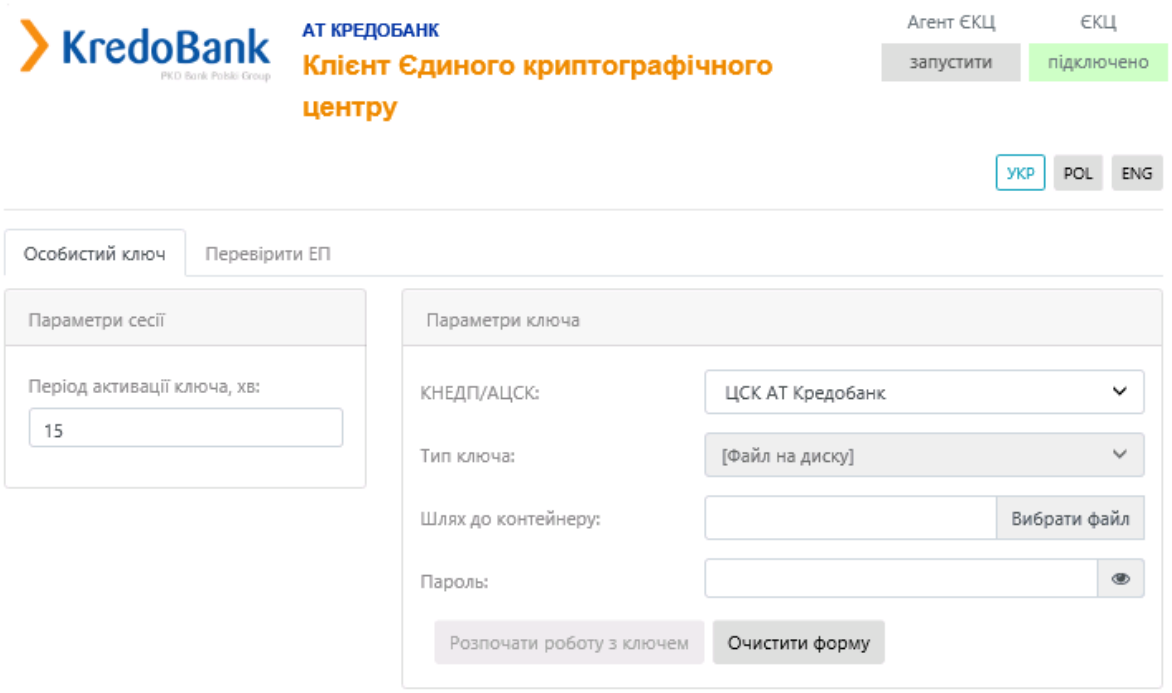

Рис. 16. Стартове вікно ЄКЦ

2. Наступним кроком слід відкрити Агент ЄКЦ, натиснувши у правому верхньому куті під написом Агент ЄКЦ кнопку «запустити», Рис. 17.

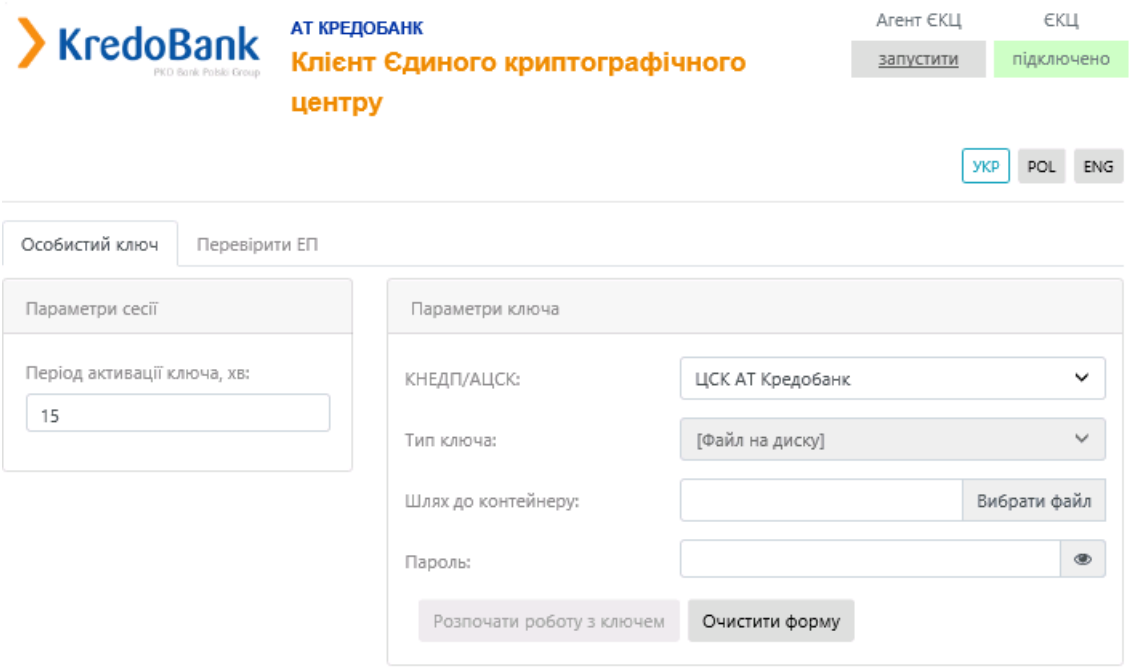

Рис. 17. Запуск Агенту ЄКЦ

3. Далі відкривається вікно Агенту Єдиного Криптографічного Центру, його слід згорнути та повернутися до веб-браузера, Рис. 18.

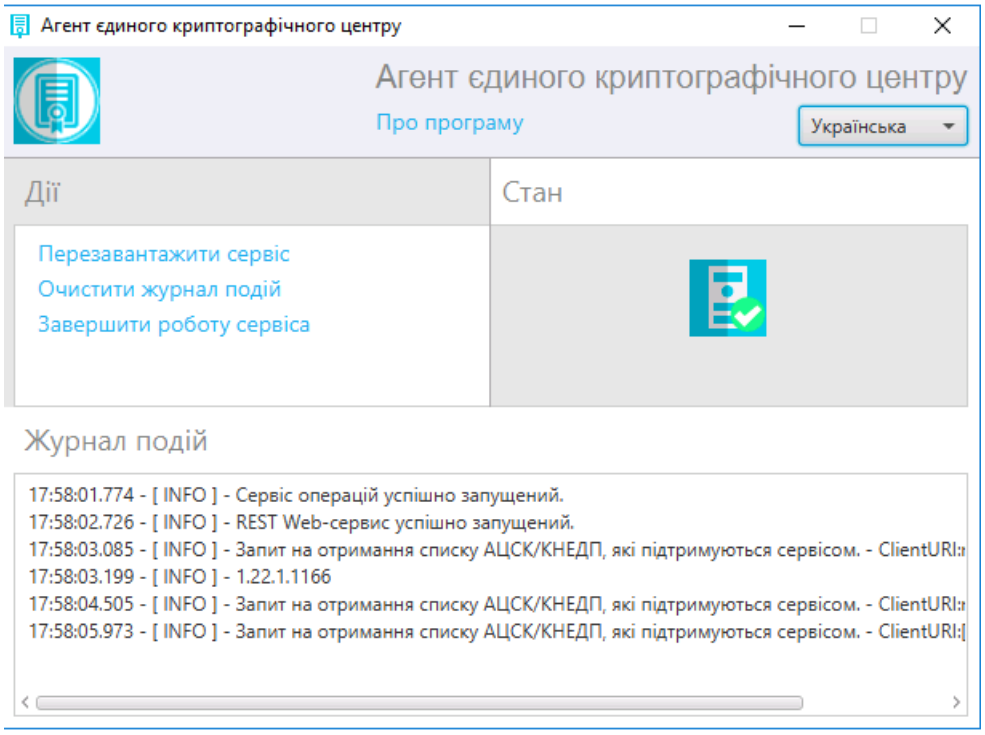

Рис. 18. Агент Єдиного Криптографічного Центру

4. У веб-сторінці одразу помітні зміни. Статус Агенту ЄКЦ змінено на «підключено» та став доступний для змін пункт «Тип ключа», Рис. 19.

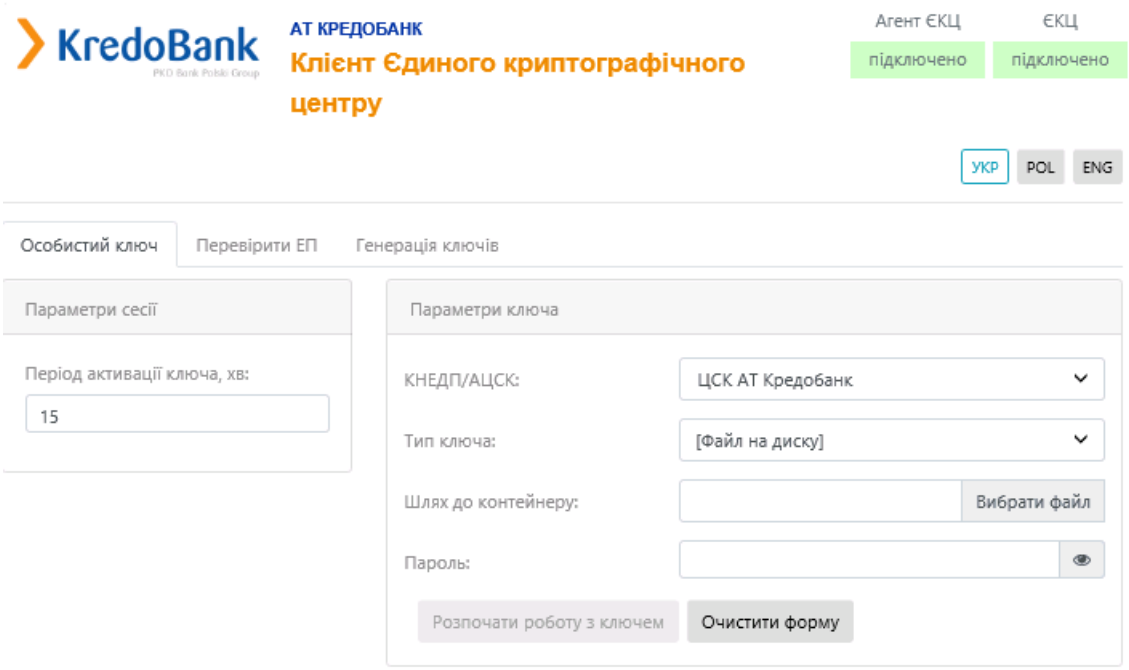

Рис. 19. Стартове вікно Агент ЄКЦ

5. На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвилинах період активації ключа, за замовчуванням 15 хв.

6. На вкладці «Особистий ключ» у розділі «Параметри ключа» слід вказати:
   1. ***КНЕДП/АЦСК***, у якому було отримано ключ;

Перелік КНЕДП/АЦСК, які підтримуються «Агентом Єдиного Криптографічного Центру»:

- ЦСК АТ Кредобанк;
- АЦСК/КНЕДП Національного банку України;
- КНЕДП ІДД ДПС;
- КНЕДП «ДІЯ»;
- АЦСК/КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
- АЦСК/КНЕДП АТ «КБ «Приватбанк»;
- АЦСК/КНЕДП ПАТ «УкрСиббанк»;
- АЦСК/КНЕДП «Masterkey» ТОВ «Арт-мастер»;
- АЦСК/КНЕДП Збройних Сил;
- АЦСК/КНЕДП Міністерства внутрішніх справ України;
- КНЕДП Державної прикордонної служби;
- АЦСК/КНЕДП Укрзалізниці;
- КНЕДП «АЦСК ринку електричної енергії»;
- АЦСК/КНЕДП ПАТ «Національний депозитарій України»;
- АЦСК/КНЕДП ТОВ «Ключові системи»;
- КНЕДП ДП «Українські спеціальні системи»;
- АЦСК/КНЕДП Генеральної прокуратури України;
- АЦСК/КНЕДП АТ «Ощадбанк»;
- КНЕДП Казначейства (з ключами, які отримано після 31.01.2020);
- КНЕДП ТОВ «Депозит Сайн».

2. ***Тип ключа*** (обрати один з режимів, активний чи пасивний):
   - Файл на диску;
   - PKCS#11 пристрої – активний режим;
   - PKCS#11 пристрої – пасивний режим.
3. **Шлях до контейнеру**, Рис. 20;

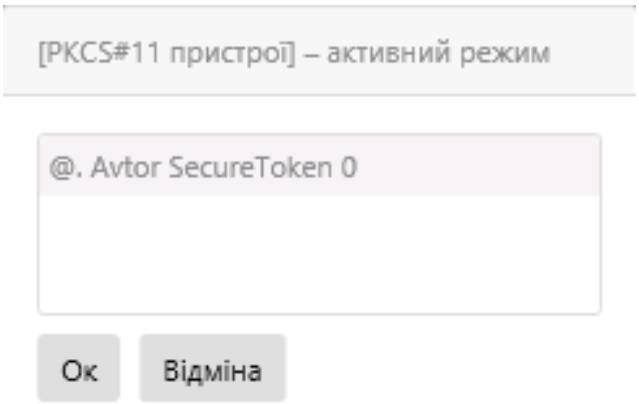

Рис. 20. Вказівка «Шлях до контейнера»

4. ***PIN*** до захищеного носія, Рис. 21.

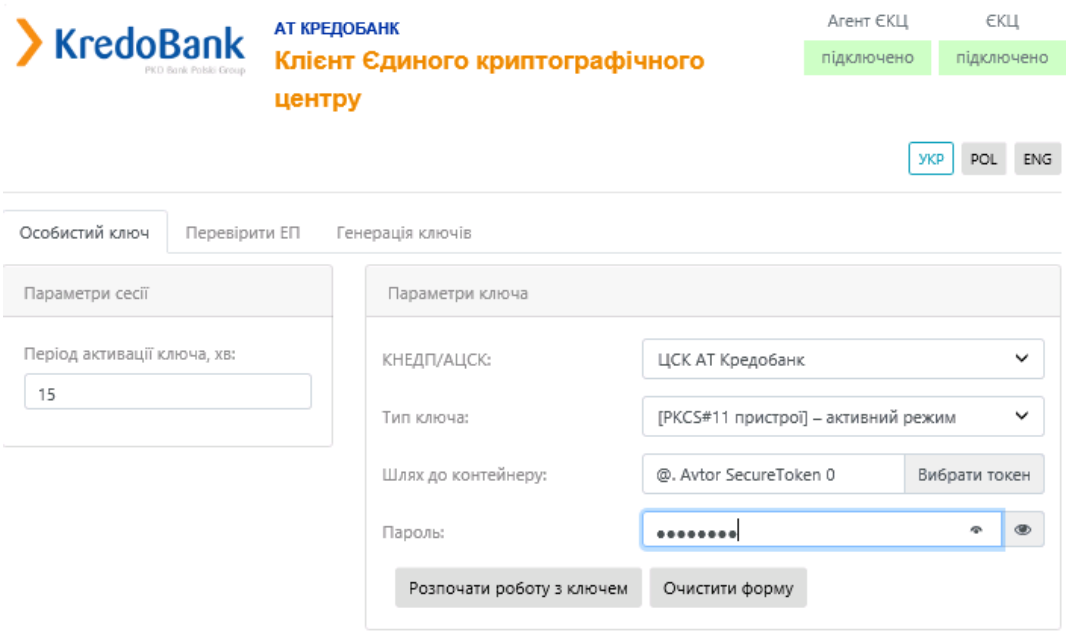

Рис. 21. Форма «Агент ЄКЦ»

7. Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем» та одразу з’являється повідомлення з інформацією, що дані ключового контейнеру успішно завантажені, Рис. 22.

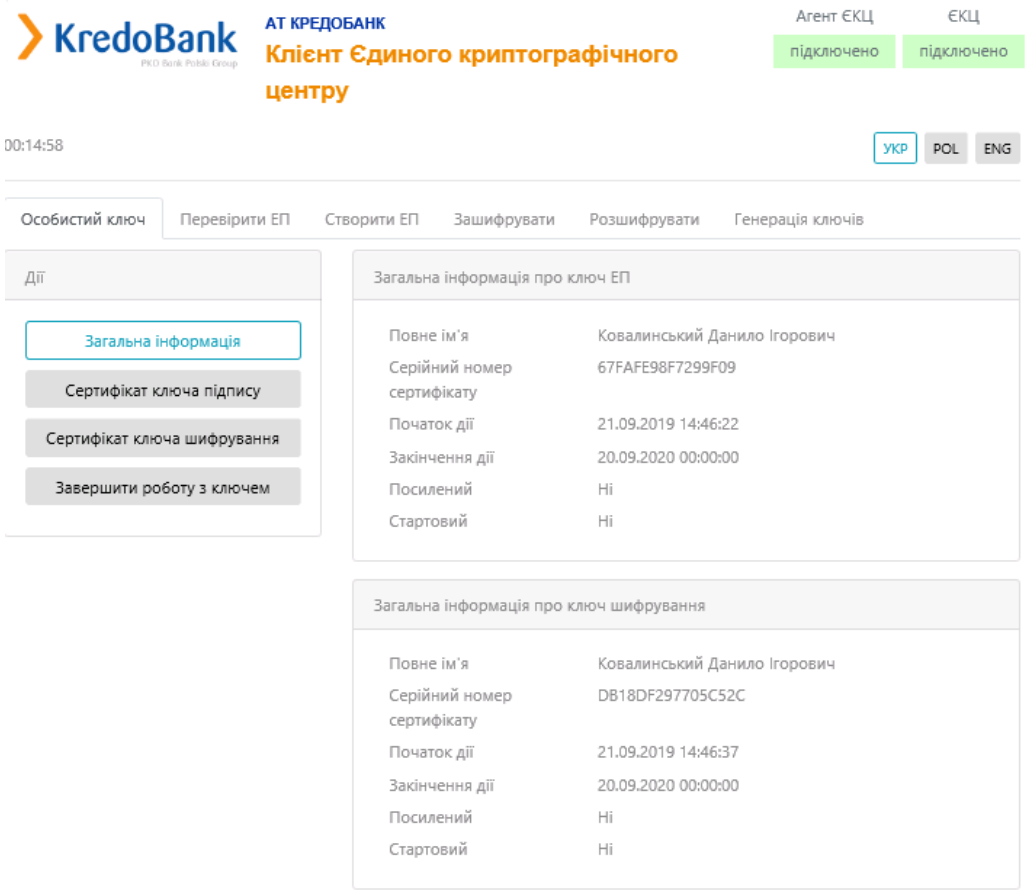

Рис. 22. Робоча область Агенту ЄКЦ

Створення ЕП

Вкладка «Створити ЕП» містить розділи: Параметри створення ЕП, Текстові дані та Файл, Рис. 23.

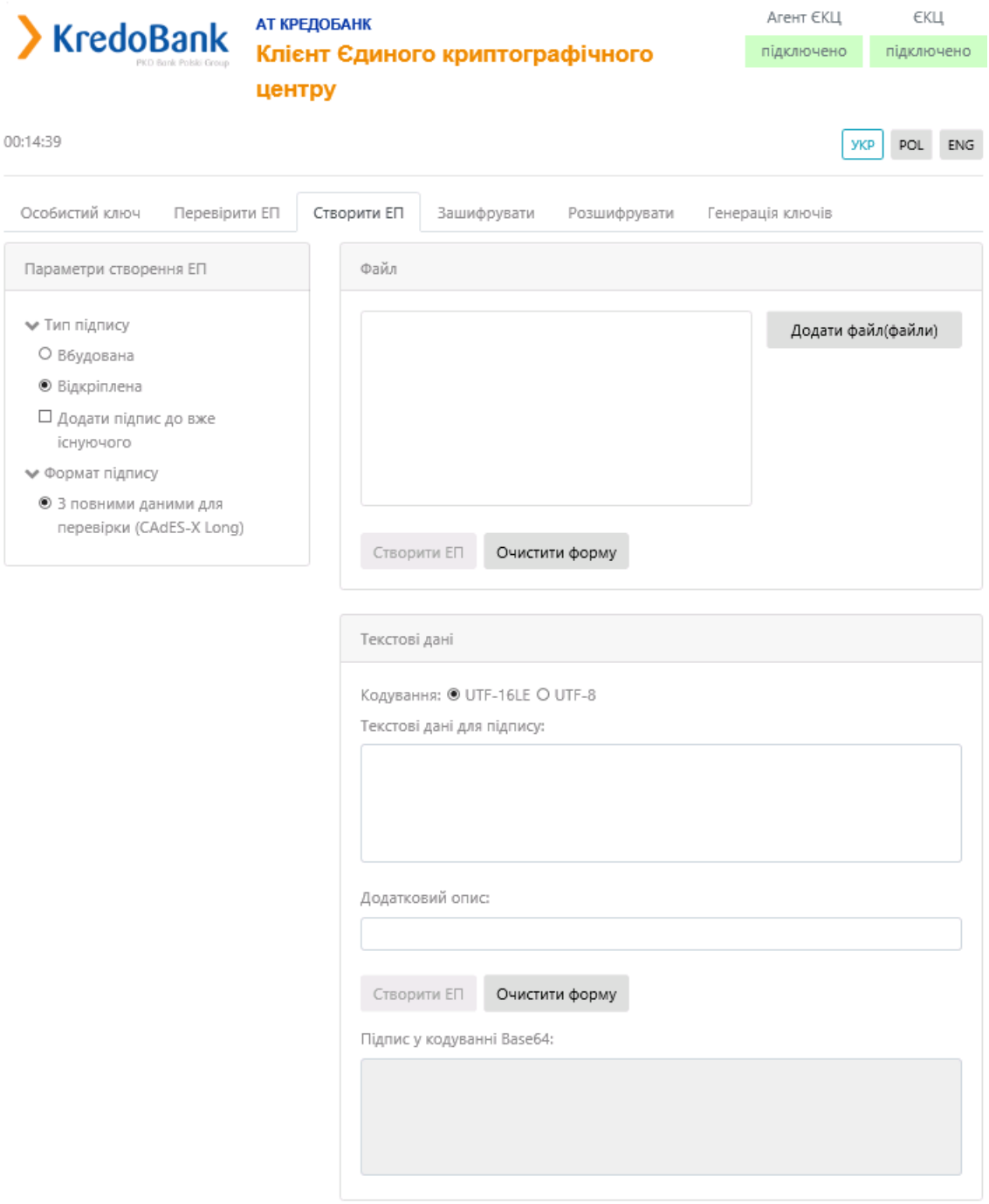

Рис. 23. Вкладка «Створити ЕП»

Розділ «Параметри створення ЕП», який у свою чергу включає:

1. Поле «Тип ЕП», яке містить:
   - Вбудована;
   - Відкріплена;

- Додати підпис до вже існуючого (накладається підпис на файл, на який вже попередньо накладено ЕП).

