САЙФЕР
Системы защиты информации
Интернет-банкинг

Сайфер ПРО, 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: 24/10/2019

Шифр-CaaS

Настанова з експлуатації веб-клієнту

ЗМІСТ

Вступ

В цьому документі описано порядок дій користувача для використання програмного комплексу «Шифр-CaaS», а саме веб-клієнту, його функціональні можливості та необхідні відомості для роботи з ним.

Системні вимоги

Перед початком 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.

Робота з Єдиного сервісом криптографічних операцій

Запуск

У веб-браузері перейти за посиланням - https://cryptocenter.cipher.kiev.ua/ до Клієнту Єдиного сервісу криптографічних операцій.

Відеоінструкція знаходиться за посиланням.

Покрокова інструкція та ознайомлення з інтерфейсом програмного комплексу:

1. Стартове вікно Клієнту Єдиного сервісу криптографічних операцій у веб-браузері показано на Рис. 1.

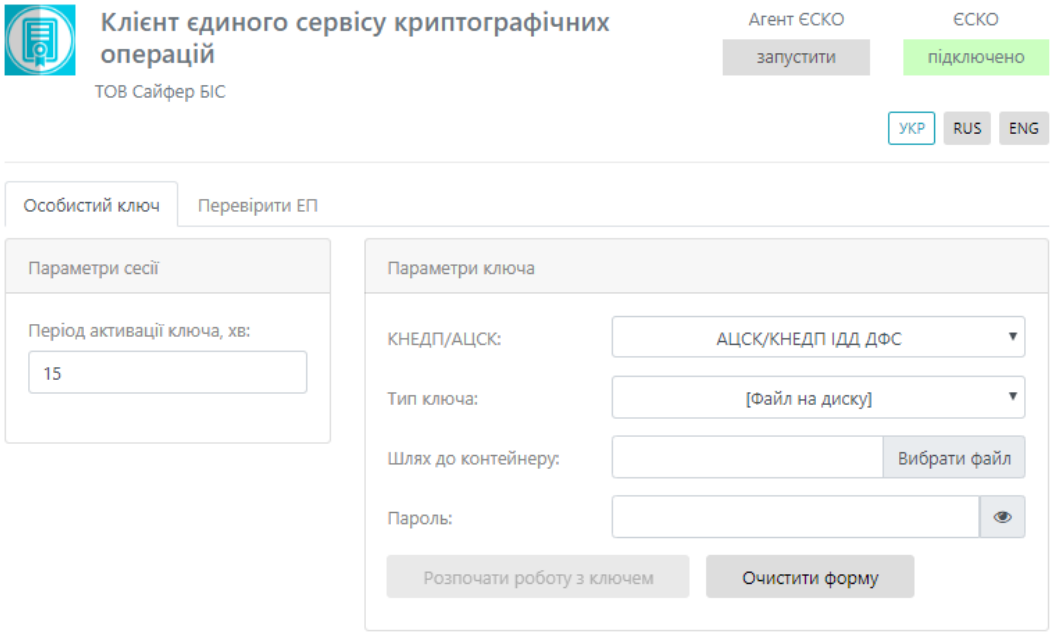

Рис. 1. Стартове вікно Клієнту ЄСКО

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

Перелік АЦСК/КНЕДП, які підтримуються «Єдиного сервісом криптографічних операцій»:

- АЦСК/КНЕДП Національного банку України;
- АЦСК/КНЕДП ІДД ДФС;
- АЦСК/КНЕДП органів юстиції України;
- АЦСК/КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
- АЦСК/КНЕДП ПАТ «КБ «Приватбанк»;
- АЦСК/КНЕДП ПАТ «УкрСиббанк»;
- АЦСК/КНЕДП «Masterkey» ТОВ «Арт-мастер»;
- АЦСК/КНЕДП Збройних Сил;
- АЦСК/КНЕДП Міністерства внутрішніх справ України;
- АЦСК/КНЕДП Державної прикордонної служби;
- АЦСК/КНЕДП Укрзалізниці;
- АЦСК/КНЕДП ринку електричної енергії;

- АЦСК/КНЕДП ПАТ «Національний депозитарій України»;
- АЦСК/КНЕДП ТОВ «Ключові системи»;
- АЦСК/КНЕДП ДП «Українські спеціальні системи»;
- АЦСК/КНЕДП Генеральної прокуратури України;
- АЦСК/КНЕДП/ ПАТ «Ощадбанк».

2. ***Тип ключа***:
   - файл на диску (за замовчуванням).
   - MobileID (вже впровадили Vodafone Україна та Lifecell (на основі стандарту ДСТУ 4145-2002)).
     Якщо необхідна робота із захищеним носієм, слід натиснути у правому верхньому куті кнопку «**запустити**» під назвою «Агент ЄСКО» та переглянути іншу інструкцію з назвою «Агент Єдиного сервісу криптографічних операцій. Настанова з установки та експлуатації Агенту ЄСКО (Java)».
3. ***Шлях до контейнеру***;
4. ***Пароль*** до ключа, Рис. 2.

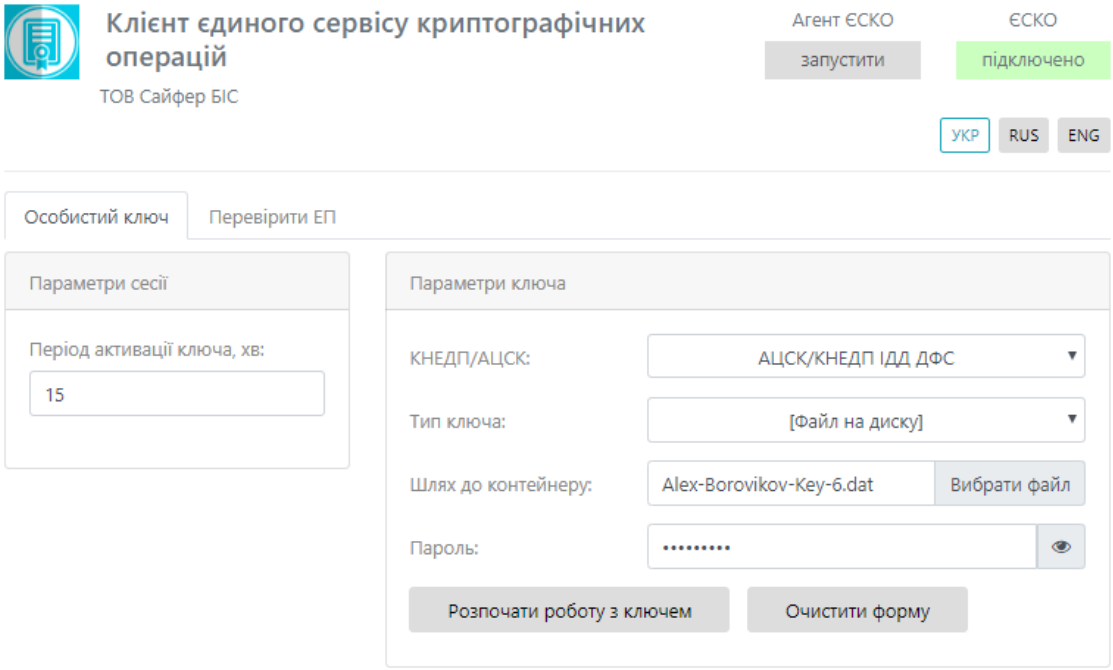

Рис. 2. Заповнення розділу «Параметри ключа»

4. Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем» та одразу відкривається робоча область, де стають доступні всі функції та операції для ЄСКО, Рис. 3.