2. Поле «Формат ЕП», яке містить:
   - CAdES-X Long. Або «ЕП з повним набором даних перевірки» можливість встановлення дійсності ЕП у довгостроковому періоді (після закінчення строку чинності сертифікату).

Розділ «Файл», який у свою чергу включає:

- Файл для підпису (натискаємо кнопку «Вибрати файл» та обираємо необхідний файл для підпису);
- Кнопка «Створити ЕП» (здійснює накладання ЕП на файл/файли, який завантажено);
- Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Розділ «Текстові дані», який у свою чергу включає:

- Кодування UTF-16LE та UTF-8.
- Текстові дані для підпису (у поле слід внести текстові дані);
- Додатковий опис (опис до текстових даних);
- Кнопка «Створити ЕП» (здійснює накладання ЕП на текстові дані, який завантажено);
- Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.
- Підпис у кодування Base64 (виведення підписаних текстових даних).

Створення ЕП за типом «Вбудована» на файл

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Вбудована» та Формат ЕП (CAdES-X Long), обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 24. За необхідності можна видалити файл натиснувши відповідну кнопку та додати ще, але слід зауважити, що максимальний об'єм всіх файлів не повинен перевищувати 100Мб.

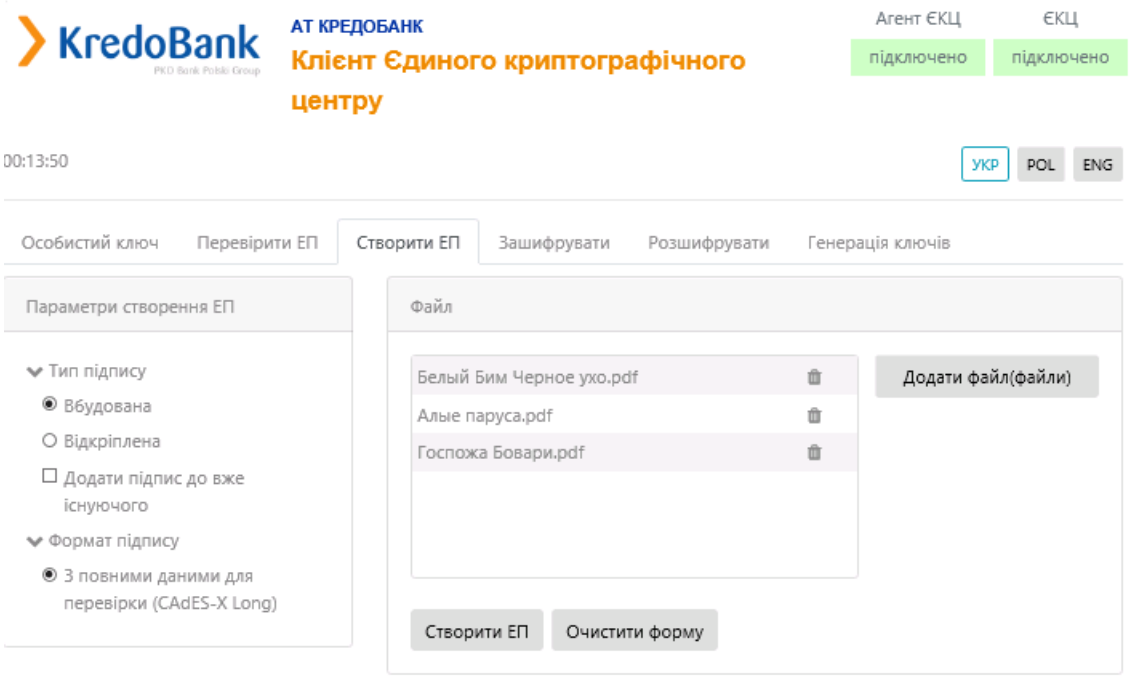

Рис. 24. Створення ЕП

Після натискання на кнопку «Створити ЕП» з'являється вікно із запитом дозволу на використання ЕП, для кожного файлу, який було додано для накладення підпису, щоб дати дозвіл необхідно натиснути «ОК», Рис. 25. Якщо натиснути кнопку «Відміна», підпис не буде створено та операція буде завершена.

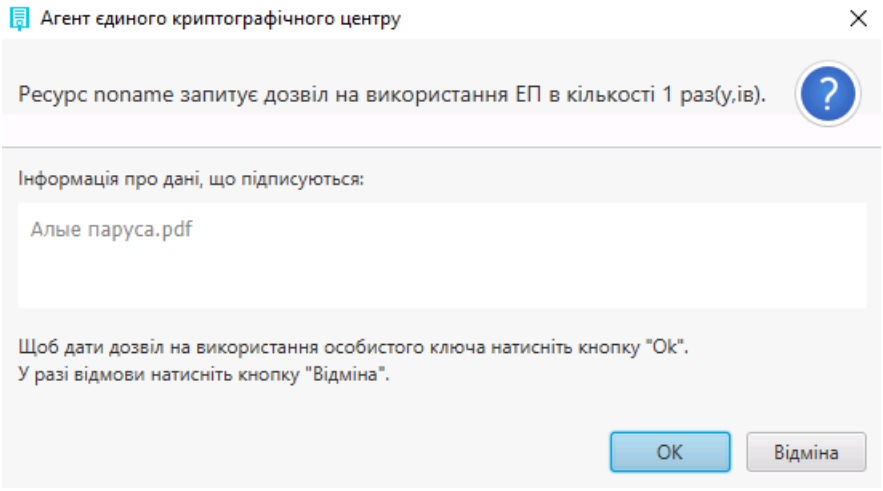

Рис. 25. Дозвіл на використання ЕП

Після натискання кнопки «ОК» з'являється вікно про успішне створення електронного підпису, Рис. 26.

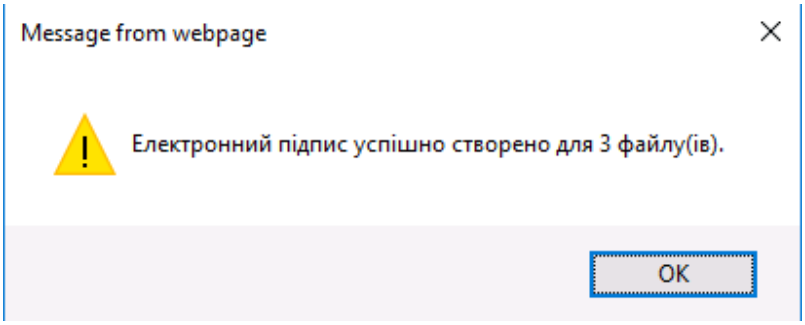

Рис. 26. Повідомлення про створення електронного підпису

Далі зберігається файл з підписом за допомогою кнопки «стрілки вниз», яка з'являється біля кожного файлу на який накладено підпис, Рис. 27.

За необхідності вказуємо шлях для збереження та очищаємо форму.

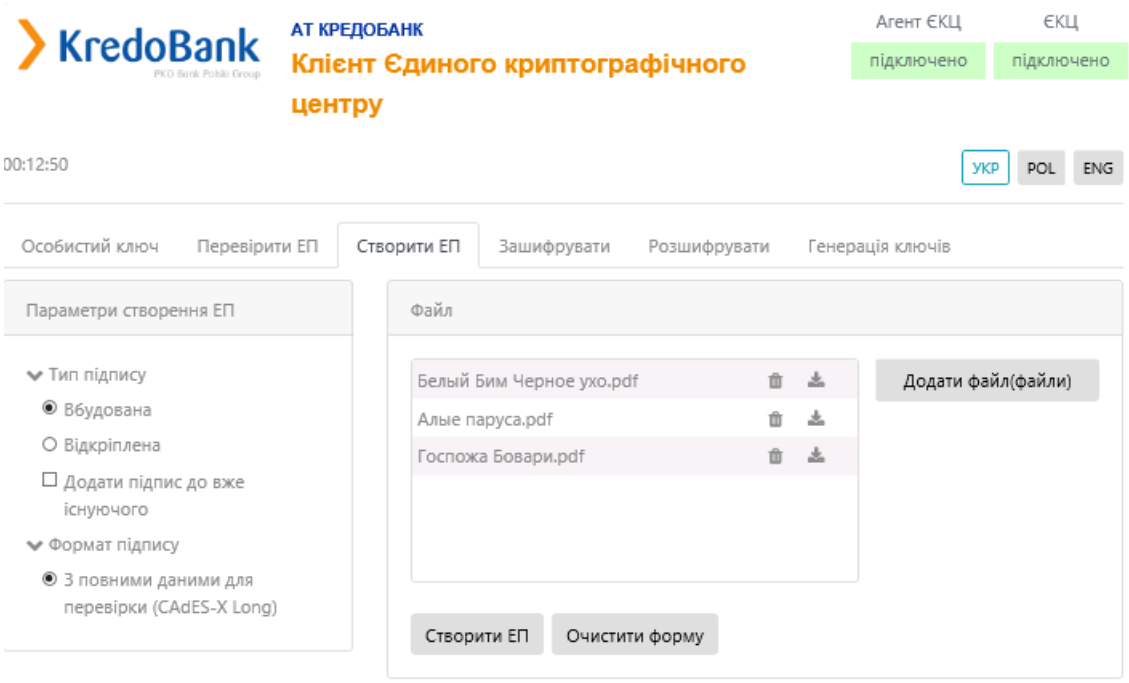

Рис. 27. Збереження підпису у файл

Рис. 28. Збереження файлу

Створення ЕП за типом «Відкріплена» на файл

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Відкріплена» та Формат ЕП (CAdES-BES чи CAdES-X Long), обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 29. За необхідності можна видалити файл натиснувши відповідну кнопку та додати ще, але слід зауважити, що максимальний об'єм всіх файлів не повинен перевищувати 100Мб.

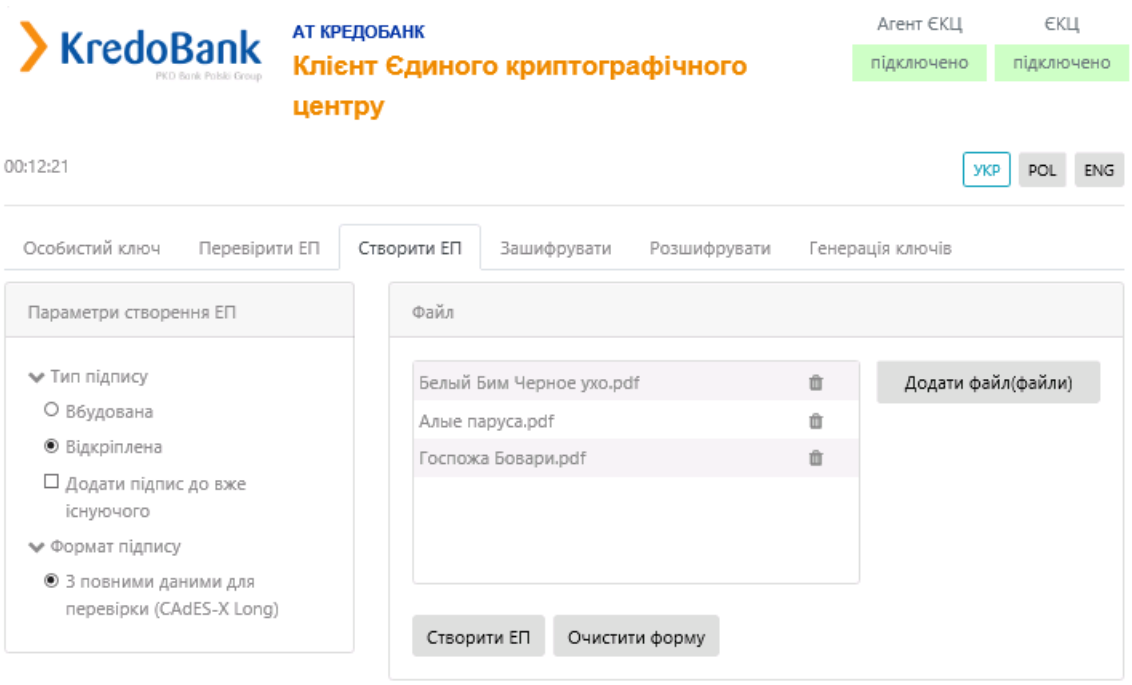

Рис. 29. Створення ЕП

Після натискання на кнопку «Створити ЕП» з'являється вікно із запитом дозволу на використання ЕП, для кожного файлу, який було додано для накладення підпису, Рис. 30, щоб дати дозвіл необхідно натиснути кнопку «Відміна», підпис не буде створено та операція буде завершена.

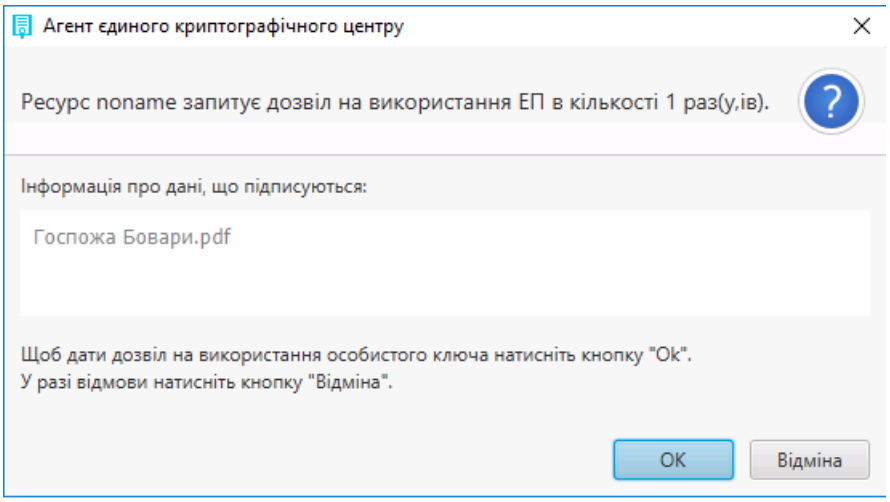

Рис. 30. Дозвіл на використання ЕП

Після натискання кнопки «ОК» з'являється вікно про успішне створення електронного підпису, Рис. 31.

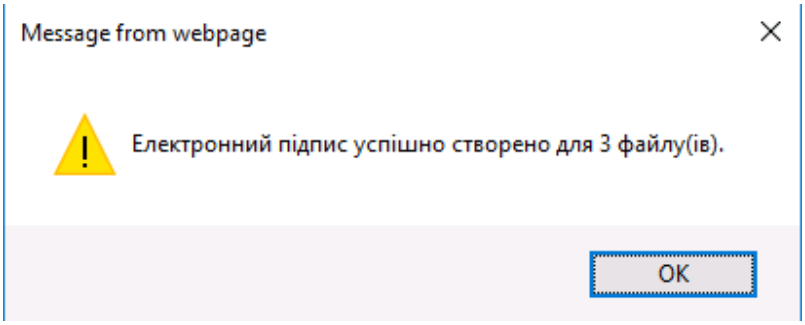

Рис. 31. Повідомлення про створення електронного підпису

Далі зберігається файл з підписом за допомогою кнопки «стрілки вниз», яка з'являється біля кожного файлу на який накладено підпис, Рис. 32.

За необхідності вказуємо шлях для збереження (Рис. 33) та очищаємо форму.

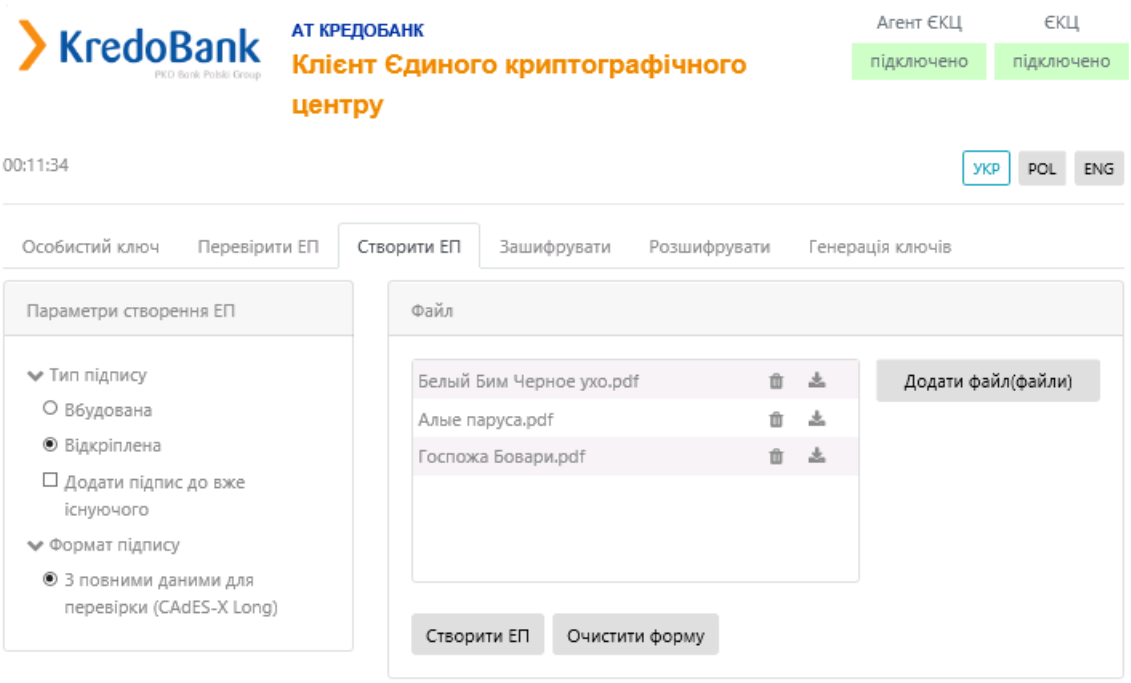

Рис. 32. Збереження підпису у файл

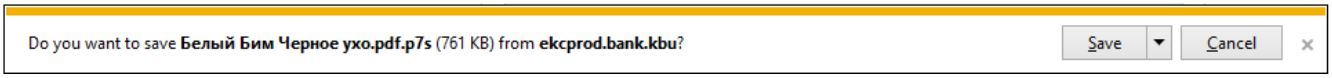

Рис. 33. Збереження файлу

Створення ЕП за типом «Вбудована» на текстові дані

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Вбудована» та Формат ЕП (CAdES-X Long), тип кодування, вказується текст для підпису, натискаємо кнопку «Створити ЕП», Рис. 34.

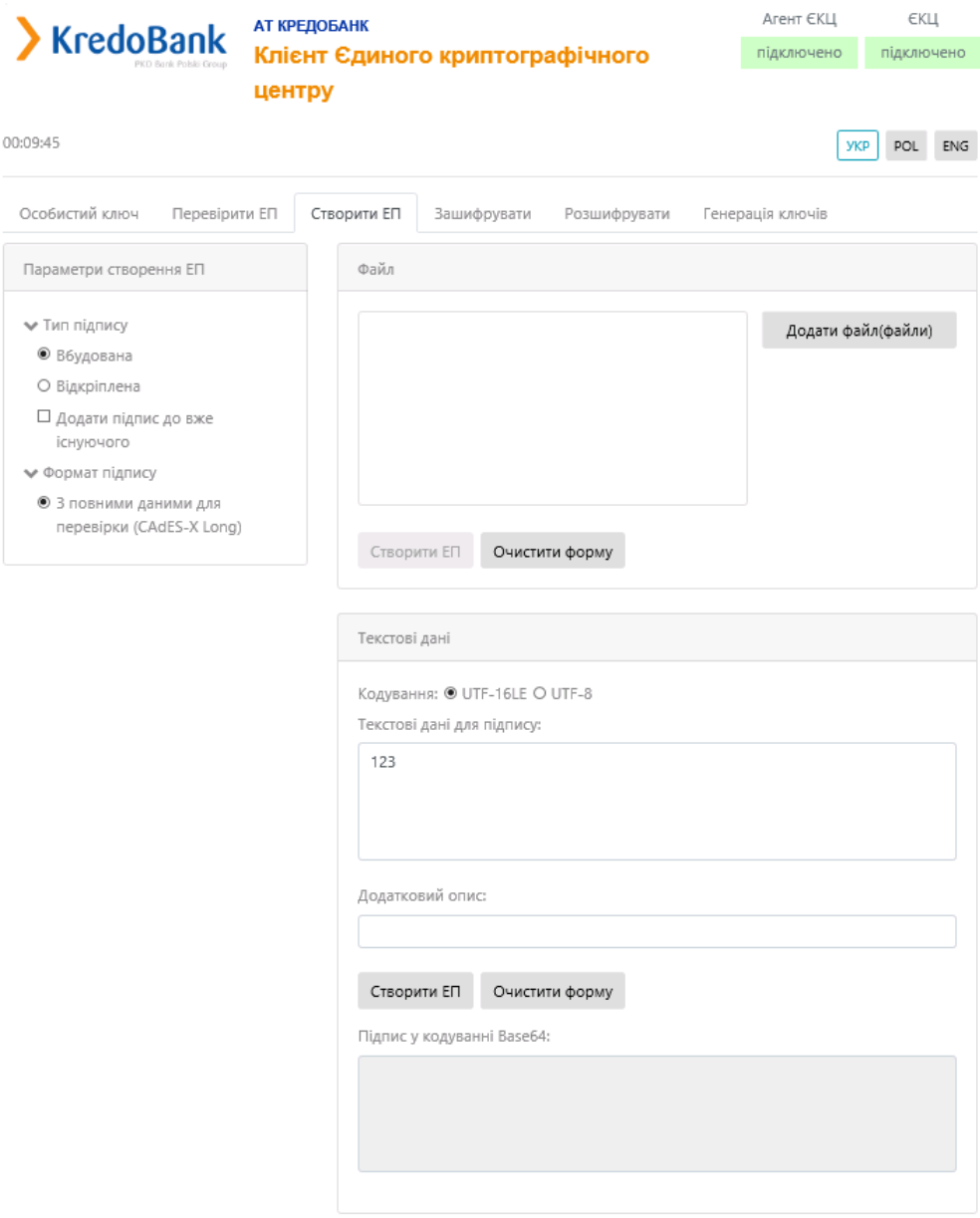

Рис. 34. Створення ЕП

Після натискання на кнопку «Створити ЕП» з'являється вікно із запитом дозволу на використання ЕП, для кожного файлу, який було додано для накладення підпису, щоб дати дозвіл необхідно натиснути кнопку «Відміна», підпис не буде створено та операція буде завершена, Рис. 35.

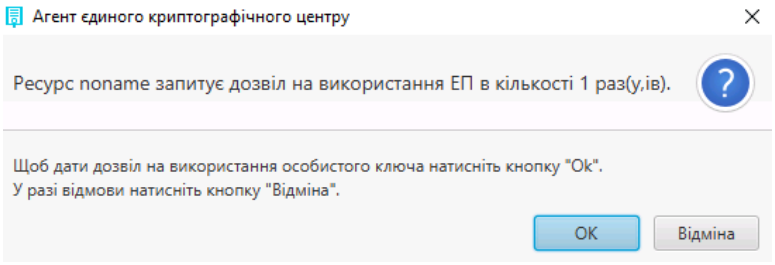

Рис. 35. Дозвіл на використання ЕП

Після натискання кнопки «ОК» з’являється вікно про успішне створення електронного підпису, Рис. 36.

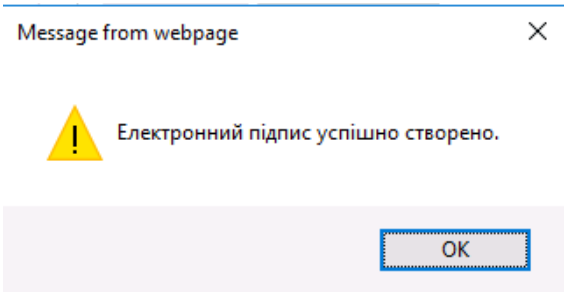

Рис. 36. Повідомлення про створення електронного підпису

Далі у полі «Підпис у кодуванні Base64» з’являється текст з підписом, Рис. 37, далі за необхідності очищаємо форму.

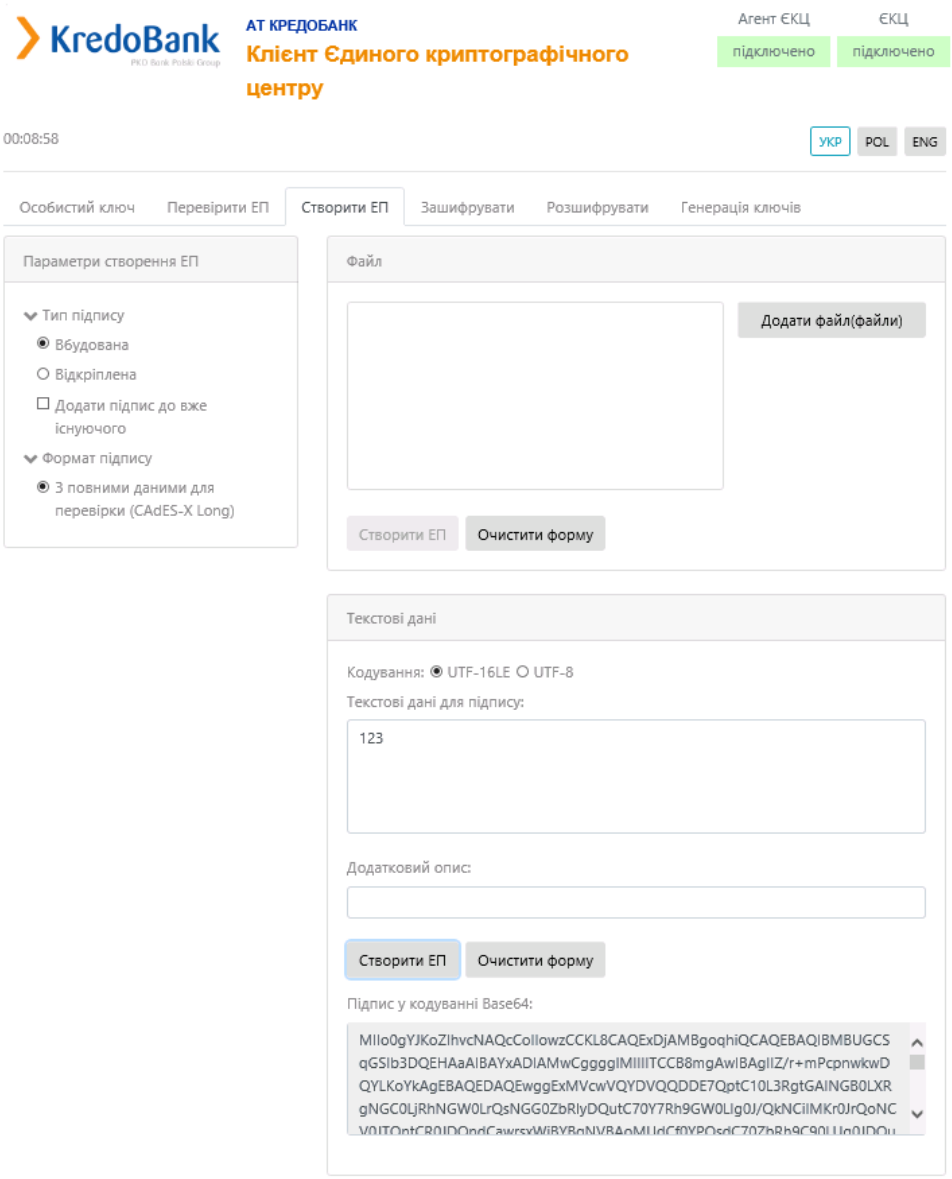

Рис. 37. Результат підпису тестових даних

Створення ЕП за типом «Відкріплена» на текстові дані

Відеоінструкція знаходиться [за посиланням](#).

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Відкріплена» та Формат ЕП (CAdES-X Long), обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 38.

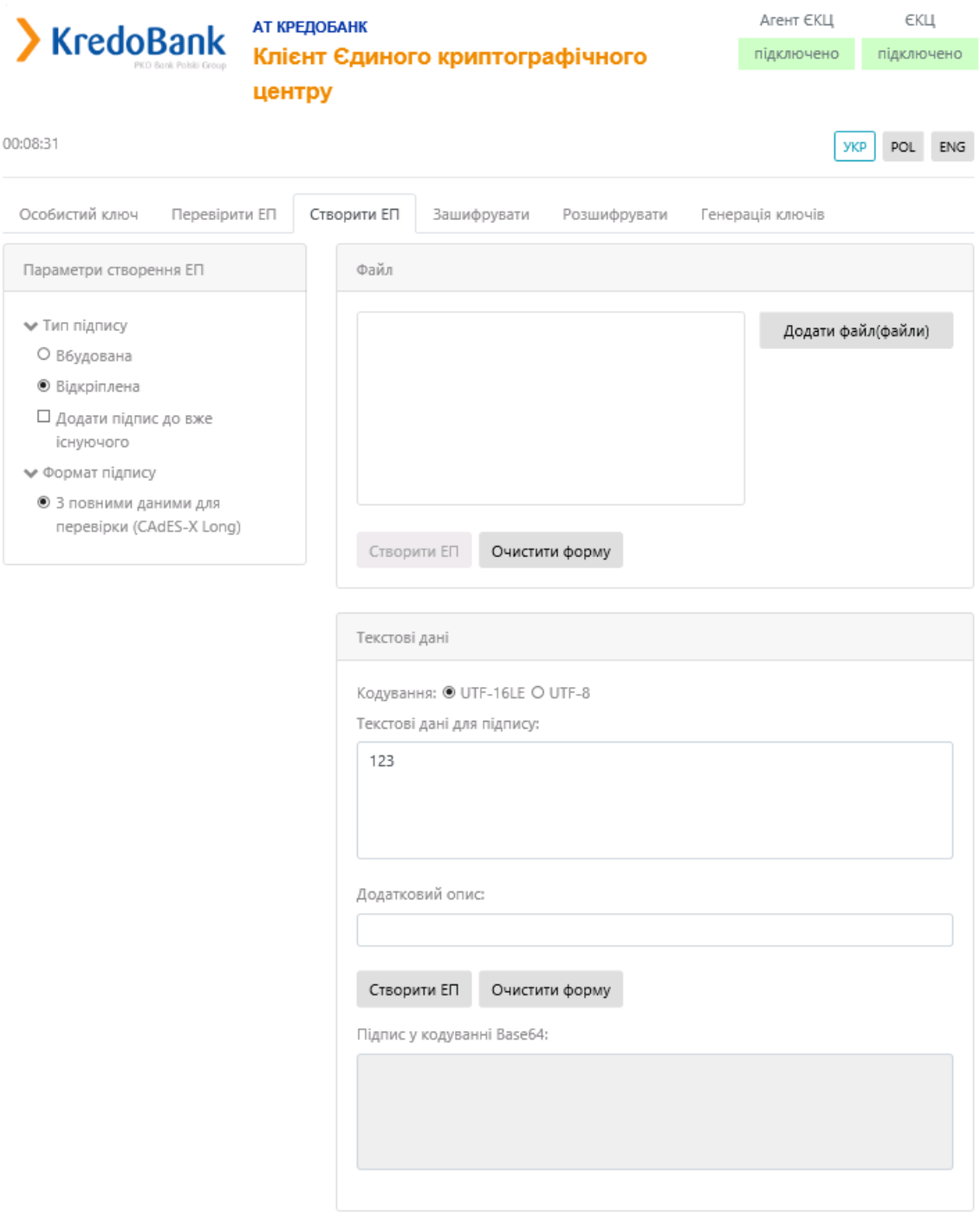

Рис. 38. Створення ЕП

Після натискання на кнопку «Створити ЕП» з’являється вікно із запитом дозволу на використання ЕП, для кожного файлу, який було додано для накладення підпису, щоб дати дозвіл необхідно натиснути кнопку «Відміна», підпис не буде створено та операція буде завершена, Рис. 39.

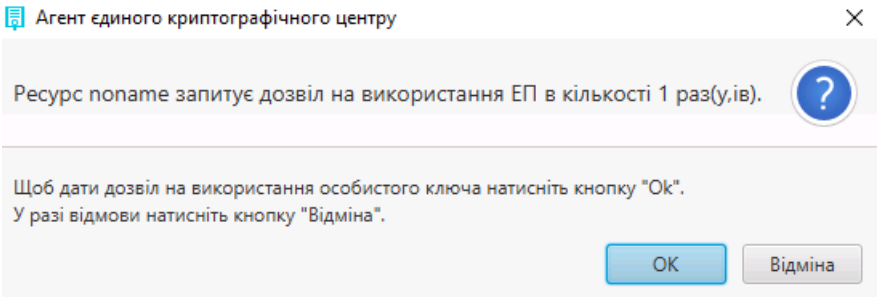

Рис. 39. Дозвіл на використання ЕП

Після натискання кнопки «ОК» з’являється вікно про успішне створення електронного підпису, Рис. 40.

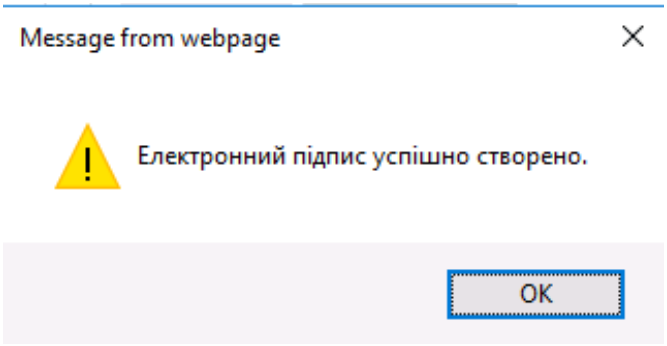

Рис. 40. Повідомлення про створення електронного підпису

Далі у полі «Підпис у кодуванні Base64» з’являється текст з підписом, Рис. 41. Далі за необхідності очищаємо форму.

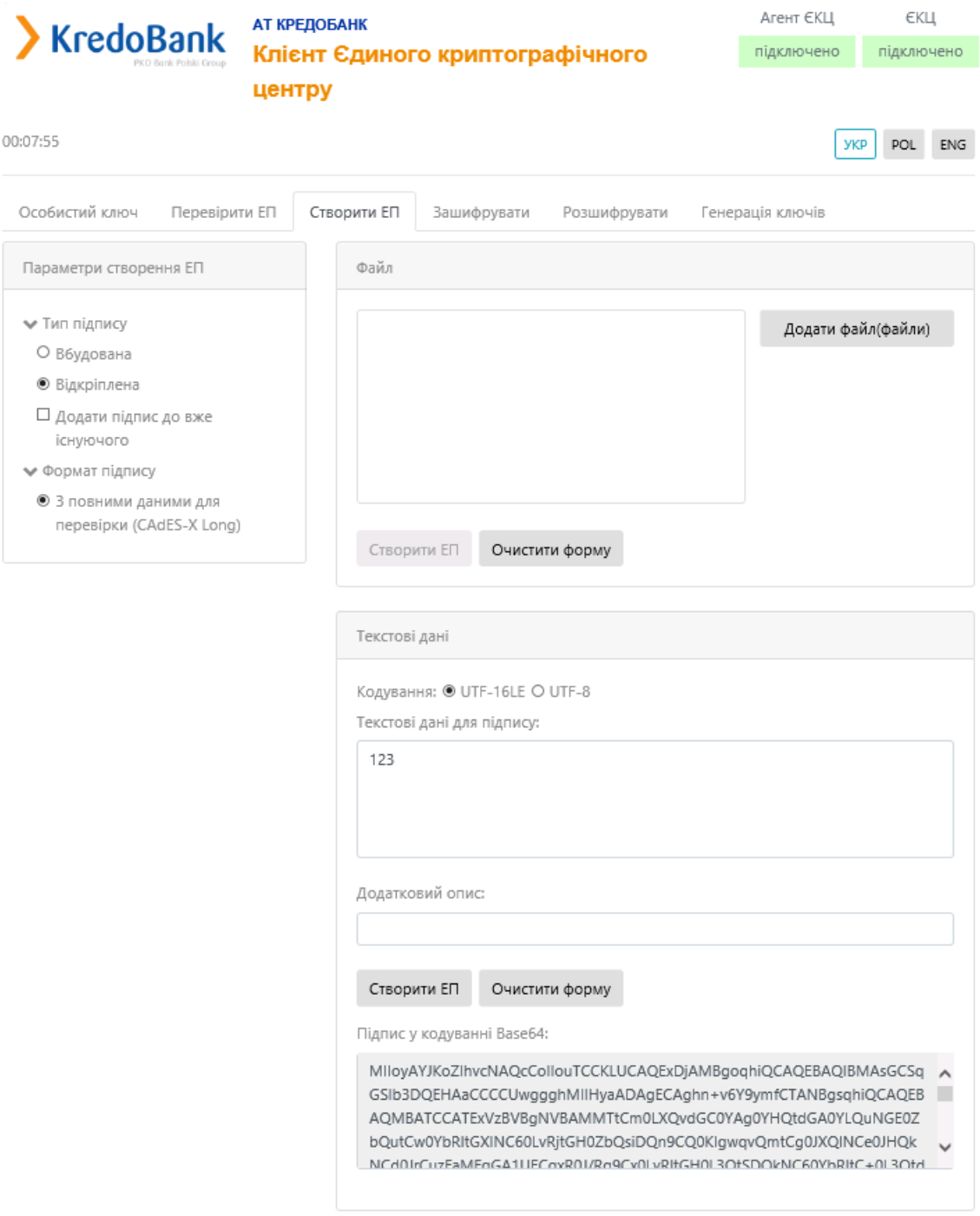

Рис. 41. Результат підпису тестових даних

Перевірка ЕП

Дана функція є доступною і без ключа.

Вкладка «Перевірити ЕП» містить розділи: Параметри перевірки ЕП, Текстові дані та Файл, Рис. 42-Рис. 43.

Розділ «Параметри перевірки ЕП», який у свою чергу включає:

1. Поле «Тип ЕП», яке містить:
   - Вбудована;
   - Відкріплена;
2. Режим перевірки електронної позначки часу для ЕП, який вказується за необхідності ігнорувати, перевіряти її наявність, чи повертати помилку за її відсутності.
3. Режим перевірки електронної позначки часу для даних, який вказується за необхідності ігнорувати, перевіряти її наявність, чи повертати помилку за її відсутності.
4. Позначка «Розширити ЕП».

Розділ «Файл», який у свою чергу включає:

Якщо перевіряється файл за типом ЕП – **Вбудована**.