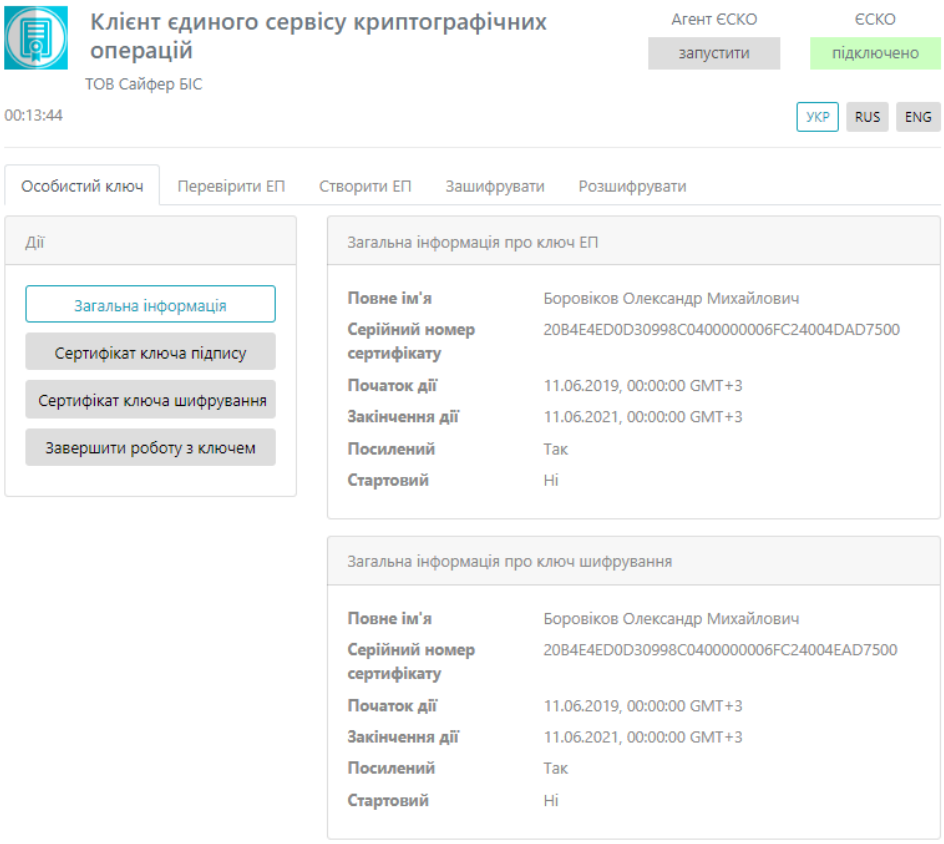

Рис. 3. Робоча область Клієнту ЄСКО

Службові функції та опції ЄСКО

Після завантаження даних ключового контейнеру у вікні «Єдиного сервісу криптографічних операцій» з'являються такі поля та відповідні опції, Рис. 4:

1. Вкладка «Особистий ключ», яка містить кнопки:
   - «Загальна інформація» - коротка інформація про ключі.
   - «Сертифікат ключа підпису» - повна інформація про сертифікат ключа ЕП.
   - «Сертифікат ключа шифрування» - повна інформація про сертифікат ключа шифрування.
   - «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 електронної 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 накладено підпис) та файл з підписом (файл, який містить підпис). Включає в себе одне поле.

- Тип ЕП – Вбудована: файл з підписом (файл який містить підпис).

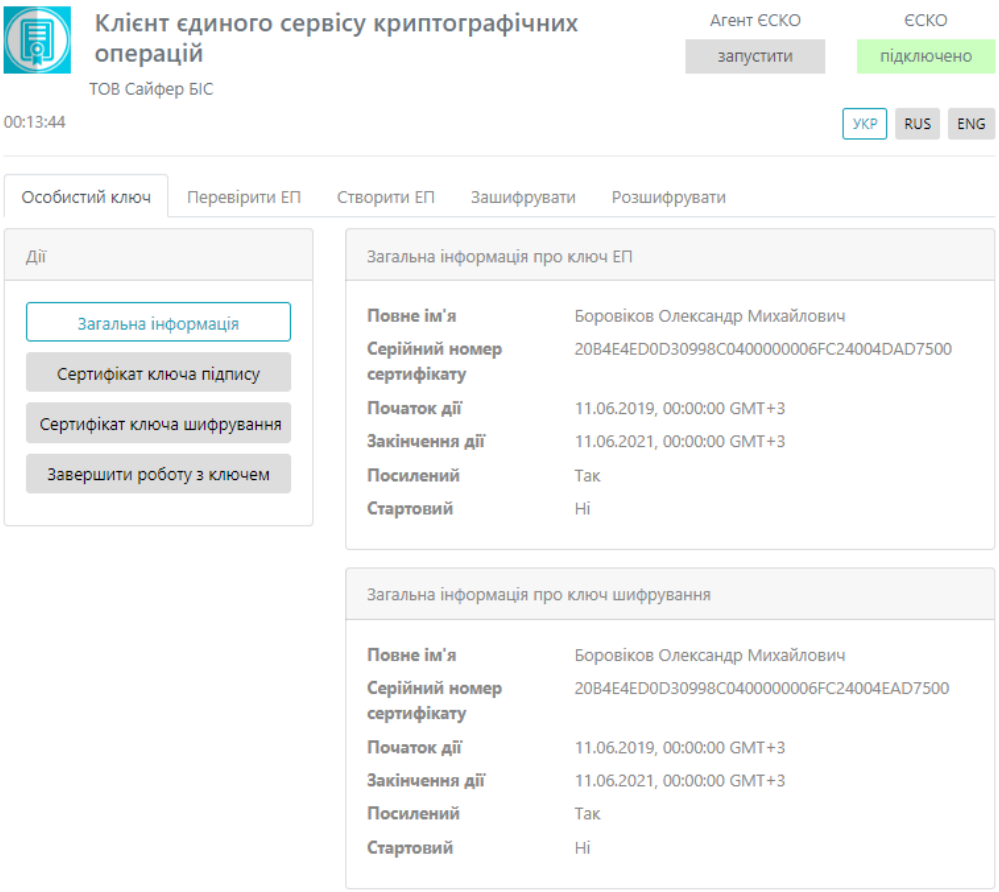

Рис. 4. Клієнт ЄСКО після завантаження даних ключового контейнеру

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: базовий (CAdES-BES) чи з повними даними для перевірки (CAdES-X Long).
- «Файл». Включає в себе поле:
  - Файл/файли для підпису (файл, який необхідно підписати).
- «Текстові дані». Включає в себе 2 поля:
  - Кодування UTF-16LE та UTF-8.
  - Текстові дані для підпису (текст, який необхідно підписати).
  - Додатковий опис (назва тексту 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 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. Час до кінця сесії – відлік у реальному часі до закінчення сесії (знаходиться у лівому верхньому куті).
7. Статус роботи програмного комплексу «Агенту ЄСКО» - знаходиться у правій верхній частині вікна. За допомогою «Агент ЄСКО» є можливість працювати не лише із файлами на диску, але із захищеними носіями.

Можливі статуси «Агенту ЄСКО»:

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

8. Статус роботи програмного комплексу «ЄСКО» - знаходиться у правій верхній частині вікна.

Можливі статуси ЄСКО:

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

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

Створення ЕП

Вкладка «Створення ЕП» містить розділи: Параметри створення ЕП, Файл та Текстові дані, Рис. 5.

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 створено ЕП).
2. Поле «Формат ЕП», яке містить:
   - CAdES-BES. Або «Базовий ЕП» використовується для автентифікації підписанта та перевірки цілісності електронного документа в період чинності сертифіката

відкритого ключа (сертифікат). Формат «Базовий ЕП» не надає можливості встановити дійсність підпису у випадку, якщо ЕП перевіряється після закінчення строку чинності сертифіката або скасування сертифіката після формування ЕП;
- CAdES-X Long. Або «З повними даними для перевірки» можливість встановлення дійсності ЕП у довгостроковому періоді (після закінчення строку чинності сертифікату).

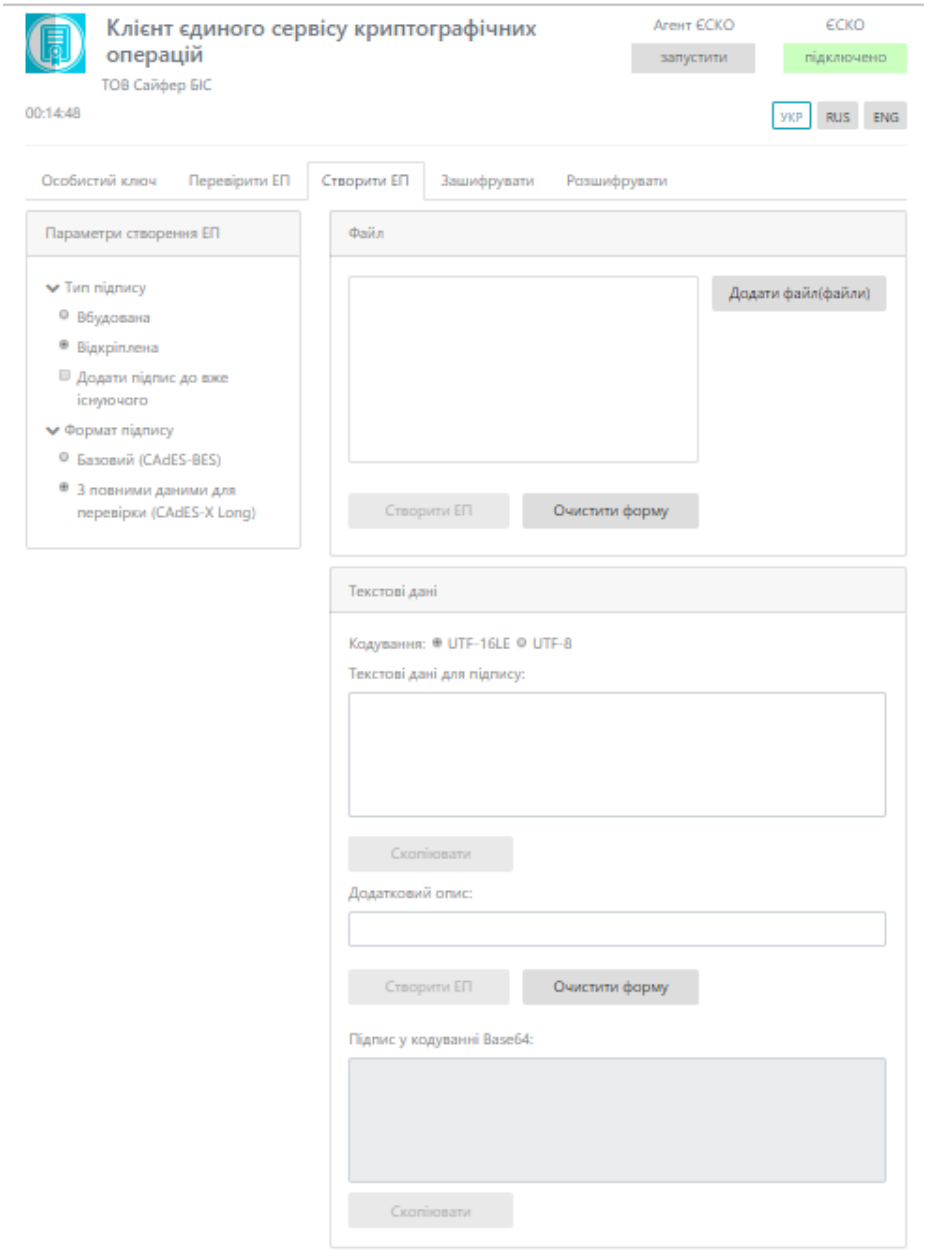

Рис. 5. Вкладка «Створення ЕП»

Розділ «Файл», який у свою чергу включає:

- Файл (натискаємо кнопку «Додати файл(файли)» та обираємо необхідний файл(файли) для підпису);
- Кнопка «Створити ЕП» (здійснює створення 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 створення ЕП на текстові дані, які 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 файли

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Вбудована» та Формат ЕП (CAdES-BES чи CAdES-X Long), обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 6. За необхідності можна видалити файл натиснувши відповідну кнопку та додати ще, але слід зауважити, що максимальний об'єм всіх файлів не повинен перевищувати 100Мб.

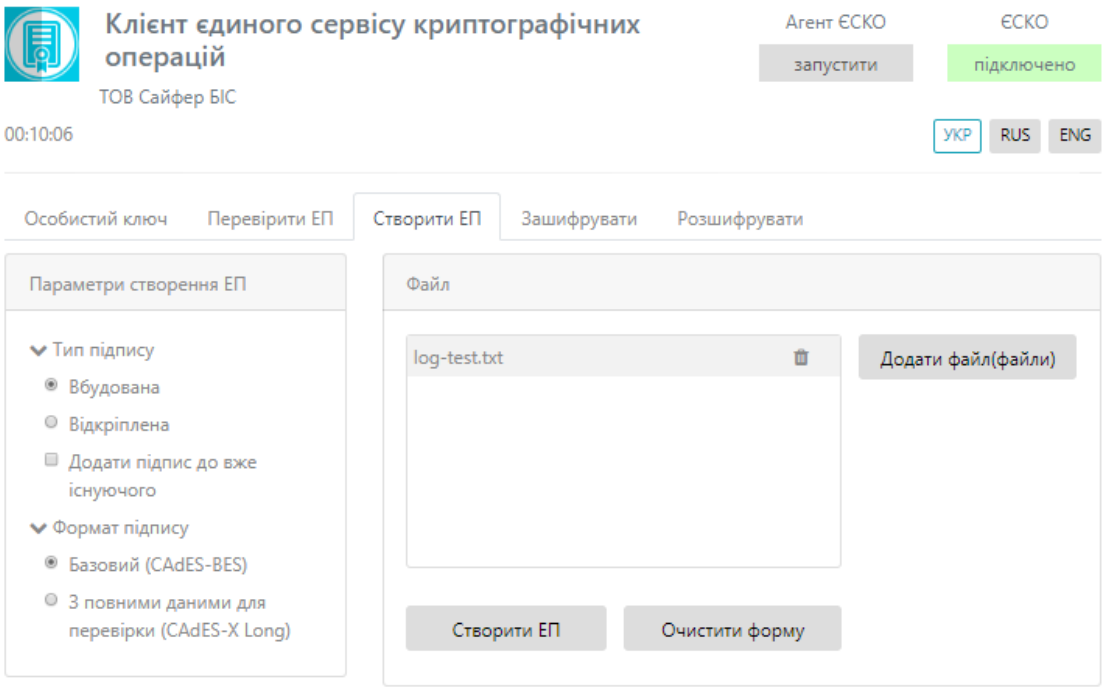

Рис. 6. Створення ЕП

Після натискання з'являється вікно про успішне створення електронного підпису, Рис. 7.