1. Поле «Файл з підписом» (обирається файл, який містить підпис за типом ЕП Вбудована).
2. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
3. Кнопка «Зберегти підписані дані» (дозволяє зберегти дані без підпису);
4. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

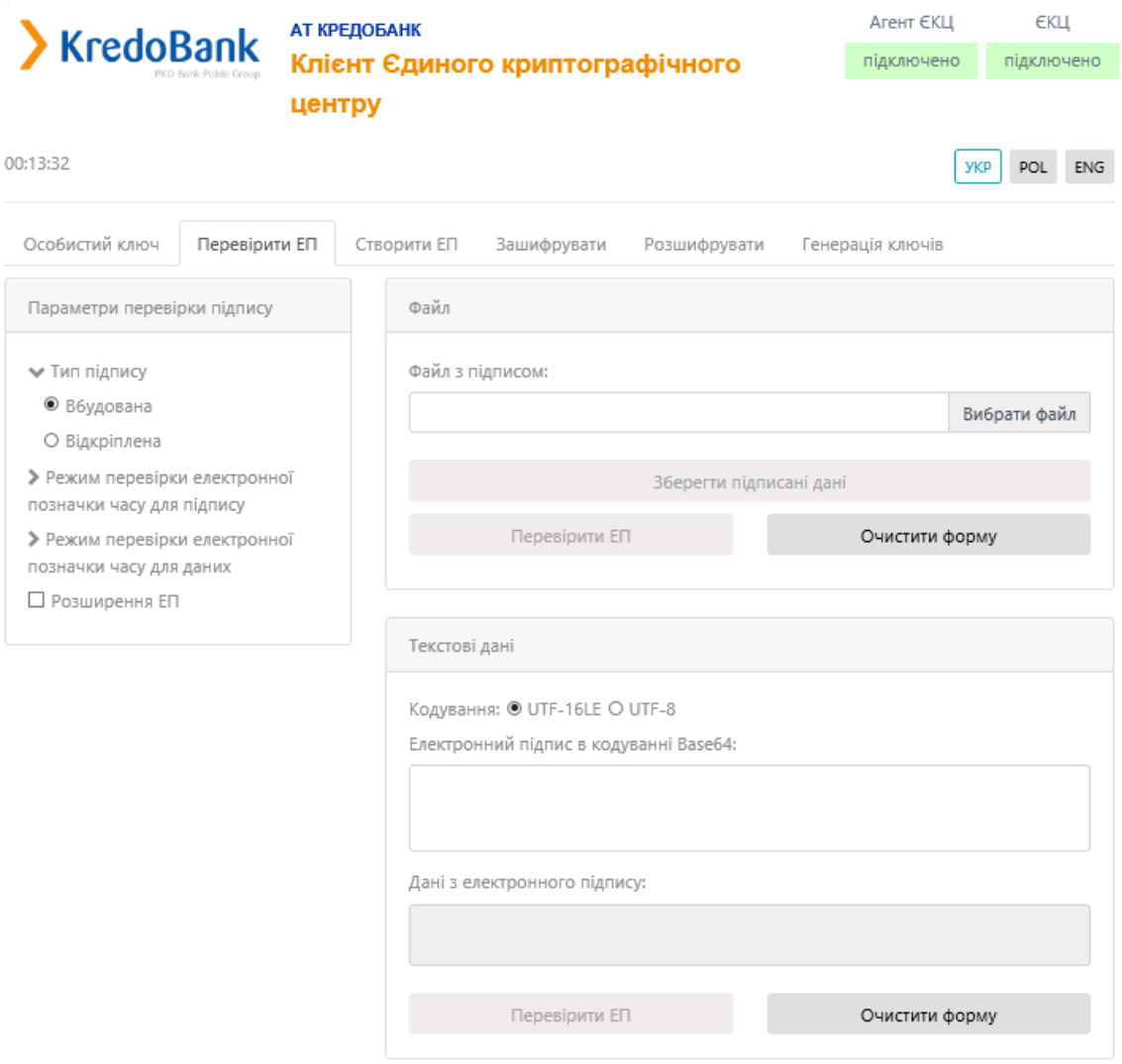

Рис. 42. Вкладка «Перевірити ЕП»

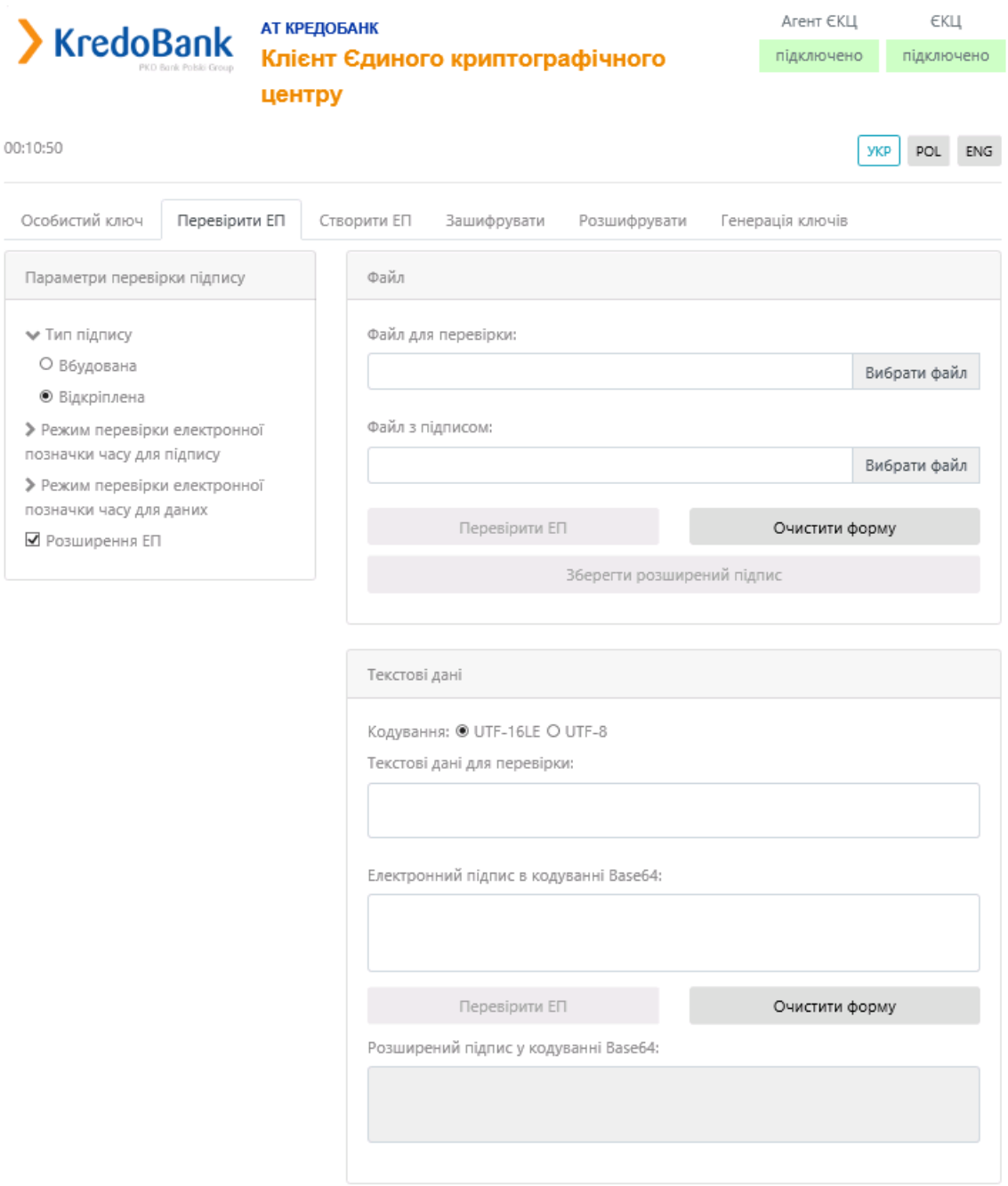

Рис. 43. Вкладка «Перевірити ЕП» зі вказівкою позначки «Розширення ЕП»

Якщо перевіряється файл за типом ЕП – **Відкріплена**.

1. Поле «Файл для перевірки» (обирається файл, який не містить підпис – початковий файл);
2. Поле «Файл з підписом» (обирається файл, який містить підпис за типом ЕП Відкріплена);
3. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису за допомогою завантаженого файлу з підписом для файлу для перевірки);
4. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов’язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Розділ «Текстові дані», який у свою чергу включає:

Якщо перевіряється файл за типом ЕП – **Вбудована**.

1. Кодування: UTF-16LE та UTF-8.
2. Поле «Підпис у кодування Base64» (вказується текст, який містить підпис за типом ЕП Вбудована).
3. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
4. Поле «Дані з електронного підпису» (виведення текст без підпсиу);
5. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Якщо перевіряється файл за типом ЕП – **Відкріплена**.

1. Кодування: UTF-16LE та UTF-8.
2. Поле «Текстові дані для перевірки» (вказуються текстові дані, який не містить підпис – початкові дані);
3. Поле «Підпис у кодуванні Base64» (вказуються текстові дані з підписом, за типом ЕП Відкріплена);
4. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
5. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Процес Перевірки ЕП починається з того, що обираються «Параметри перевірки ЕП», обирається файл/текстові дані з підписом, натискаємо кнопку «Перевірити ЕП». За необхідності можна змінити файл/дані.

Перевірка ЕП за типом «Вбудована», файл

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Вбудована» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Вбудована, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо файл з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 44.

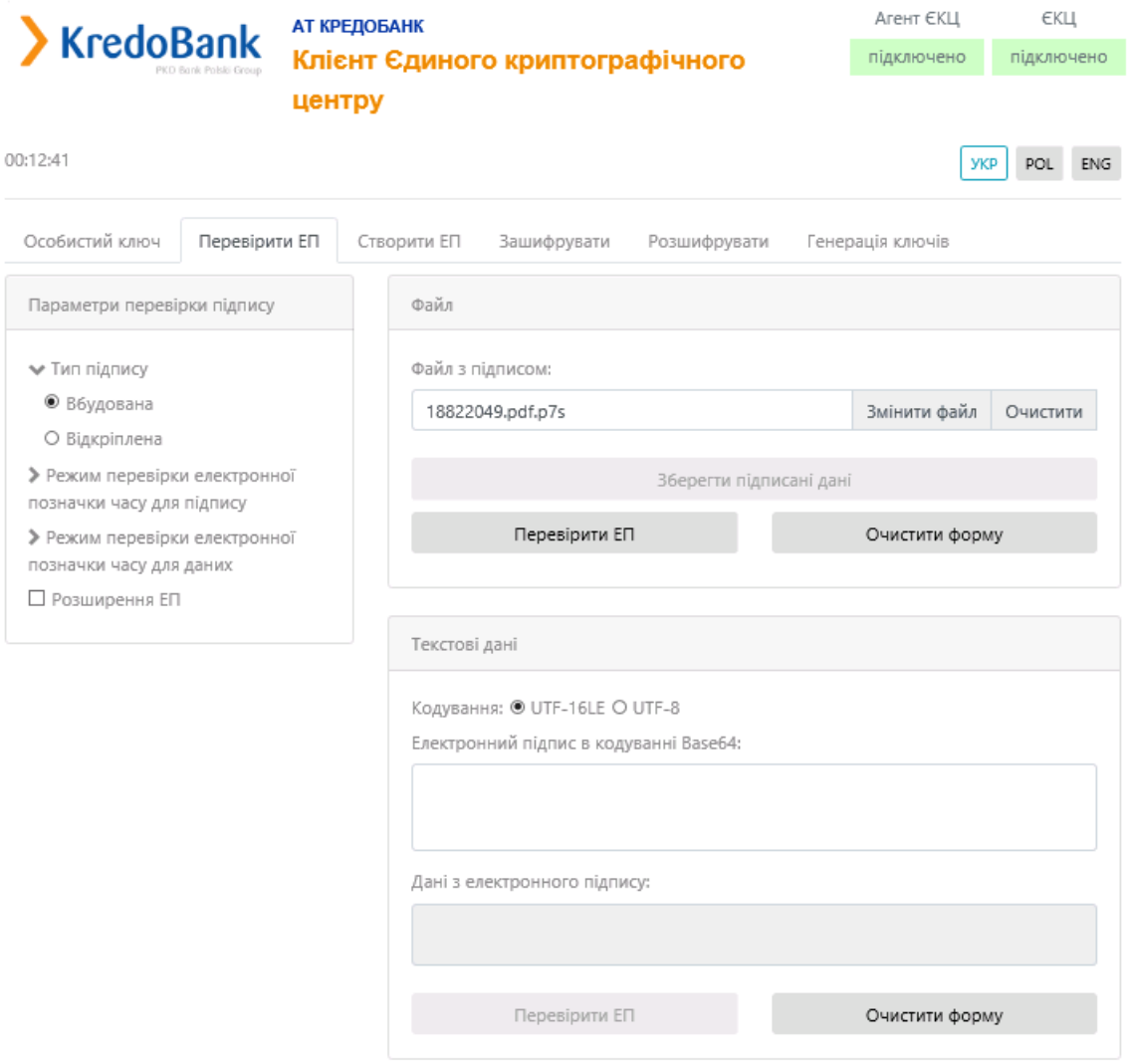

Рис. 44. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 45.

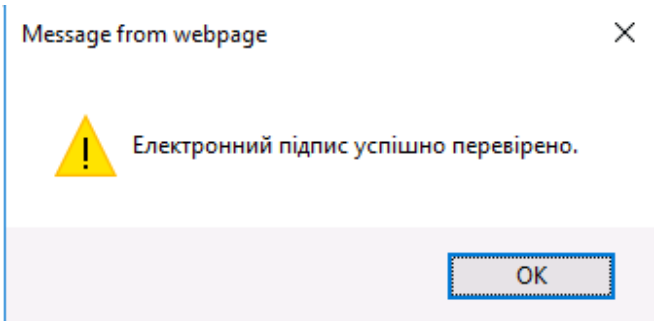

Рис. 45. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дату підпису, Рис. 46. За необхідності зберегти первинні дані (без підпису), натиснувши на кнопку «Зберегти підписані дані». Після чого, натискаємо кнопку «Очистити форму».

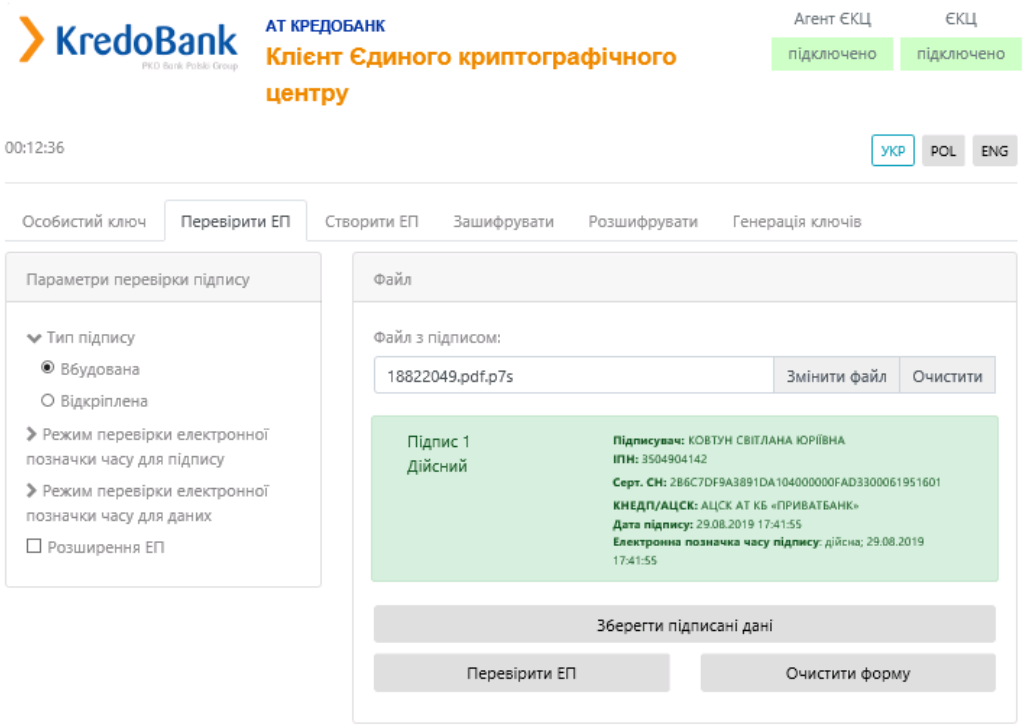

Рис. 46. Результат перевірки

Перевірка ЕП за типом «Відкріплена», файл

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Відкріплена» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Відкріплена, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо файл з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 47.

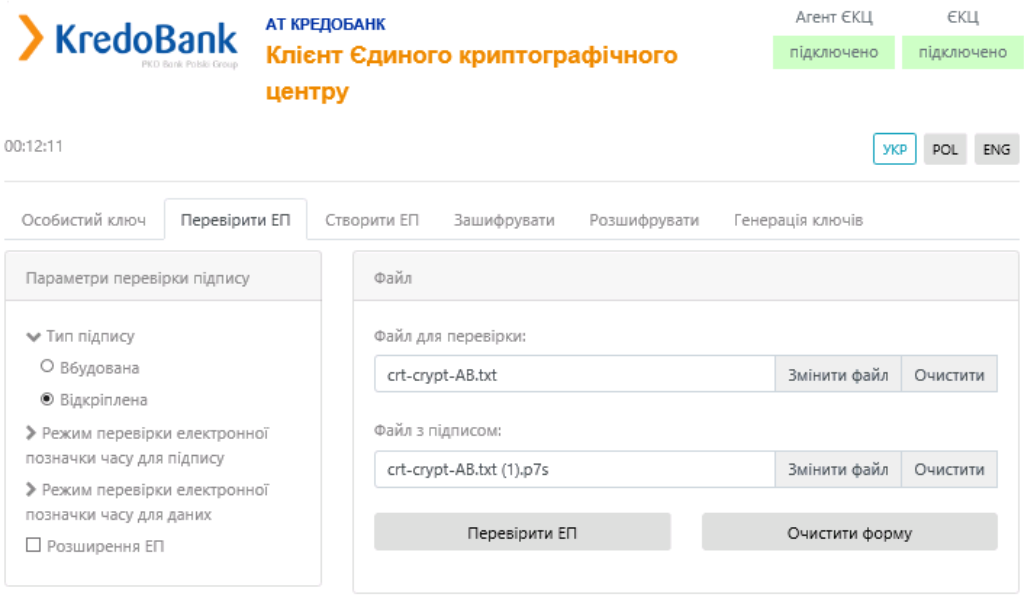

Рис. 47. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 48.

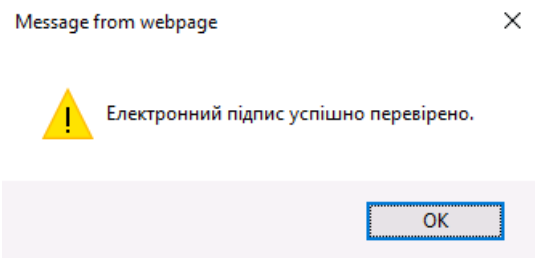

Рис. 48. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дата підпису, Рис. 49. Після чого, натискаємо кнопку «Очистити форму».

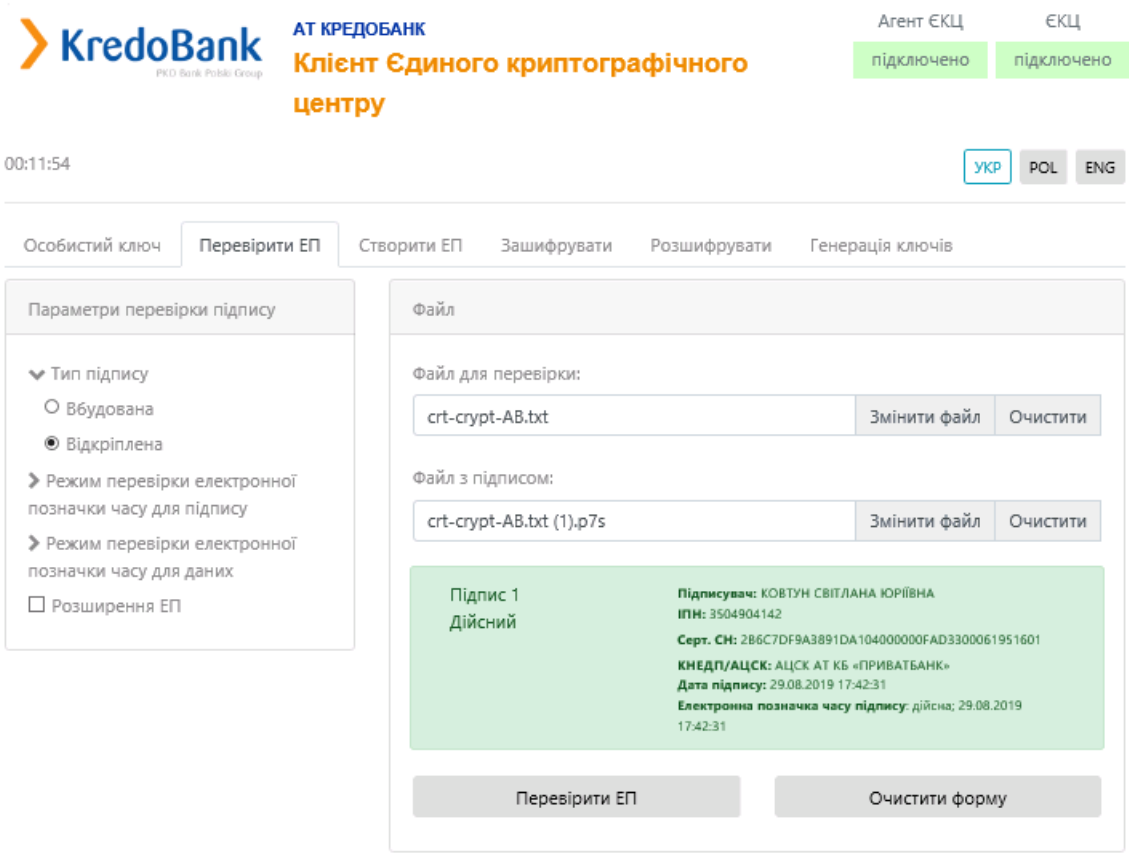

Рис. 49. Результат перевірки

Перевірка ЕП за типом «Вбудована», текстові дані

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Вбудована» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Вбудована, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо текст з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 50.

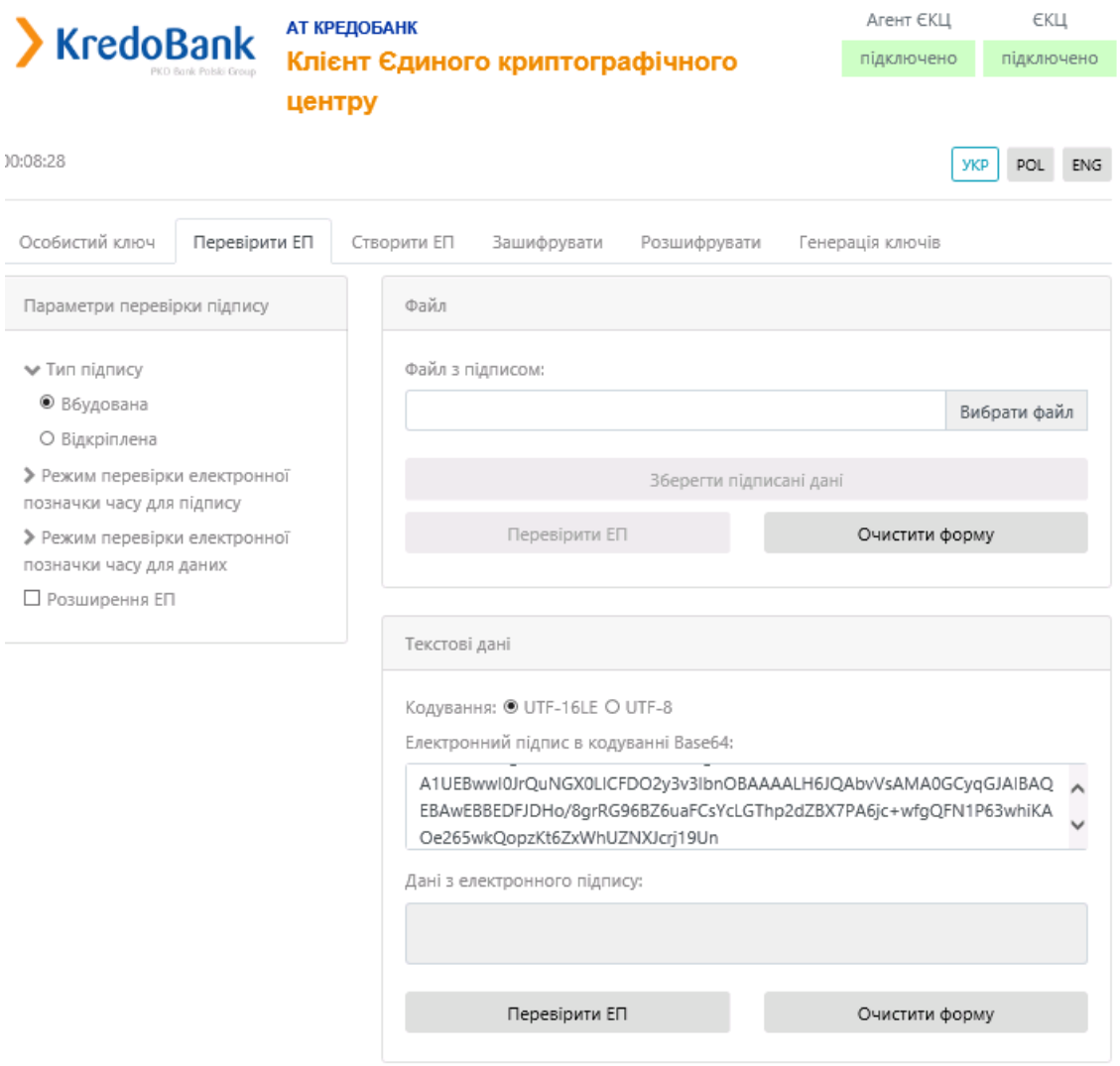

Рис. 50. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 51.

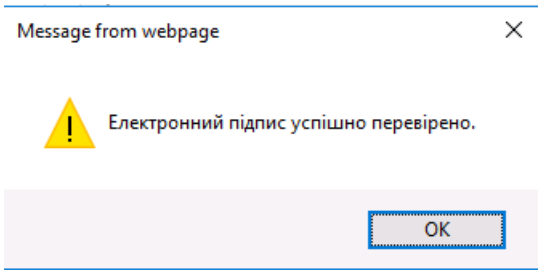

Рис. 51. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дату підпису, Рис. 52. Після чого, натискаємо кнопку «Очистити форму».

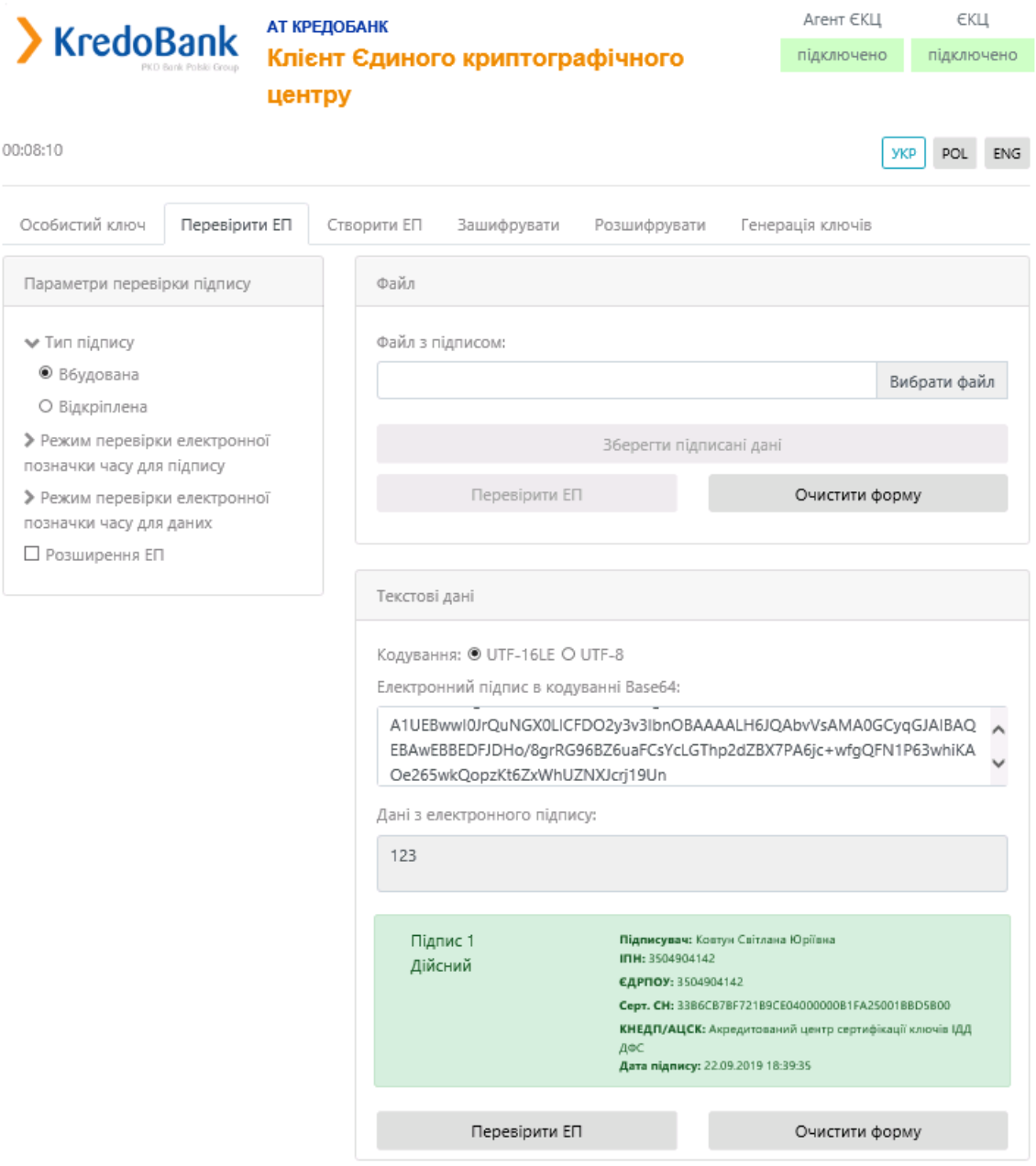

Рис. 52. Результат перевірки

Перевірка ЕП за типом «Відкріплена», текстові дані

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Відкріплена» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Відкріплена, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо текст з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 53.

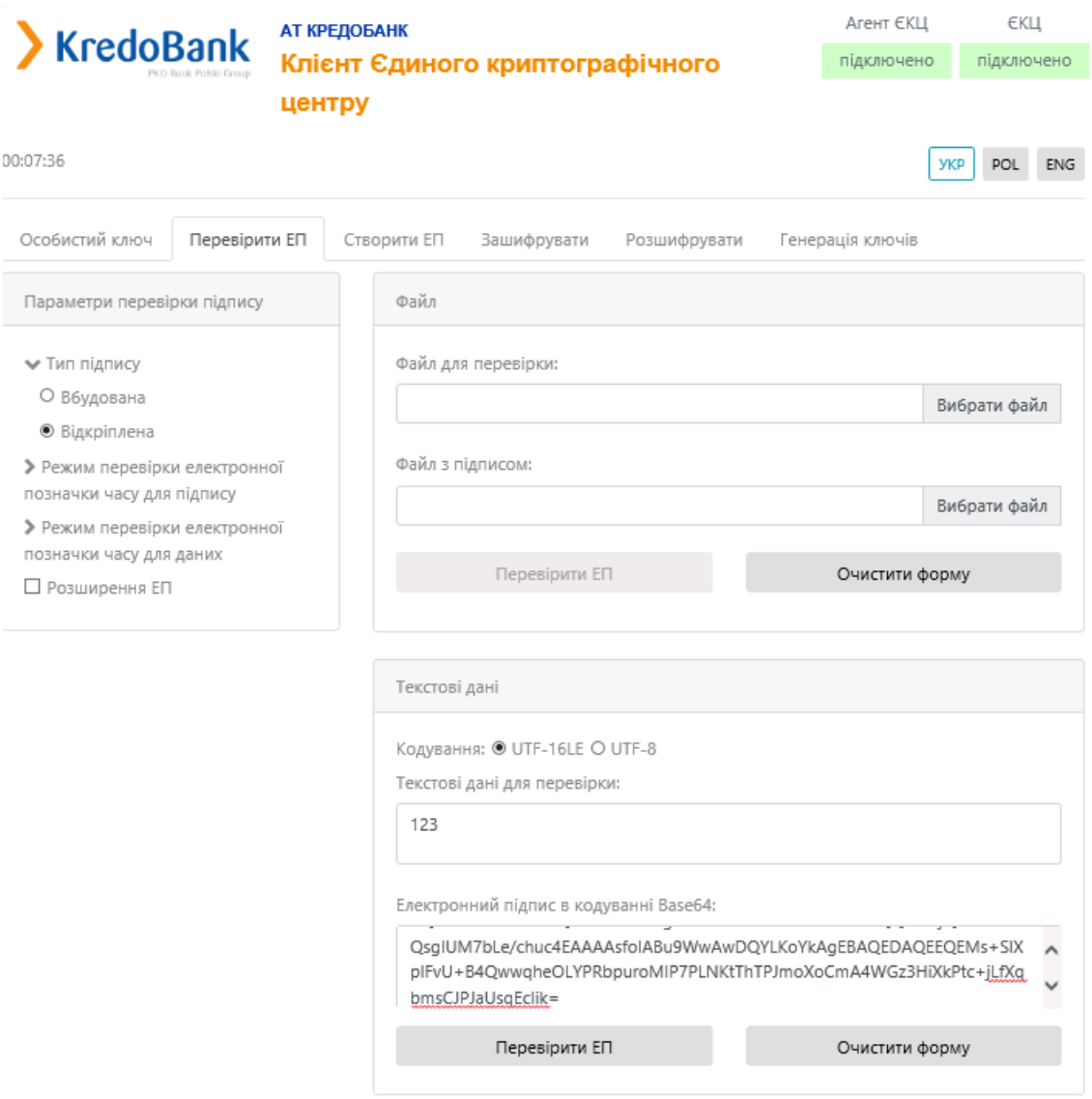

Рис. 53. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 54.

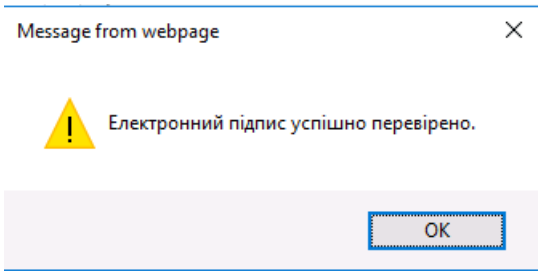

Рис. 54. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дата підпису, Рис. 55. Після чого, натискаємо кнопку «Очистити форму».

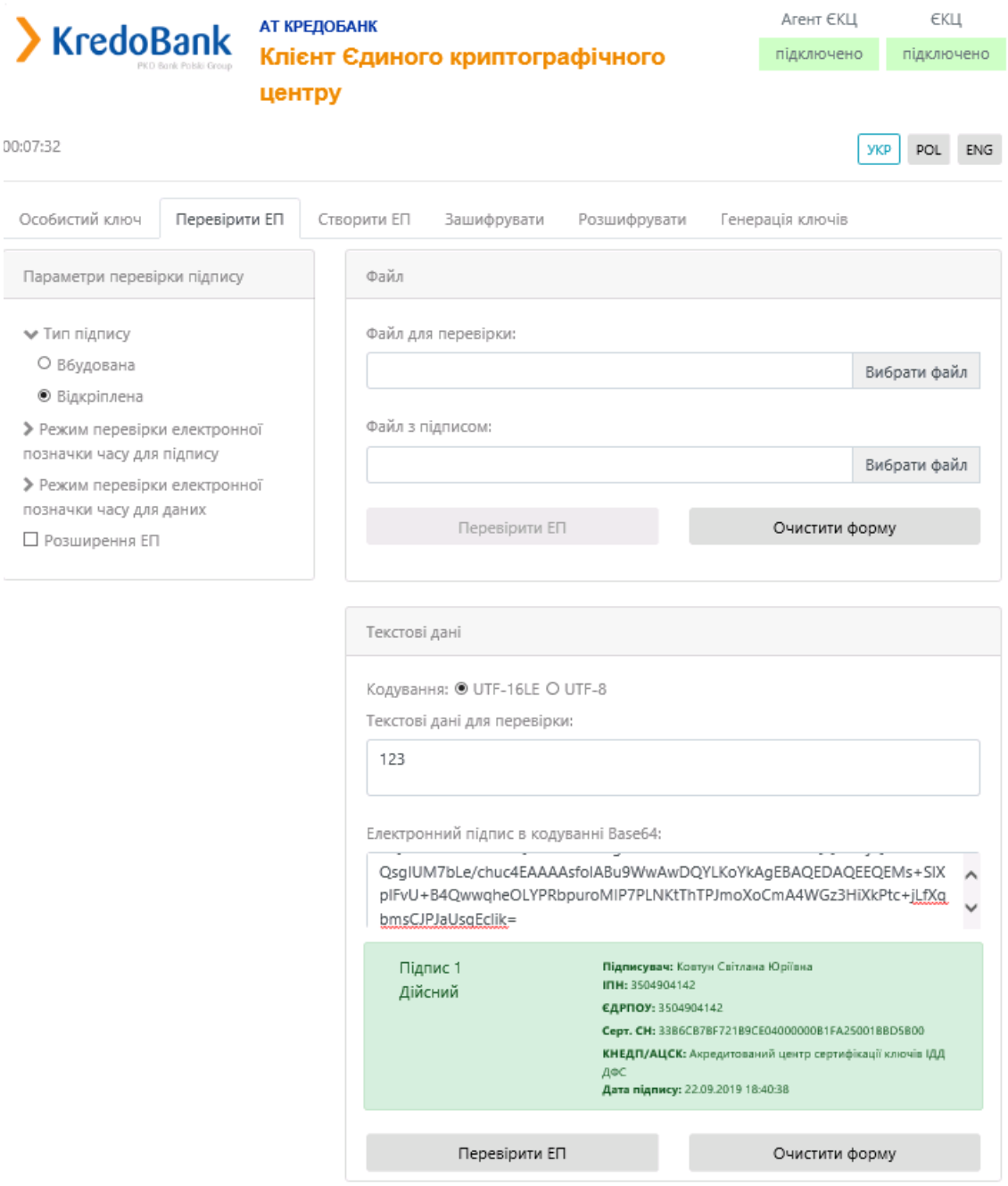

Рис. 55. Результат перевірки

Перевірка базового ЕП

Для перевірки ЕП за типом «Вбудована», формат ЕП «Базовий» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Вбудована та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо файл з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 56.

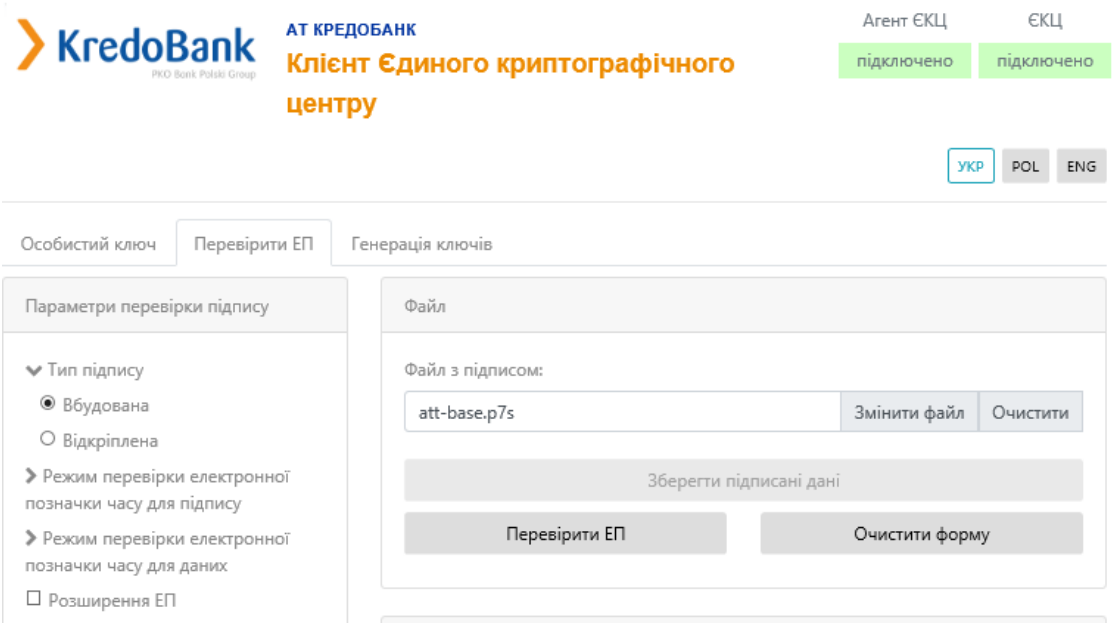

Рис. 56. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 57.

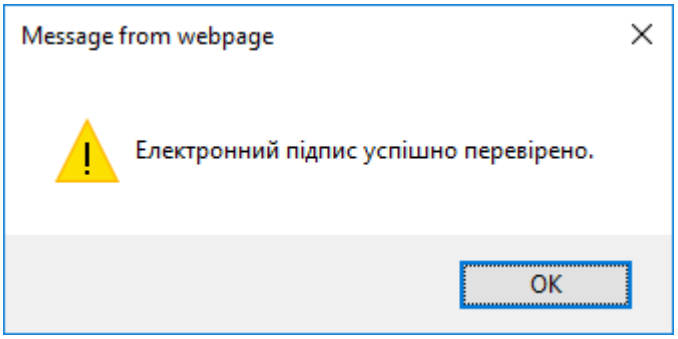

Рис. 57. Повідомлення про перевірку електронного підпису

Після натискання «ОК», з'являється інформація про перевірку підпису, вказується інформація про підписанта, дату підпису та повідомлення, що підпис є Базовий, Рис. 58. За необхідності зберегти первинні дані (без підпису), натиснувши на кнопку «Зберегти підписані дані». Після чого, натискаємо кнопку «Очистити форму».

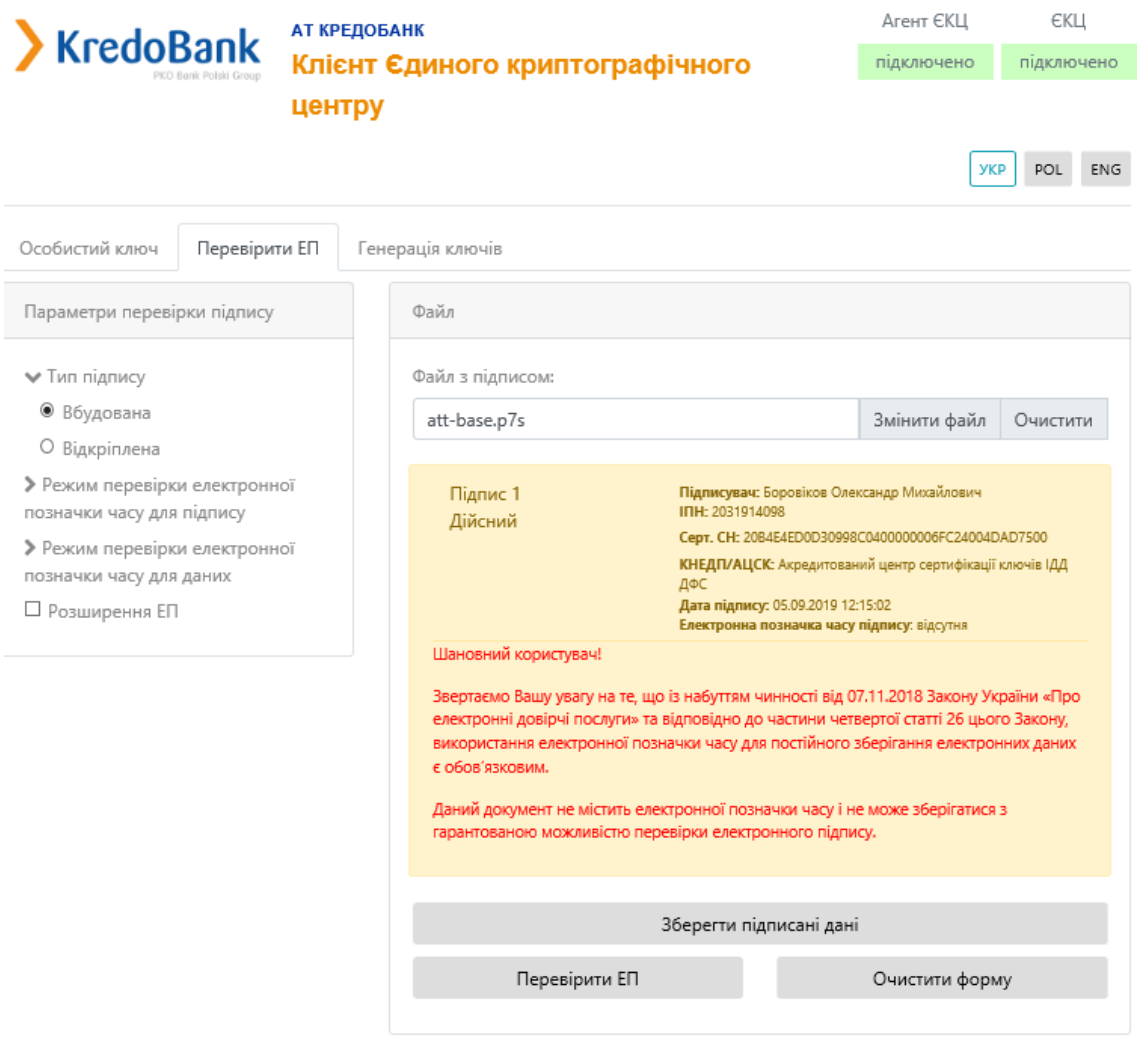

Рис. 58. Результат перевірки

Розширення ЕП

Вкладка «Перевірити ЕП» містить додаткову позначку «Розширити ЕП», при її вказівці, зовнішній вигляд сторінки видозмінюється та стають доступні нові кнопки, Рис. 59.