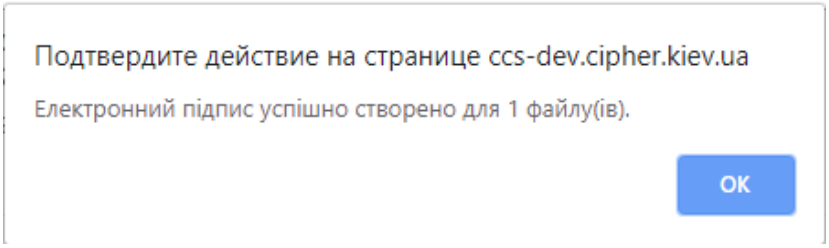

Рис. 7. Повідомлення про створення електронного підпису

Далі за допомогою «стрілки вниз», яка розташована напроти кожного файлу дає змогу зберегти файл, Рис. 8.

Далі за необхідності обираємо шлях для збереження файлу та очищаємо форму.

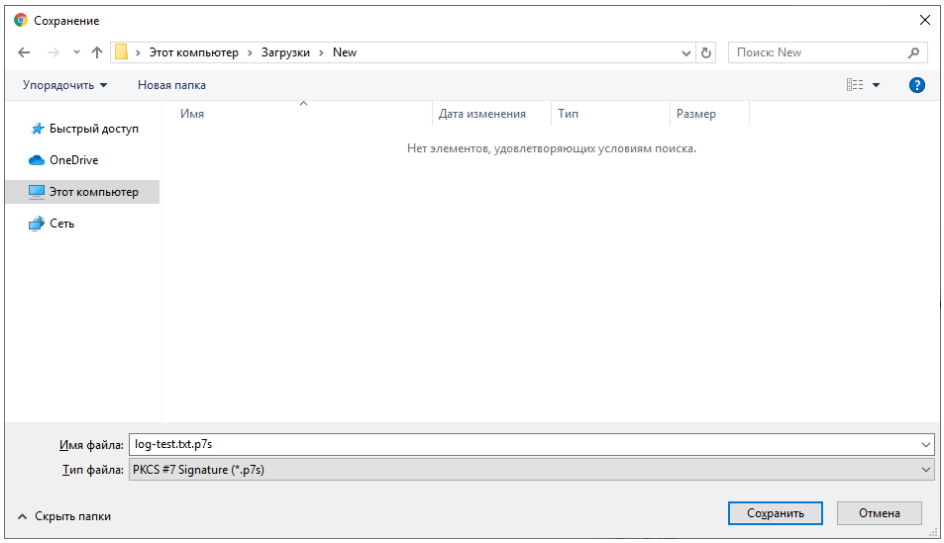

Рис. 8. Збереження підпису у файл

Створення ЕП за типом «Відкріплена» на файли

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. 9. За необхідності можна видалити файл натиснувши відповідну кнопку та додати ще, але слід зауважити, що максимальний об’єм всіх файлів не повинен перевищувати 100Мб.

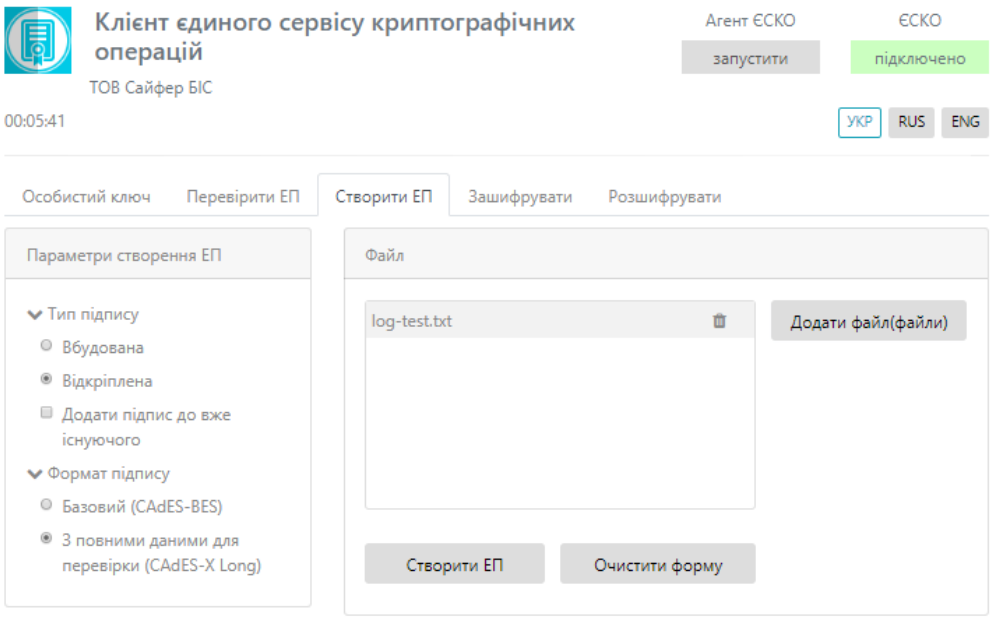

Рис. 9. Створення ЕП

Після натискання з’являється вікно про успішне створення електронного підпису, Рис. 10.

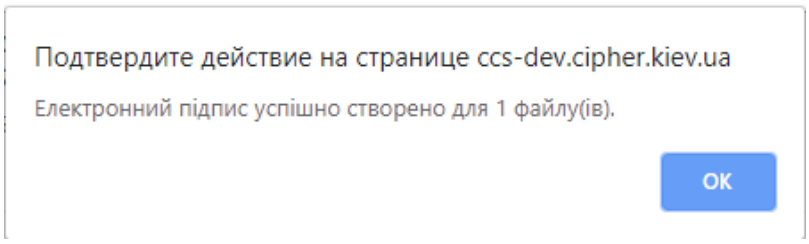

Рис. 10. Повідомлення про створення електронного підпису

Далі за допомогою «стрілки вниз», яка розташована напроти кожного файлу дає змогу зберегти файл, Рис. 11. Далі за необхідності обираємо шлях для збереження файлу та очищаємо форму.

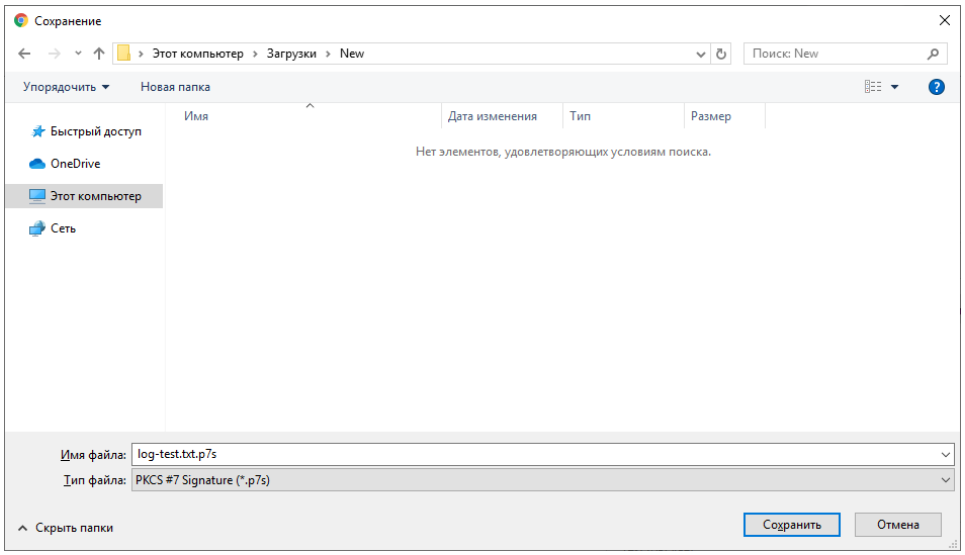

Рис. 11. Збереження підпису у файл

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-BES чи CAdES-X Long), тип кодування, вказується текст для підпису, натискаємо кнопку «Створити ЕП», Рис. 12.

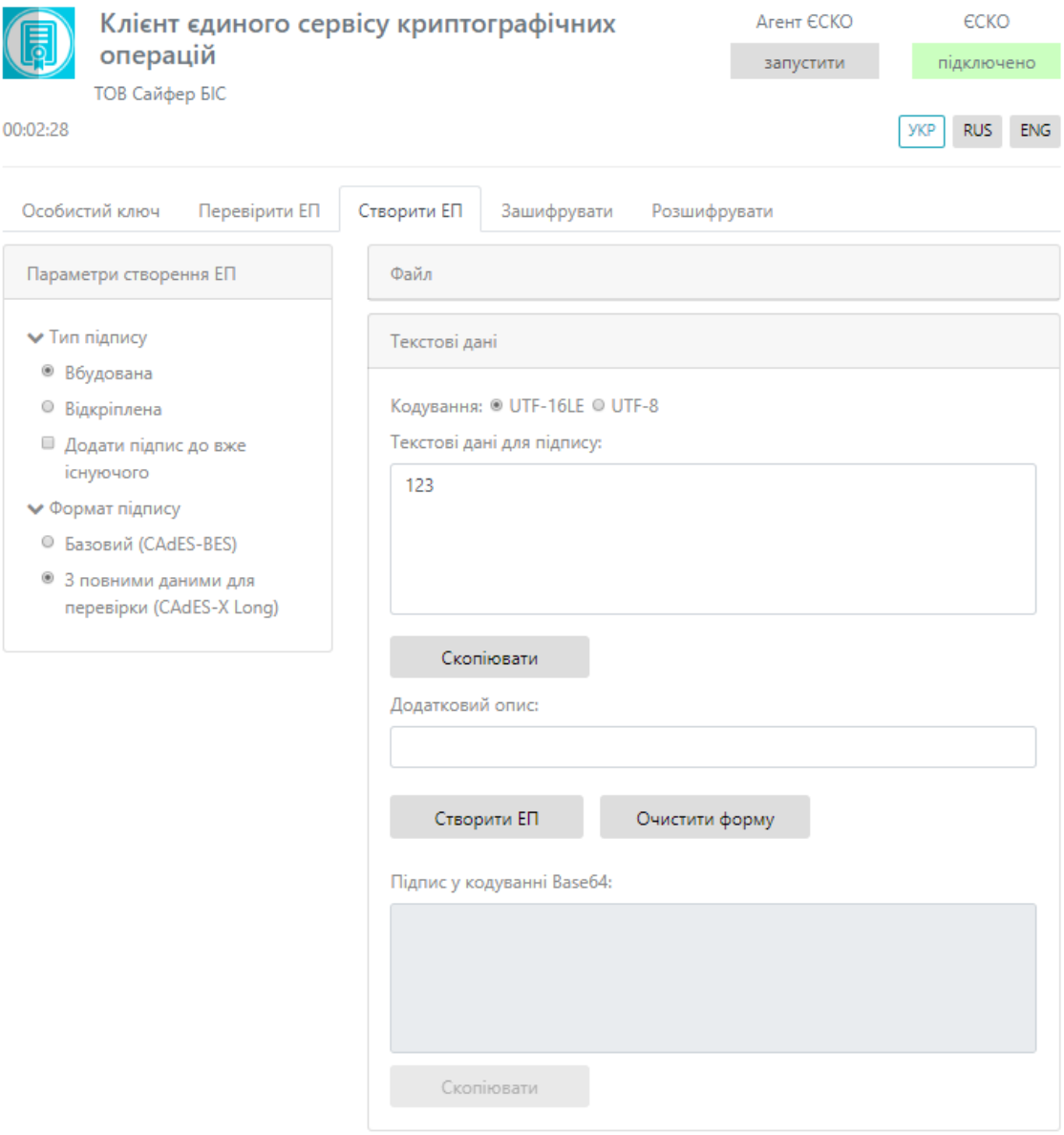

Рис. 12. Створити ЕП

Після натискання з’являється вікно про успішне створення електронного підпису, Рис. 13.

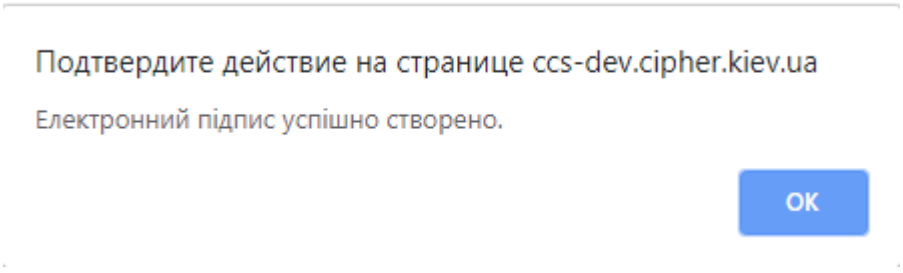

Рис. 13. Повідомлення про створення електронного підпису

Далі у полі «Підпис у кодуванні Base64» з’являється текст з підписом, Рис. 14, далі за необхідності очищаємо форму.