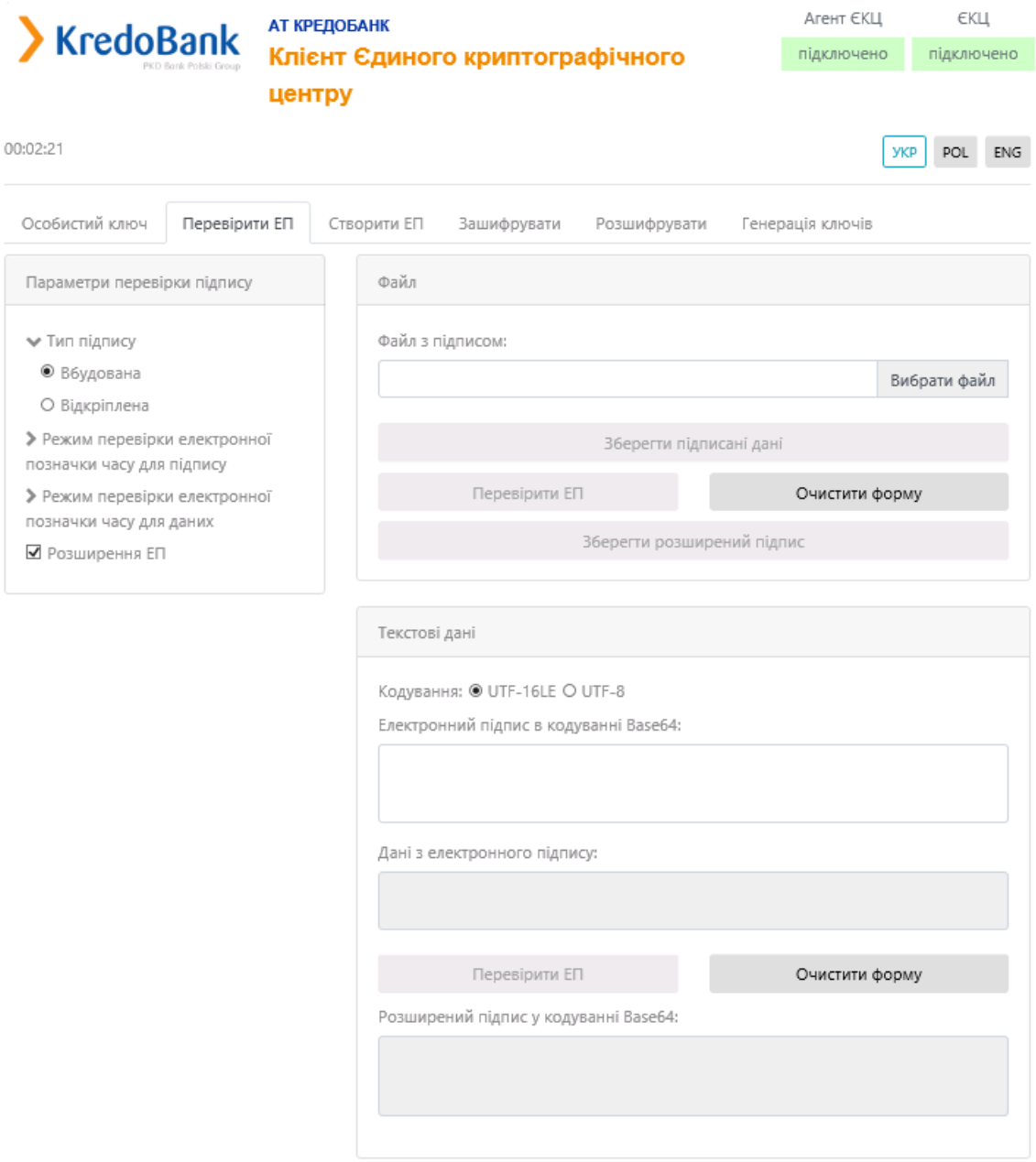

Рис. 59. Вкладка «Перевірити ЕП» з позначкою «Розширення ЕП»

Розширення ЕП для файлу

Відеоінструкція доступна за посиланням.

На прикладі вбудованого електронного підпису, який отримано раніше. Слід обрати файл та натиснути кнопку «Перевірити ЕП», Рис. 60.

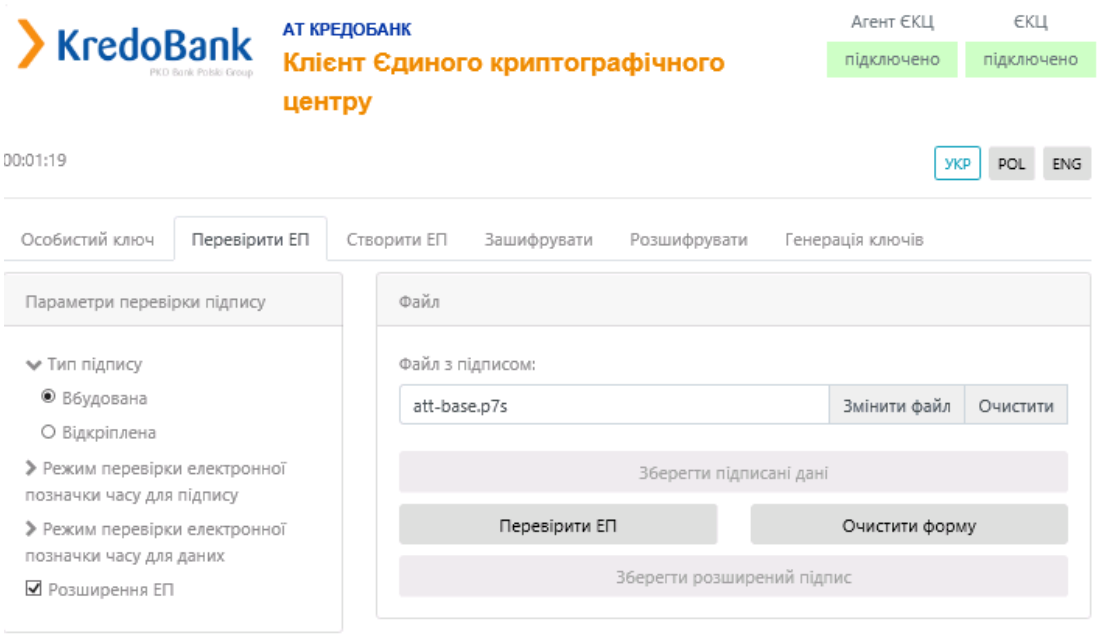

Рис. 60. Розширення вбудованого ЕП

Отримати повідомлення про успішне розширення підпису, Рис. 61.

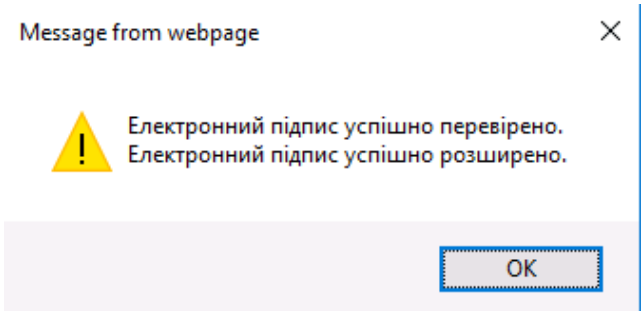

Рис. 61. Повідомлення про результат перевірки та розширення ЕП

Отримати результат перевірки електронного підпису, Рис. 62.

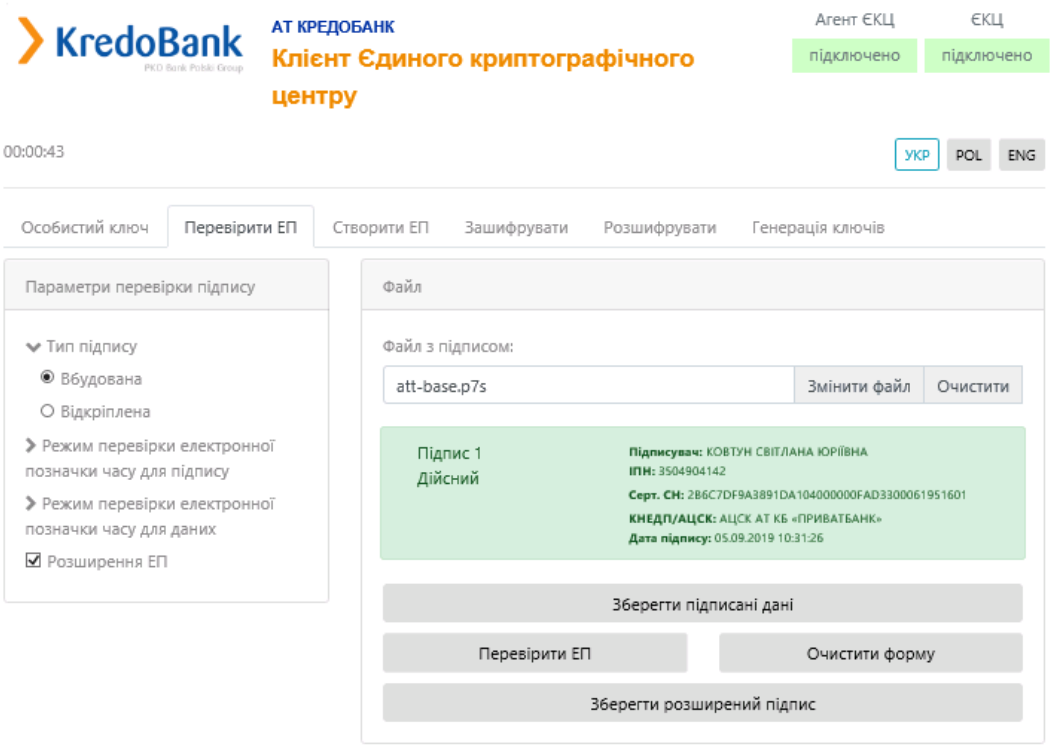

Рис. 62. Розширення вбудованого ЕП

За умови, якщо було завантажено файл вже з повними даними для перевірки, то з’явиться повідомлення про це, Рис. 63.

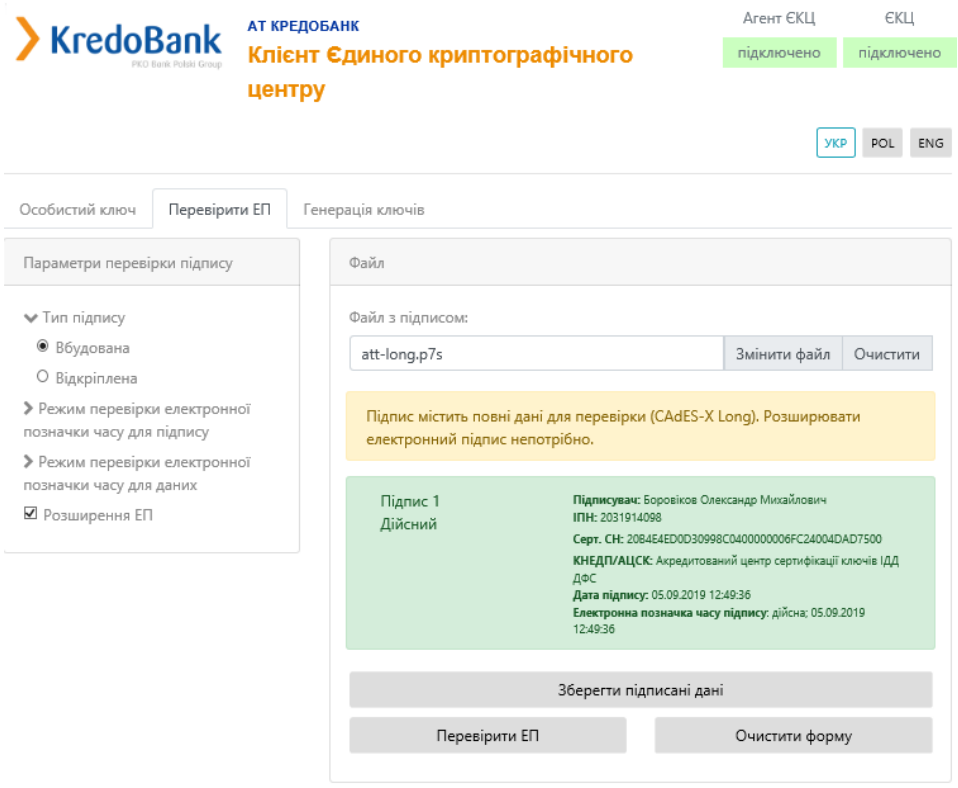

Рис. 63. Результати розширення підпису з повними даними для перевірки

Розширення ЕП для текстових даних

Відеоінструкція доступна за посиланням.

На прикладі відкріпленого електронного підпису, який отримано раніше. Слід вказати підписані дані та натиснути кнопку «Перевірити ЕП», Рис. 64.

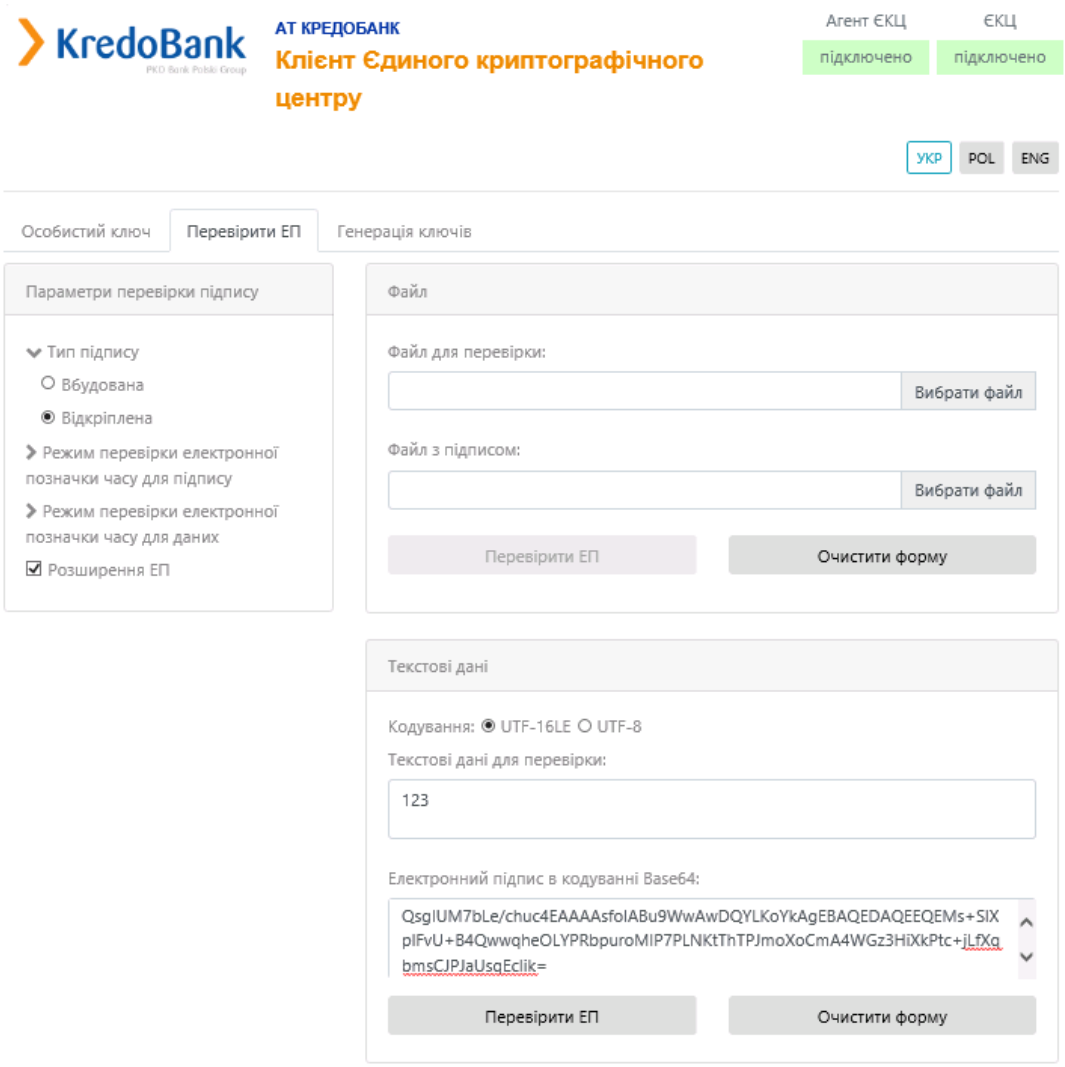

Рис. 64. Розширення відкріпленого ЕП

Отримати повідомлення про успішне розширення підпису, Рис. 65.

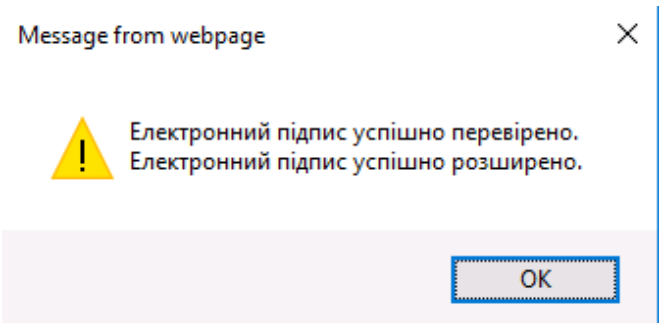

Рис. 65. Повідомлення про перевірку та розширення підпису

Отримати результат перевірки електронного підпису, Рис. 66.