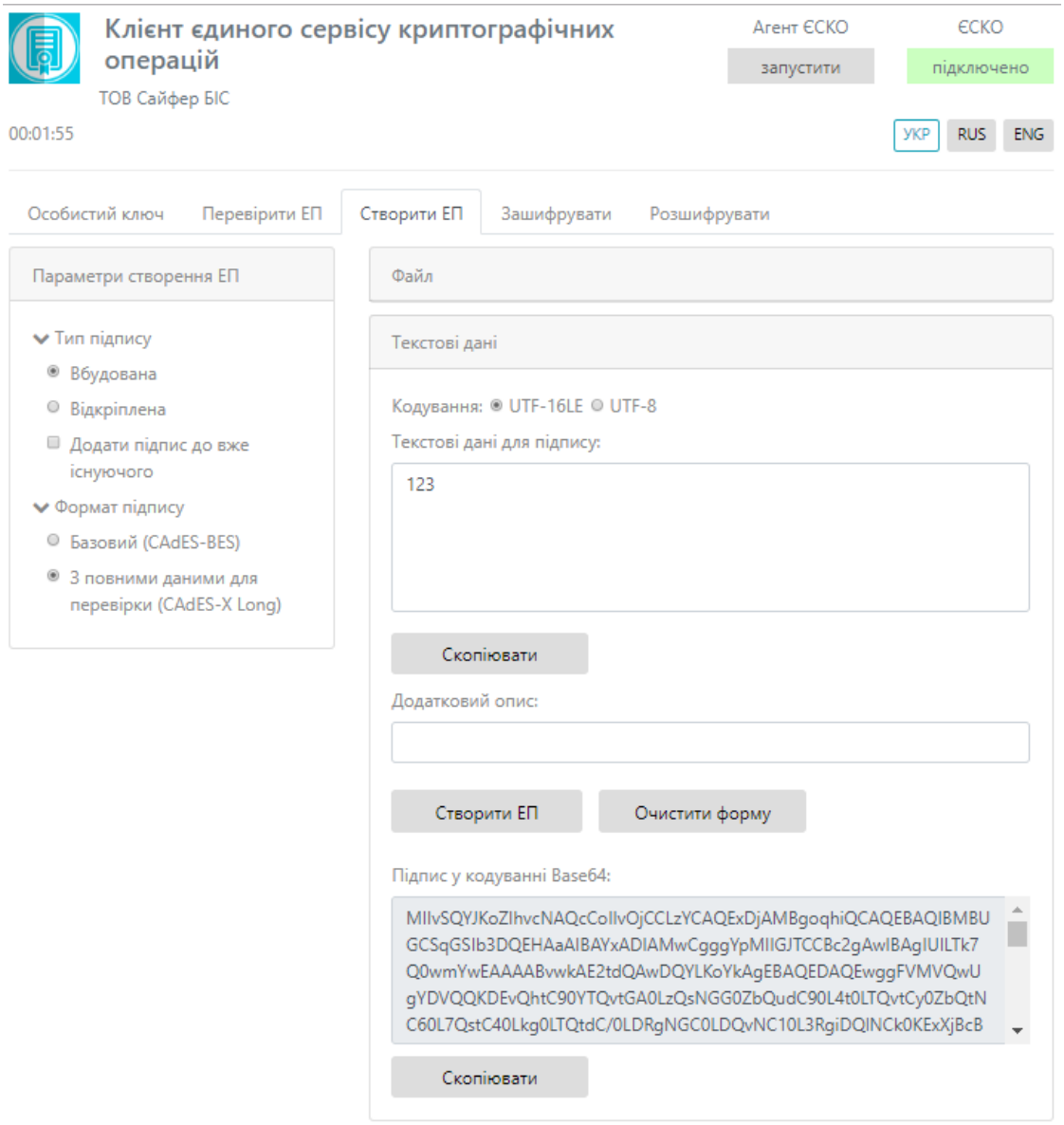

Рис. 14. Результат підпису тестових даних

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-BES чи CAdES-X Long), обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 15.

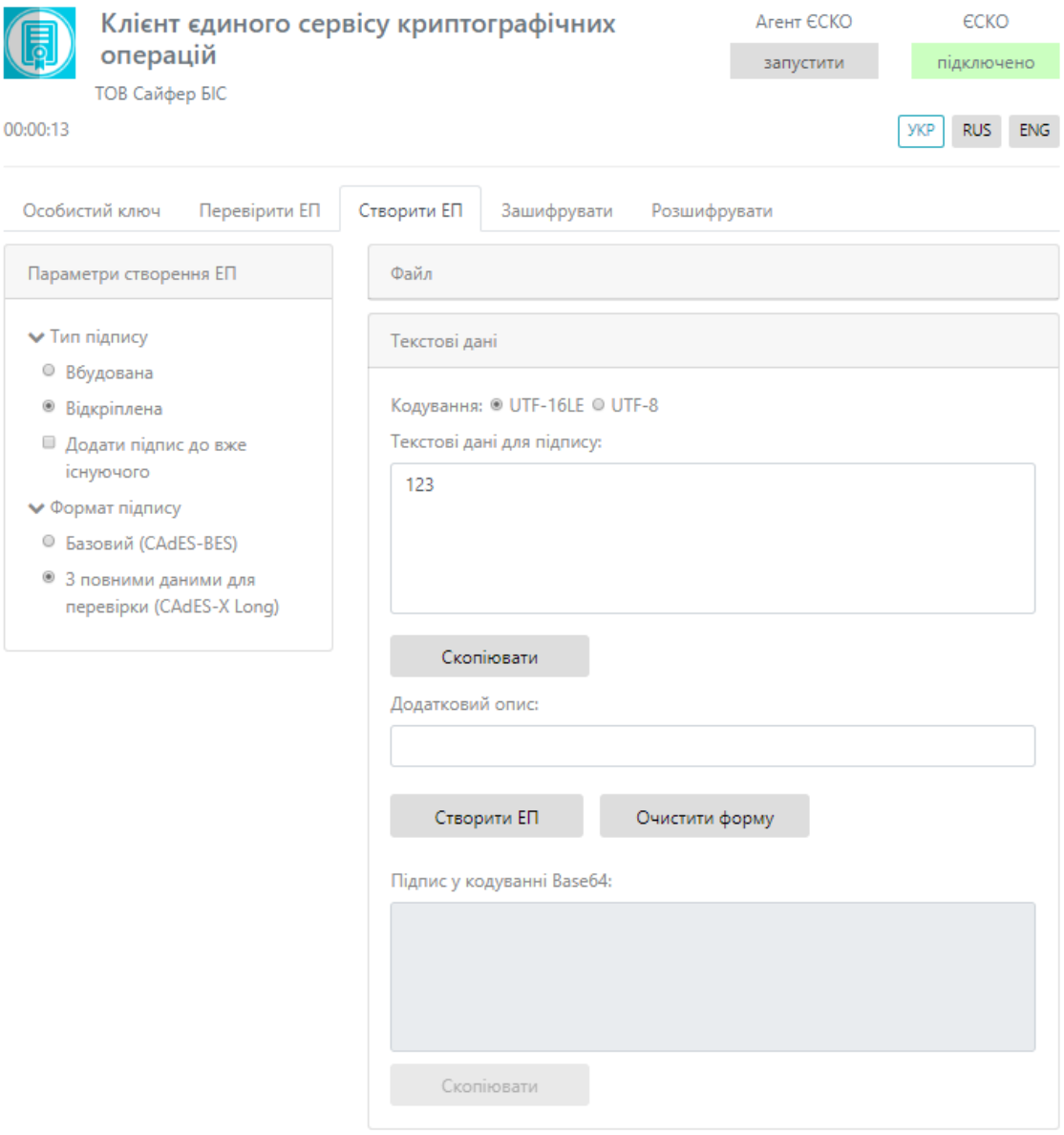

Рис. 15. Створити ЕП

Після натискання з’являється вікно про успішне створення електронного підпису, Рис. 16.

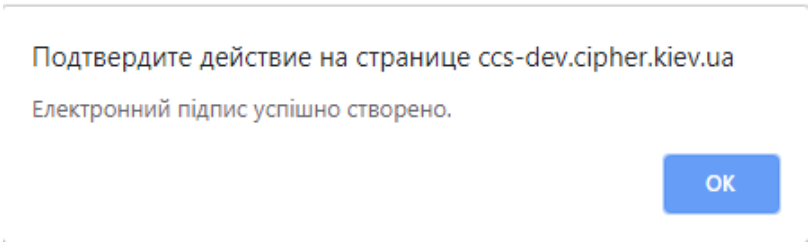

Рис. 16. Повідомлення про створення електронного підпису

Далі у полі «Підпис у кодуванні Base64» з’являється текст з підписом, Рис. 17. Далі за необхідності очищаємо форму.