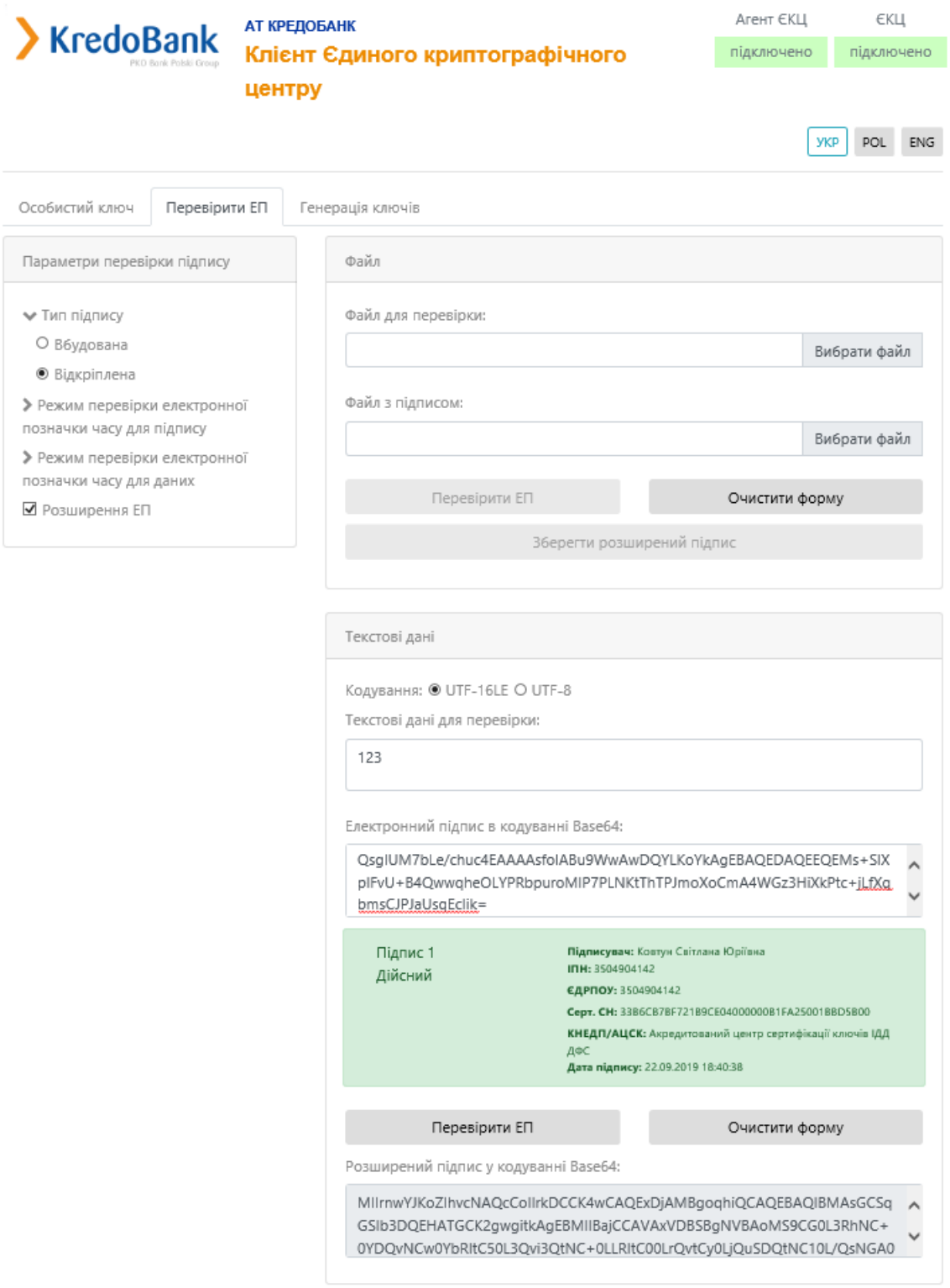

Рис. 66. Результат розширення та перевірки ЕП

За умови, якщо було завантажено текстові дані вже з повними даними для перевірки, то з’явиться повідомлення про це, Рис. 67.

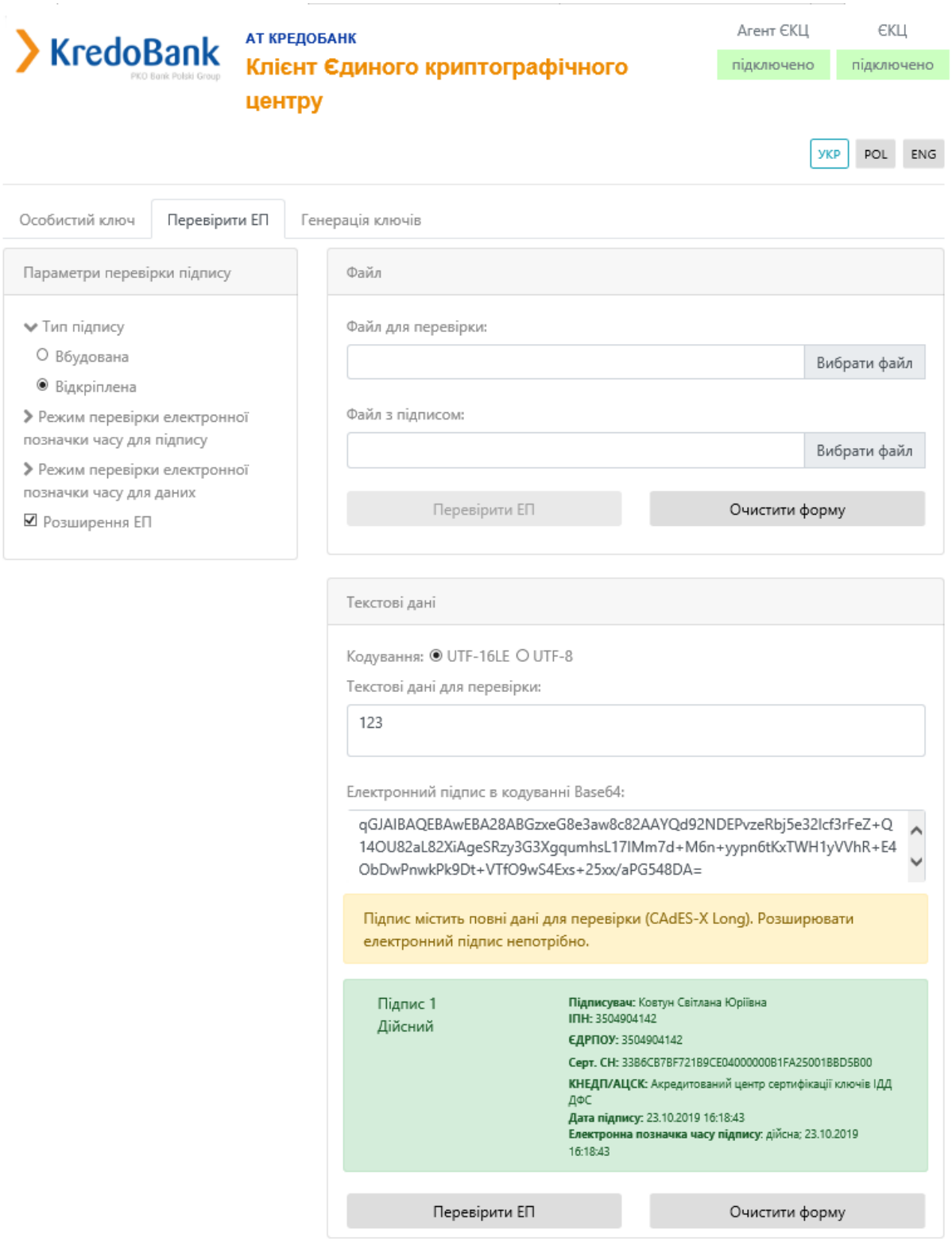

Рис. 67. Результати розширення підпису з повними даними для перевірки

Зашифрувати

Процес зашифрування здійснюється із застосуванням захищеного носія (в активному та пасивному режимі) чи файлового ключового контейнеру.

За умови, якщо генерація ключа здійснювалася за допомогою Агенту ЄКЦ у активному чи пасивному режимі – процес зашифрування здійснюється коректно, або самостійний запис ключа за допомогою «Модуля роботи з ключовим контейнером» у пасивному режимі.

Вкладка «Зашифрувати» містить такі розділи: Параметри шифрування, Сертифікат отримувача, Текстові дані та Файл, Рис. 68.

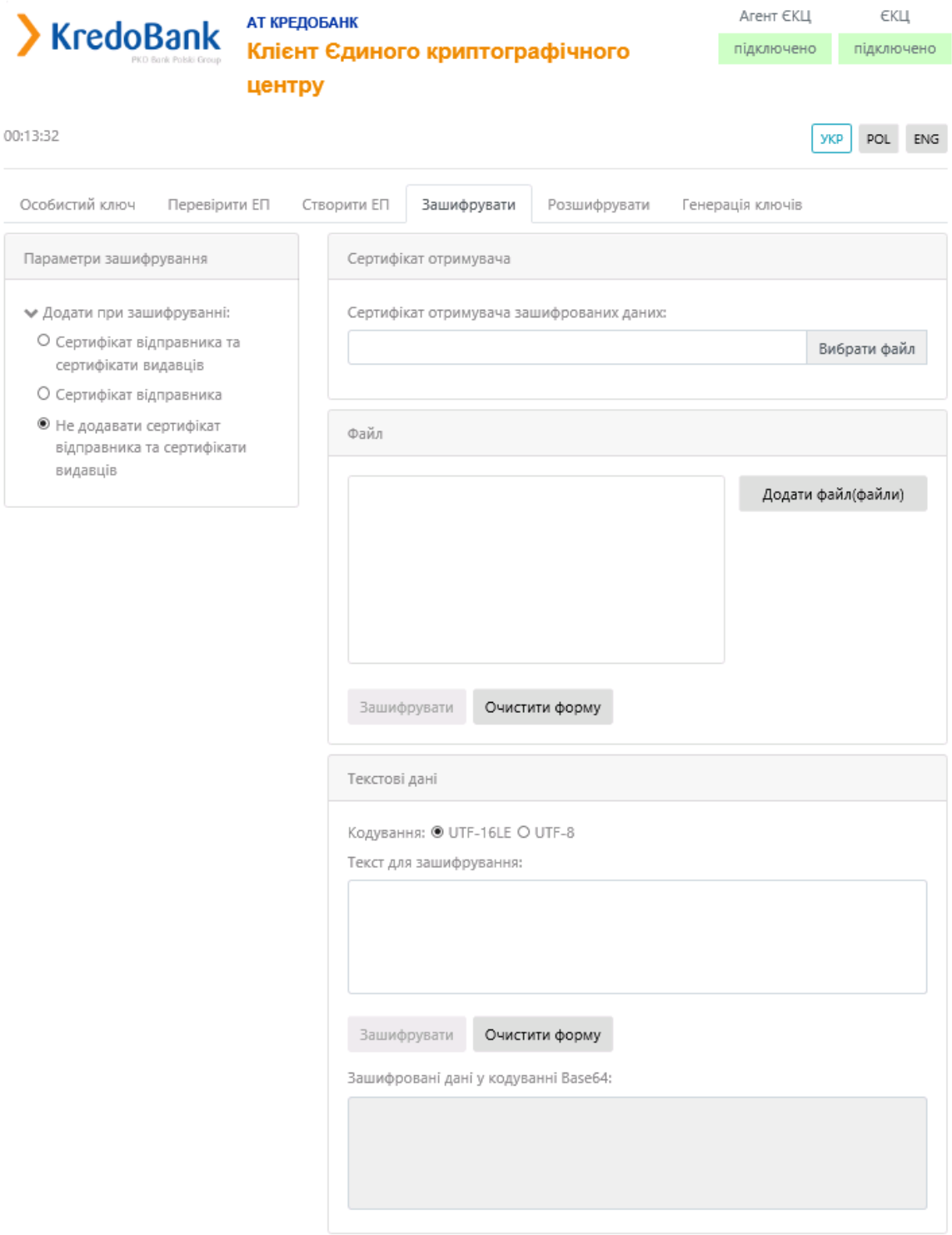

Рис. 68. Вкладка «Зашифрувати»

Розділ «Параметри шифрування», який включає:

1. Додати при шифруванні:
   - Сертифікат відправника та сертифікати видавців;
   - Сертифікати відправника;
   - Не додавати сертифікат відправника та сертифікати видавців.

Розділ «Сертифікат отримувача», який включає:

2. Поле «Сертифікат отримувача зашифрованих даних» (завантажуємо файл-сертифікат отримувача).

Розділ «Файл», який включає:

1. Поле «Файл» для додавання файлу/файлів для шифрування;
2. Кнопка «Зашифрувати» (здійснює зашифрування файлу);
3. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов’язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Розділ «Текстові дані», який включає:

1. Тип кодування UTF-16LE та UTF-8.
2. Поле «Текст для зашифрування»;
3. Кнопка «Зашифрувати» (здійснює зашифрування тексту);
4. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов’язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.
5. Поле «Зашифровані дані у кодуванні Base64».

Операція зашифрування файлу

Відеоінструкція знаходиться за посиланням.

Для того, щоб зашифрувати файл/текстові дані, у розділі «Параметри шифрування», обрати один з пунктів (сертифікат відправника та сертифікати видавців чи сертифікат відправника чи не додавати сертифікат відправника та сертифікати видавців), у розділі «Сертифікат отримувача» додати сертифікат отримувача зашифрованих даних, у розділі «Файл» обрати файл для шифрування, натиснути кнопку «Зашифрувати», Рис. 69.

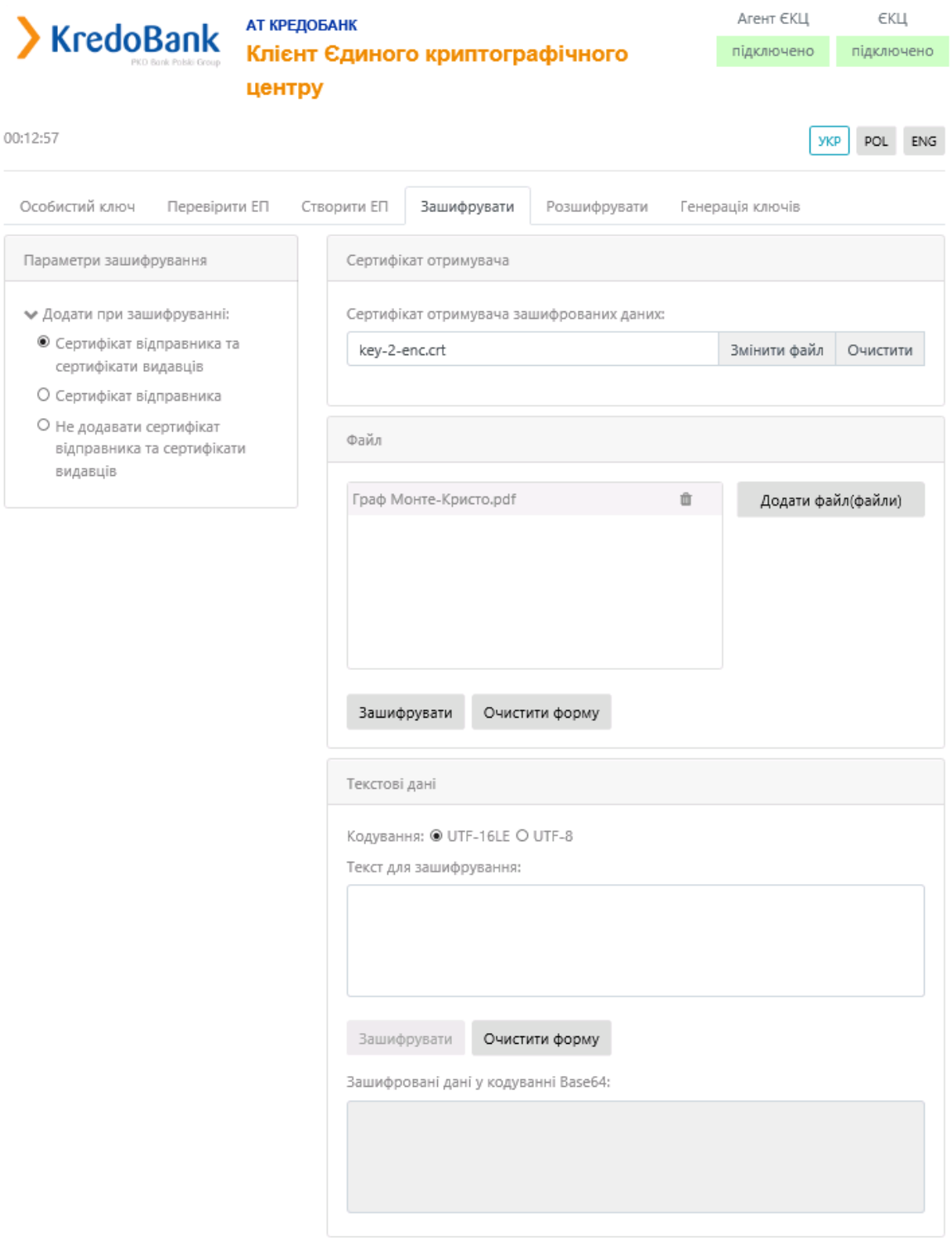

Рис. 69. Процес зашифрування

Після натискання на кнопку «Зашифрувати» з’являється вікно з повідомленням з результатом зашифрування, Рис. 70.

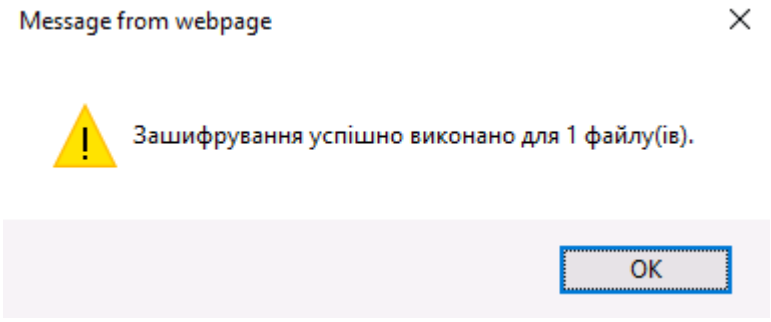

Рис. 70. Повідомлення про успішне зашифрування даних

Після, за допомогою відповідної кнопки «стрілка вниз» можна зберегти зашифрований файл та очищаємо форму, Рис. 71.

Рис. 71. Збереження зашифрованого файлу

Операція зашифрування текстових даних

Відеоінструкція знаходиться за посиланням.

Для того, щоб зашифрувати текстові дані, у розділі «Параметри шифрування», обрати один з пунктів (сертифікат відправника та сертифікати видавців чи сертифікат відправника чи не додавати сертифікат відправника та сертифікати видавців), у розділі «Сертифікат отримувача» додати сертифікат отримувача зашифрованих даних, у розділі «Текстові дані» вказати текст для шифрування, натиснути кнопку «Зашифрувати», Рис. 72.

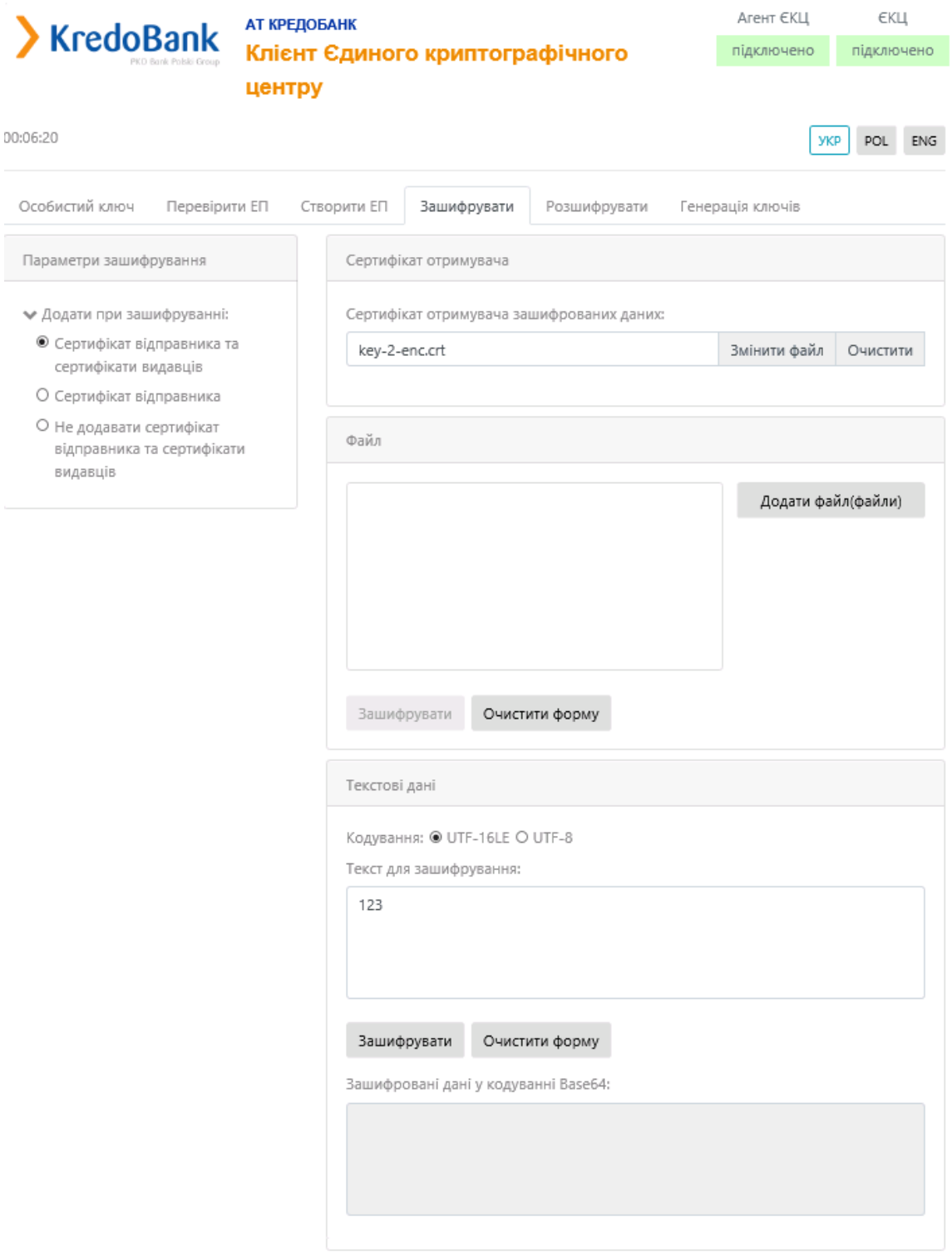

Рис. 72. Процес зашифрування

Після натискання на кнопку «Зашифрувати» з’являється у полі «Зашифровані дані у кодуванні Base64», Рис. 73.

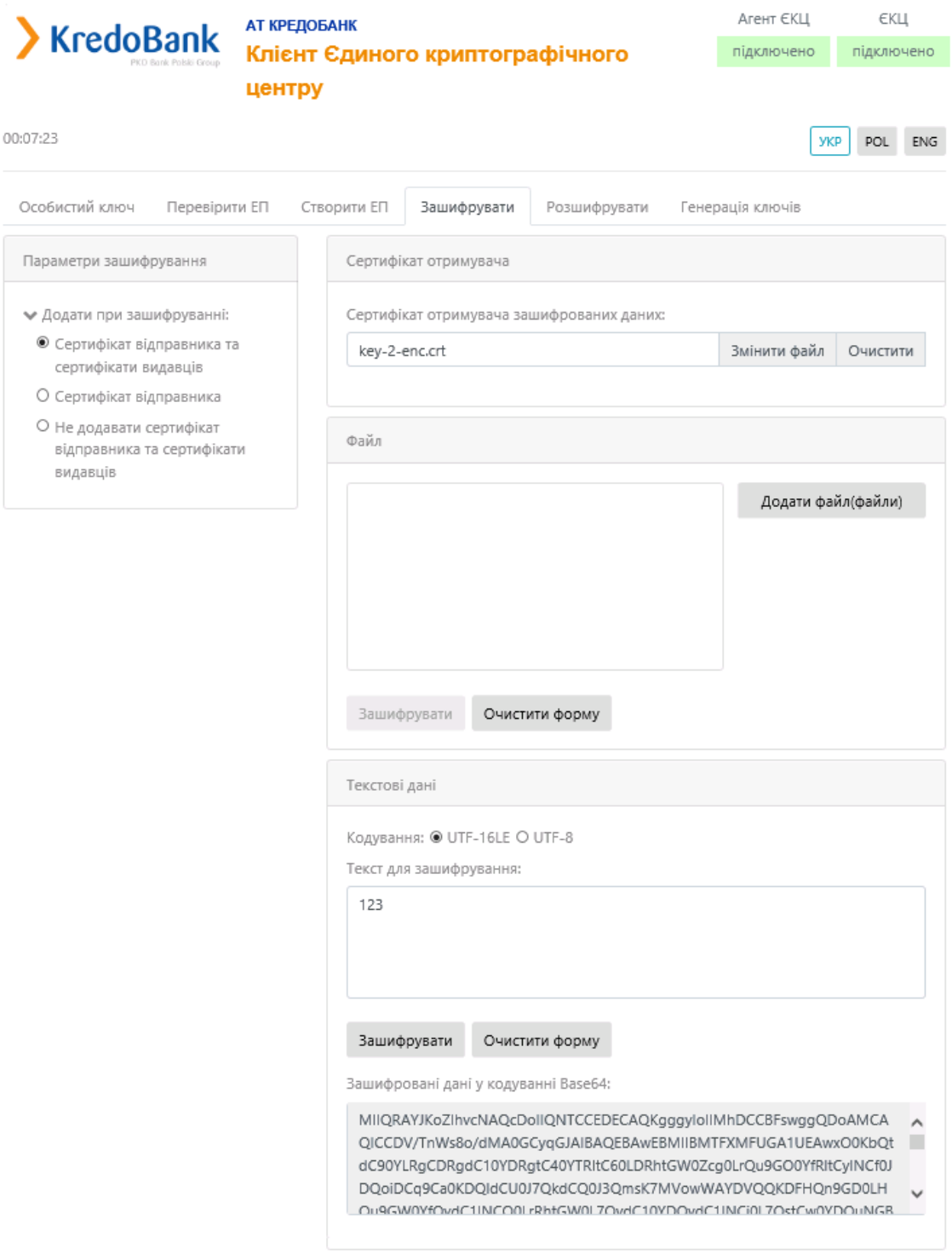

Рис. 73. Повідомлення про успішне зашифрування даних

Розшифрувати

Дана вкладка містить розділ Файл.

Розділ «Файл», який включає, Рис. 74:

1. Поле «Файл для розшифрування» (обирається файл, який необхідно розшифрувати);

2. Кнопка «Розшифрувати» (Здійснює дешифрування файлу);
3. Кнопка «Зберегти розшифровані дані у файл»;
4. Кнопка «Очистити форму» (здійснює очищення форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Розділ «Текстові дані», який включає:Рис. 74

1. Тип кодування: UFT-16LE та UTF-8.
2. Поле «Зашифровані дані у кодуванні Base64» (вказується текст, який необхідно розшифрувати);
3. Кнопка «Розшифрувати» (здійснює дешифрування текстових даних);
4. Кнопка «Очистити форму» (здійснює очищення форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

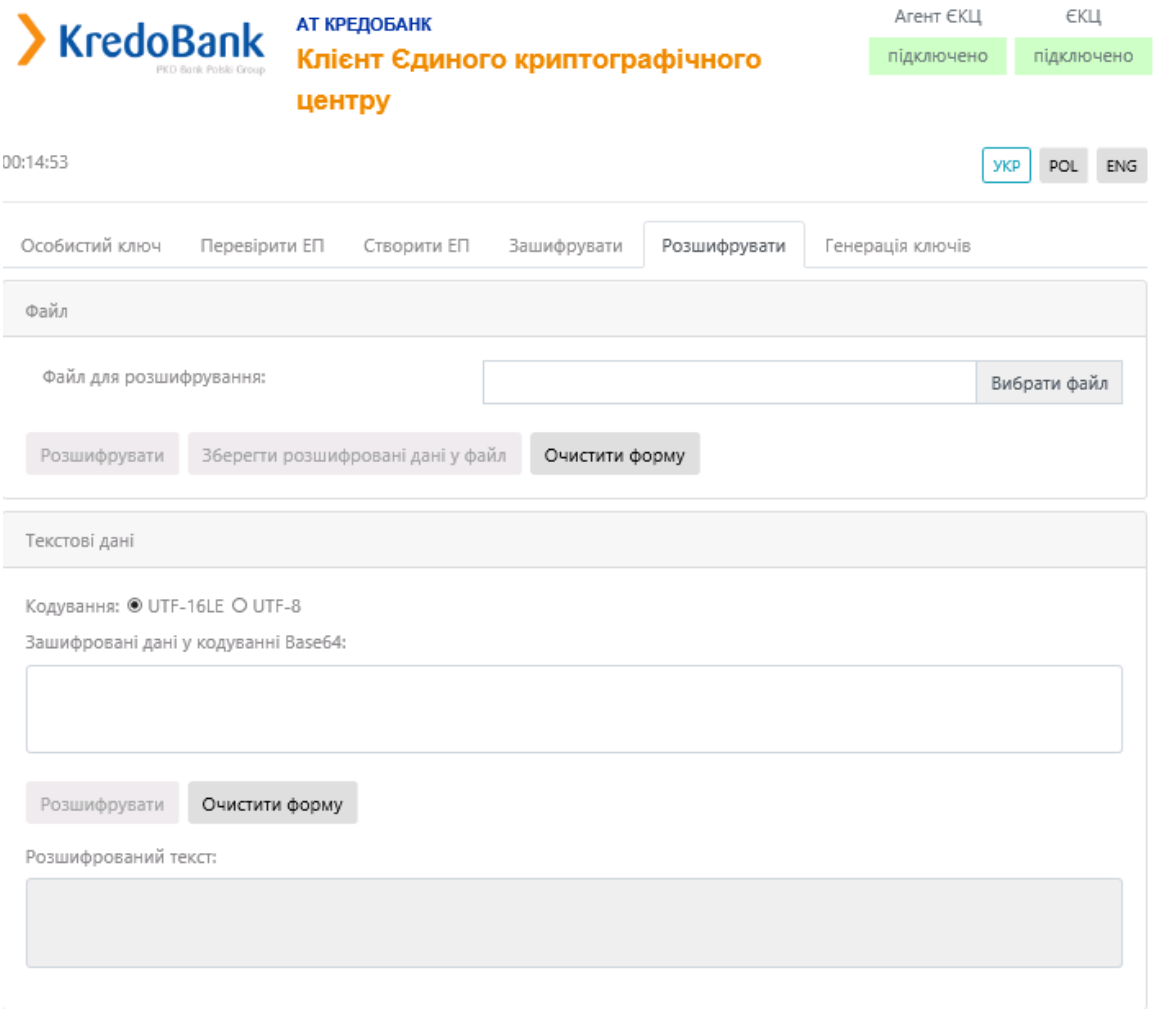

Рис. 74. Вкладка «Розшифрувати»

Операція розшифрування файлу

Відеоінструкція знаходиться за посиланням.

Для того, щоб розшифрувати файл, у розділі «Файл», необхідно вказати файл для розшифрування та натиснути кнопку «Розшифрувати», Рис. 75.

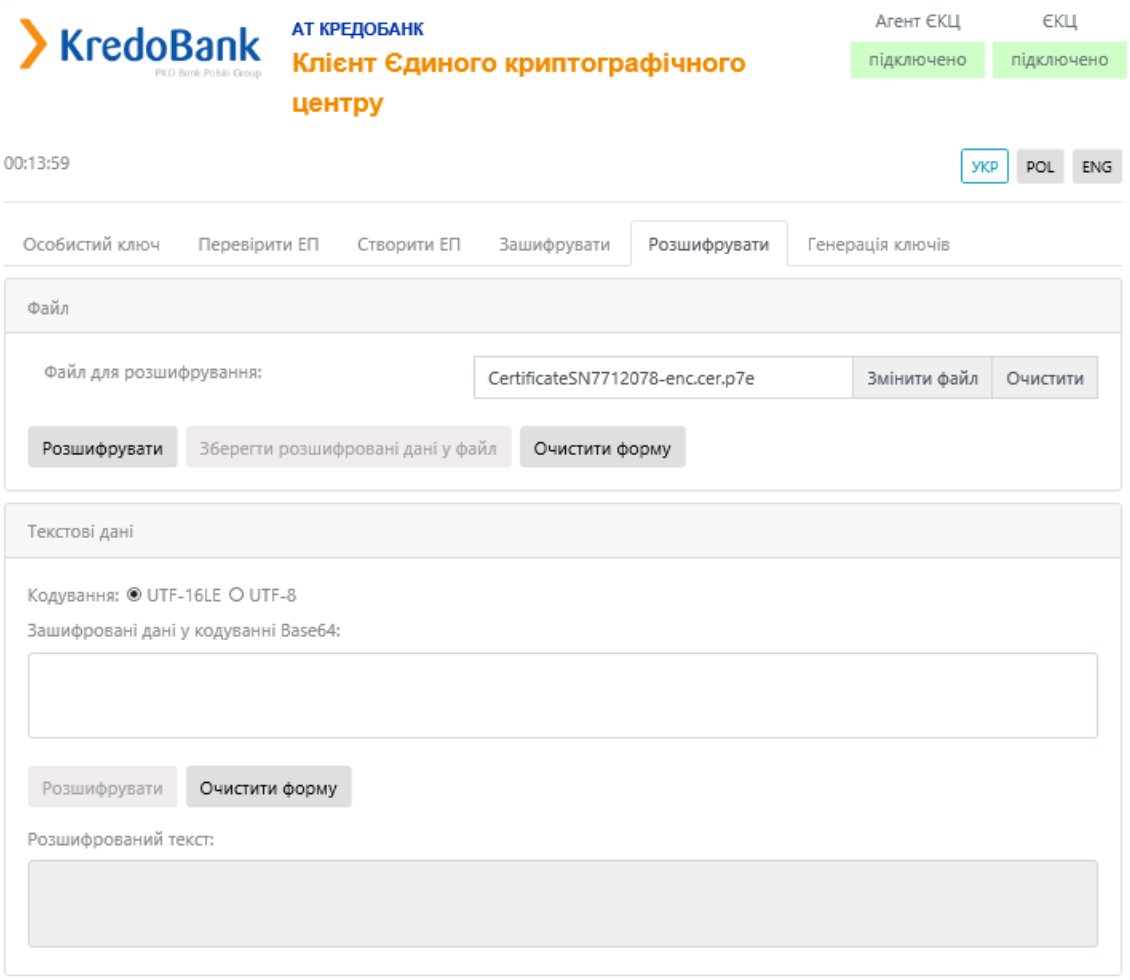

Рис. 75. Процес розшифрування

Після натискання на кнопку «Розшифрувати» з'являється вікно з повідомленням з результатом зашифрування, Рис. 76, де слід натиснути кнопку «ОК» та для збереження розшифрованих даних необхідно натиснути кнопку «Зберегти розшифровані дані у файл», Рис. 77 та очистити форму.

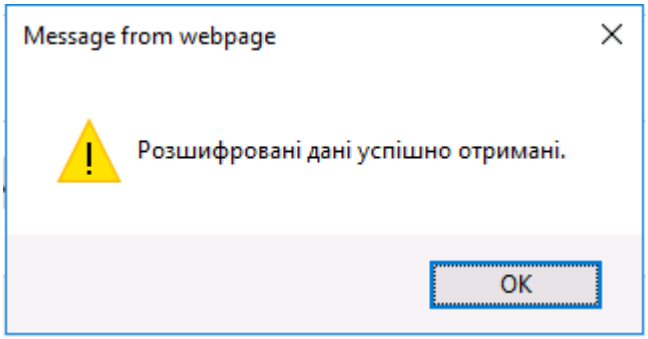

Рис. 76. Повідомлення про успішне розшифрування даних

Рис. 77. Збереження зашифрованих даних

Операція розшифрування текстових даних

Відеоінструкція знаходиться за посиланням.

Для того, щоб розшифрувати текст, у розділі «Текстові дані», необхідно вказати текст для розшифрування та натиснути кнопку «Розшифрувати», Рис. 78.

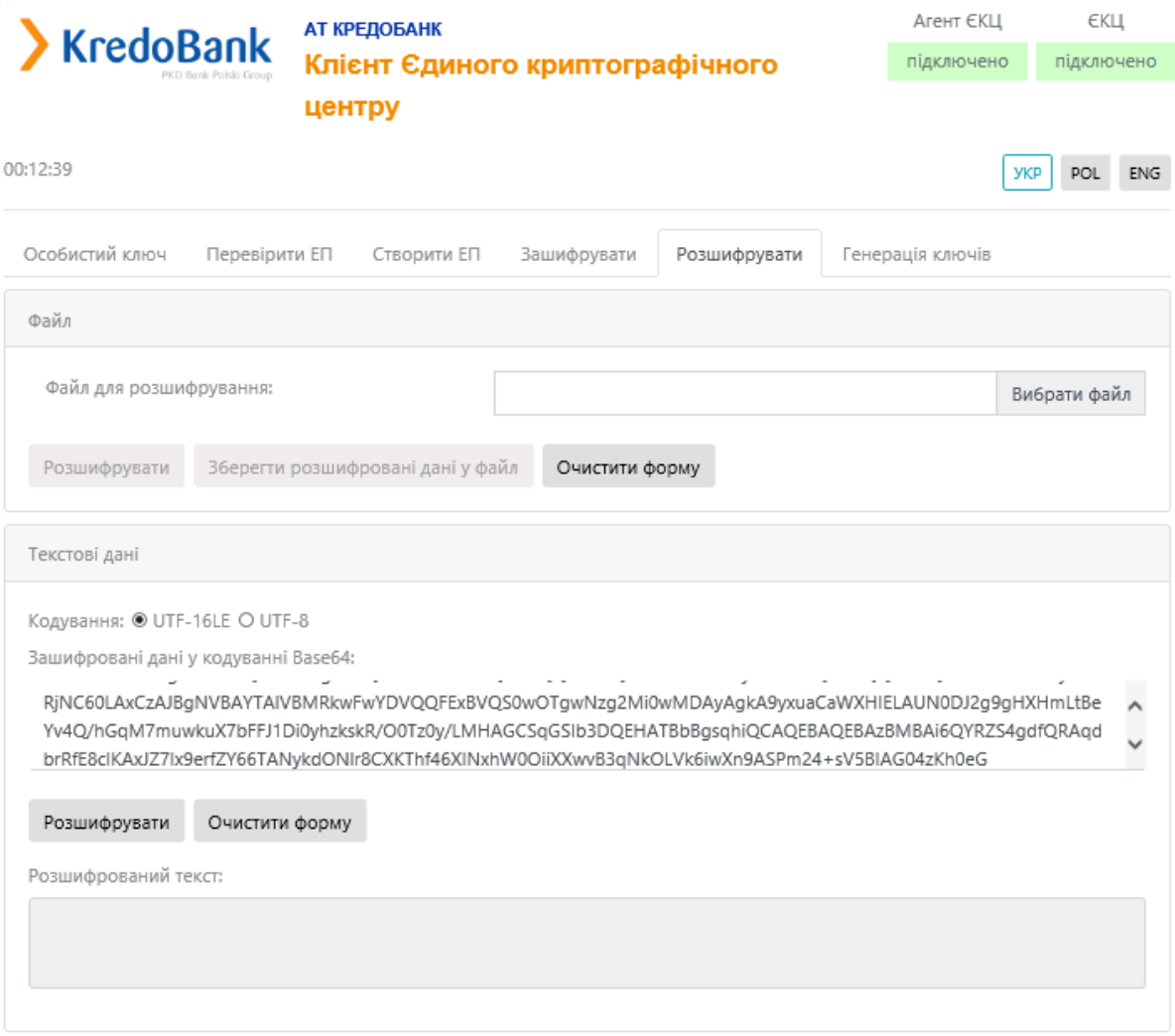

Рис. 78. Процес розшифрування

Після натискання на кнопку «Розшифрувати» з’являється розшифровані текстові дані у полі «Розшифрований текст», Рис. 79 та очистити форму.

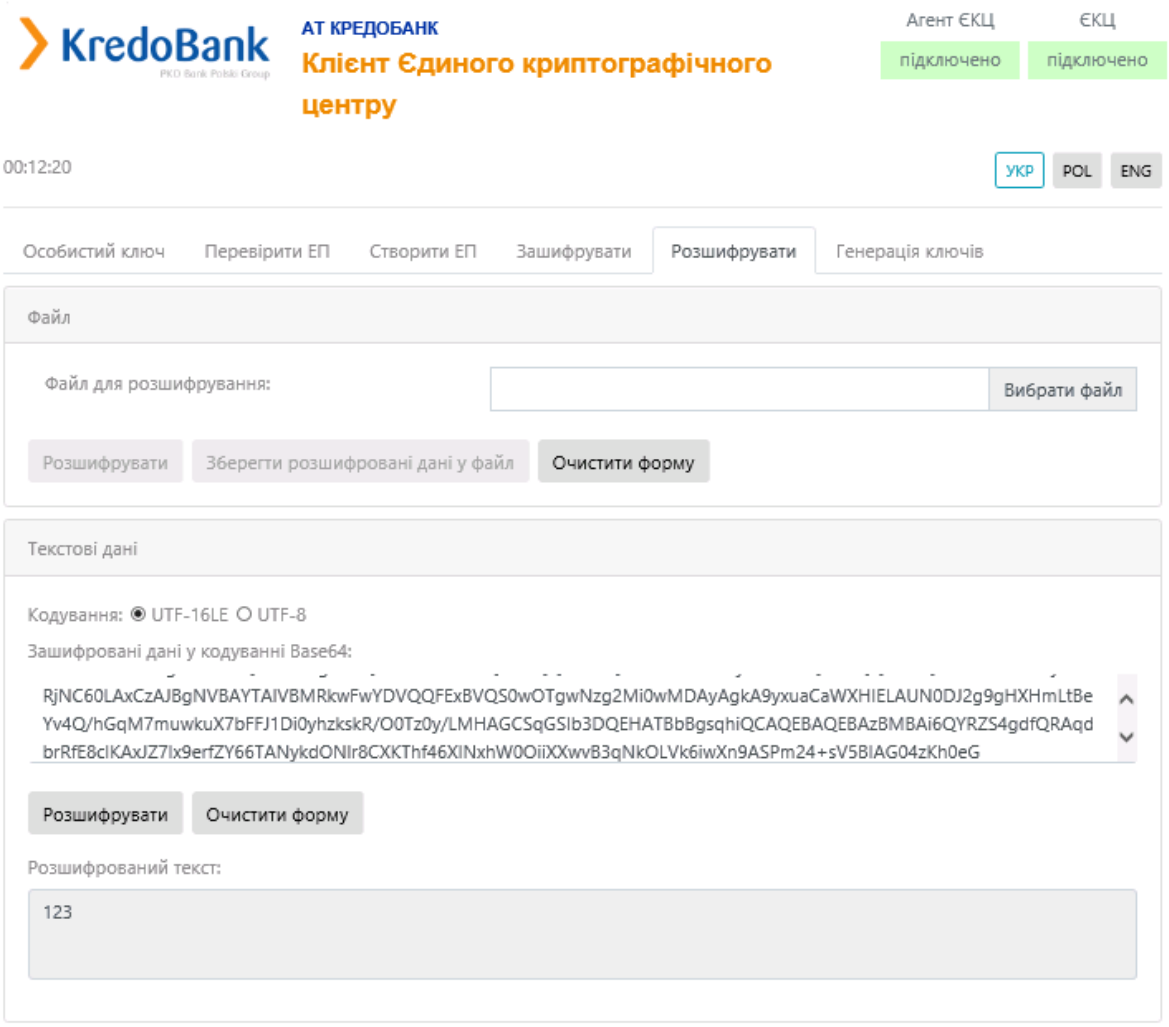

Рис. 79. Розшифровані текстові дані