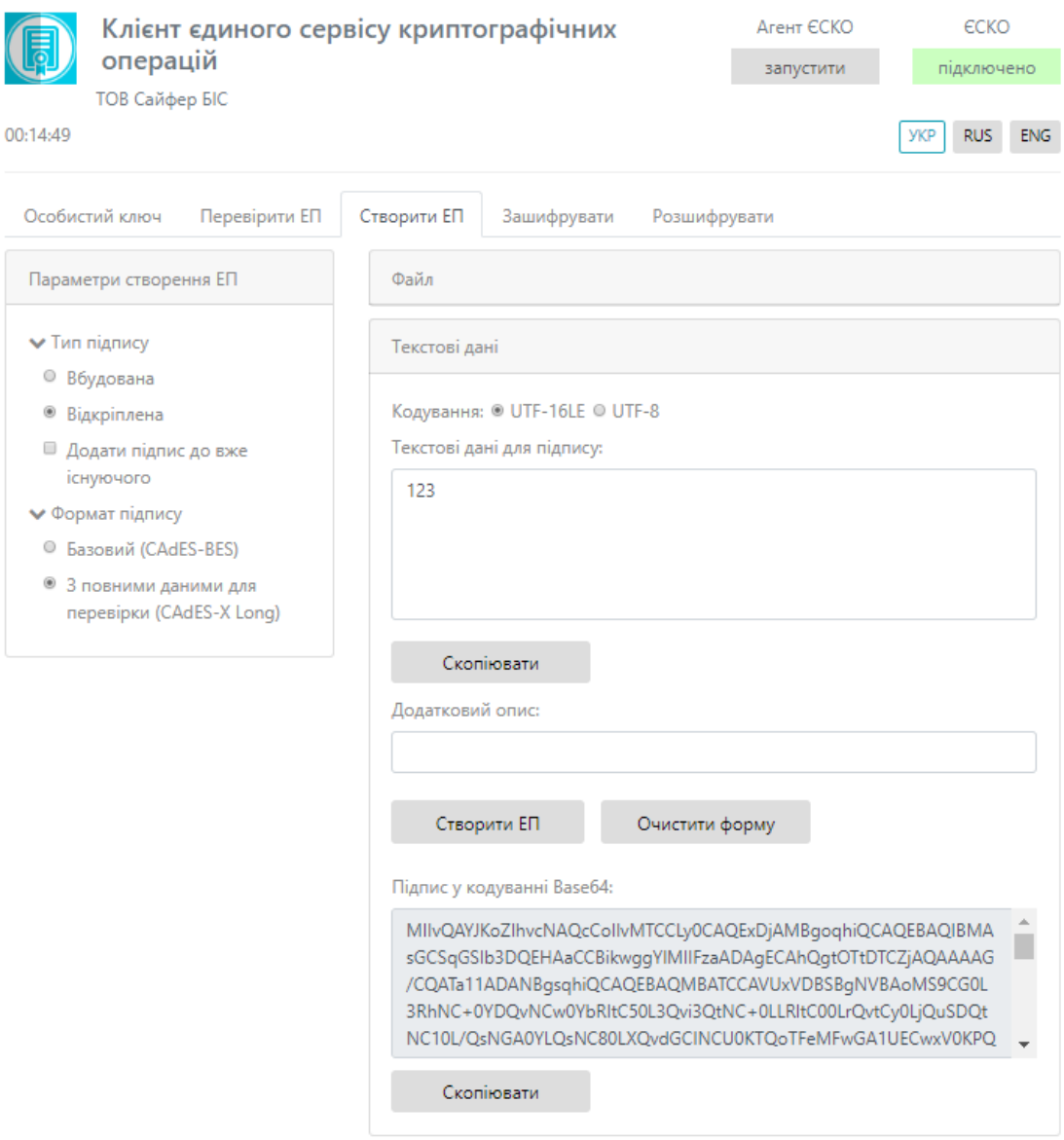

Рис. 17. Результат підпису тестових даних

Перевірка ЕП

Дана функція є доступною і без ключа.

Вкладка «Перевірити ЕП» містить розділи: Параметри перевірки ЕП, Текстові дані та Файл, Рис. 18-Рис. 19.

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

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

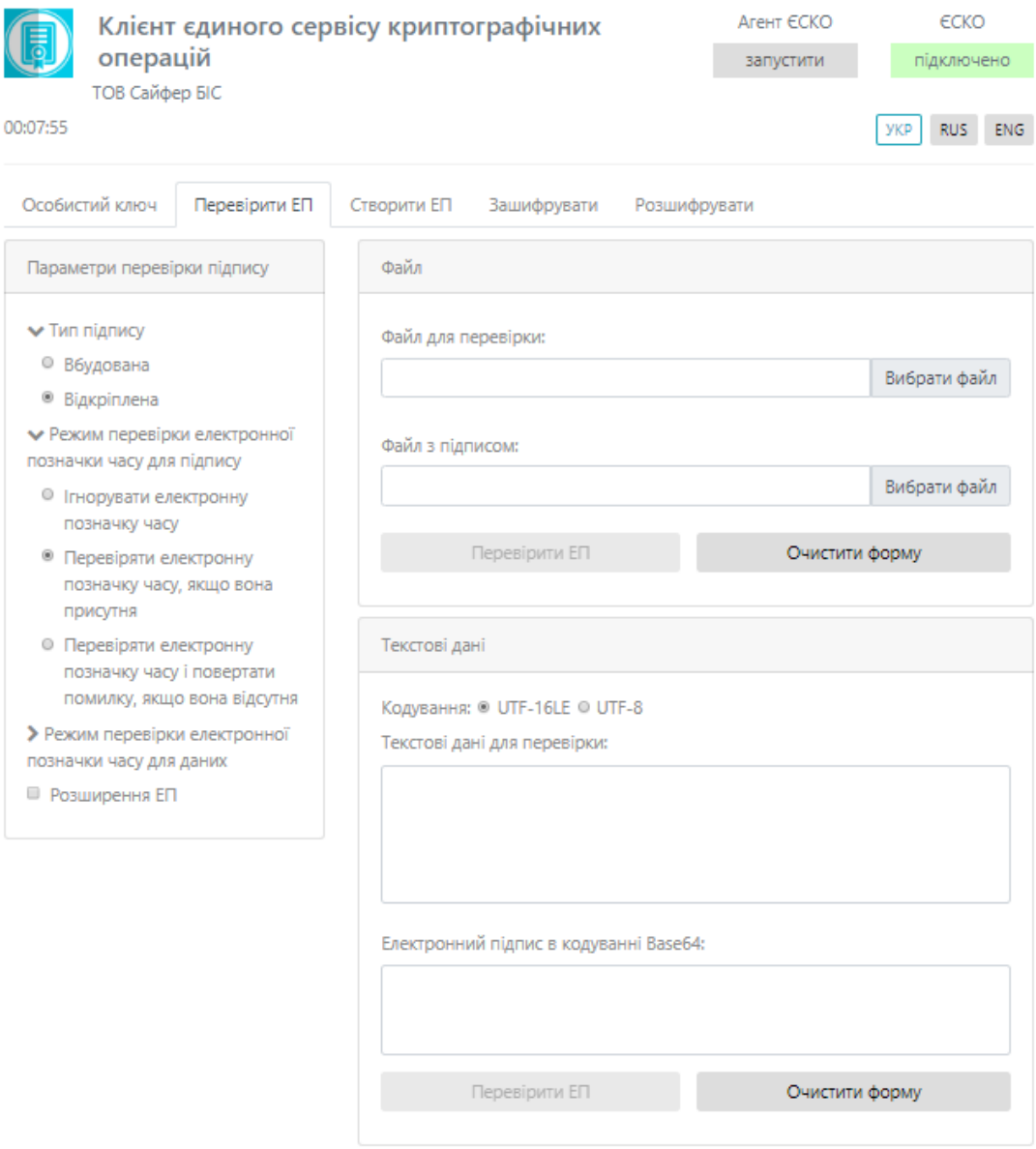

Рис. 18. Вкладка «Перевірити ЕП»

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.

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.

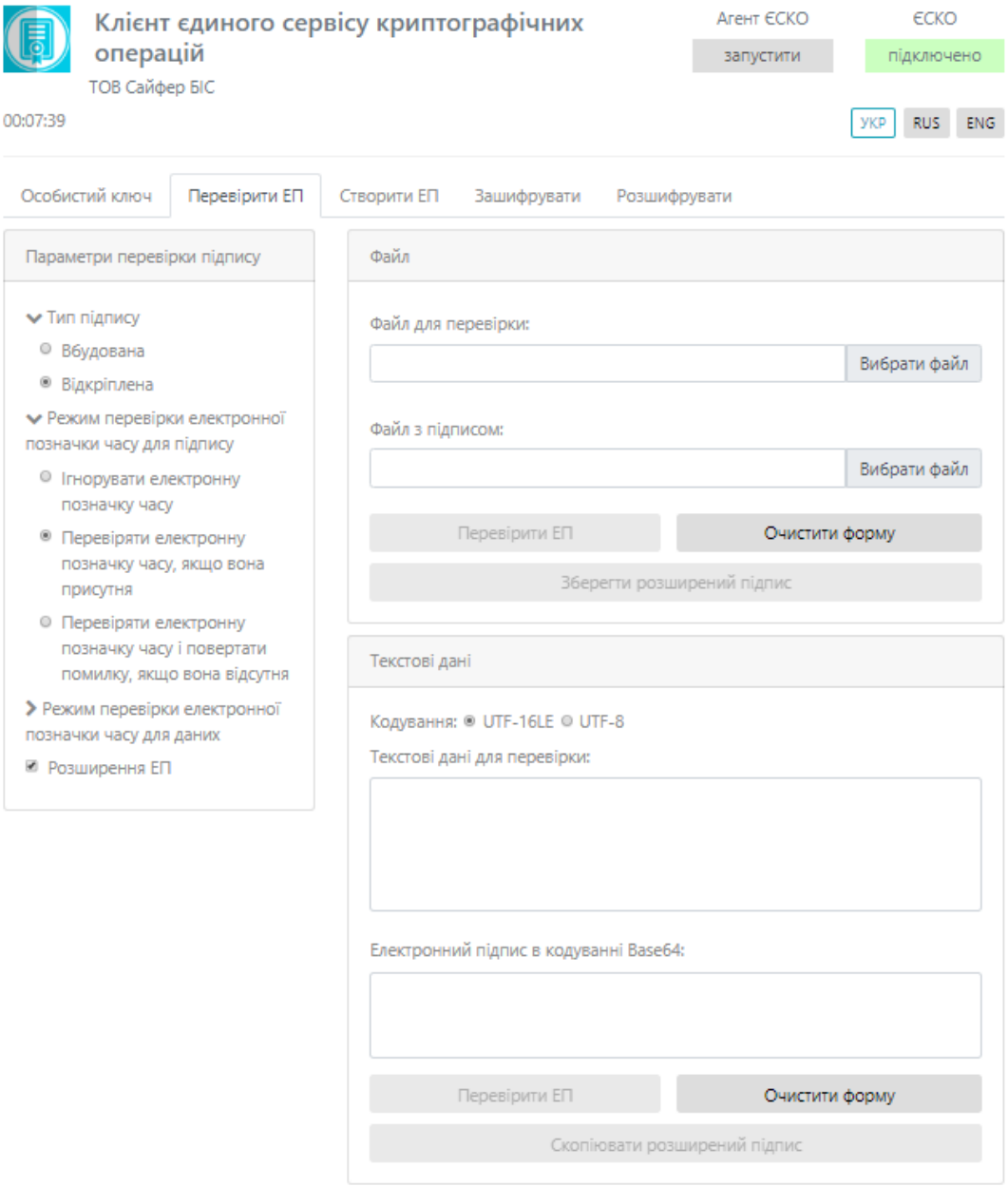

Рис. 19. Вкладка «Перевірити ЕП» зі вказівкою позначки «Розширення ЕП»

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 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.

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 з підписом/тест з підписом, натискаємо кнопку «Перевірити ЕП». За необхідності можна змінити файл/текст.

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. 20.

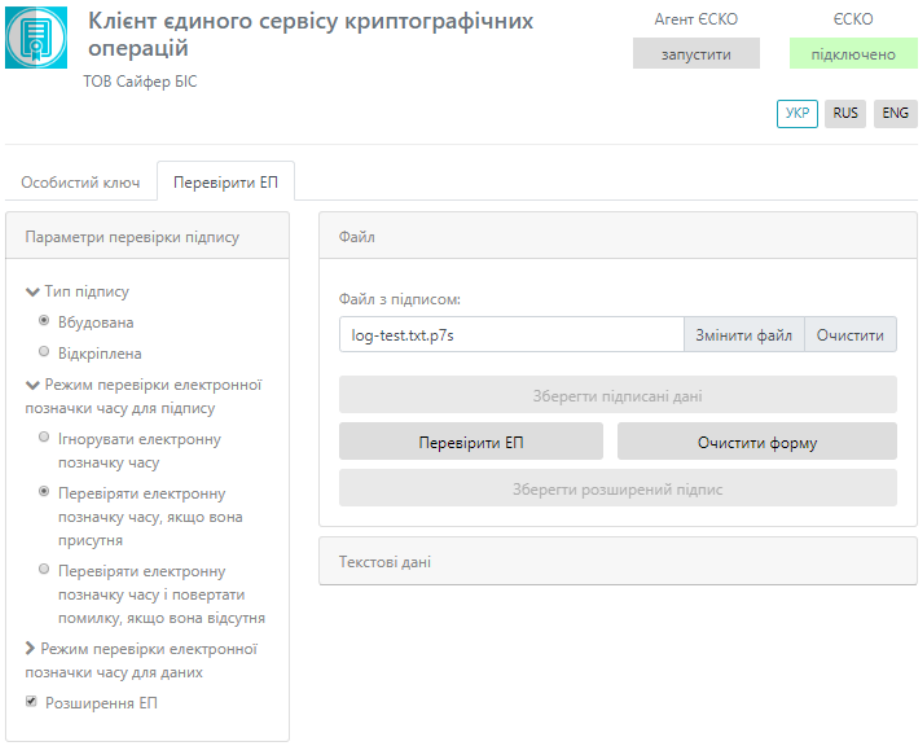

Рис. 20. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з’являється повідомлення з результатами перевірки електронного підпису, Рис. 21.

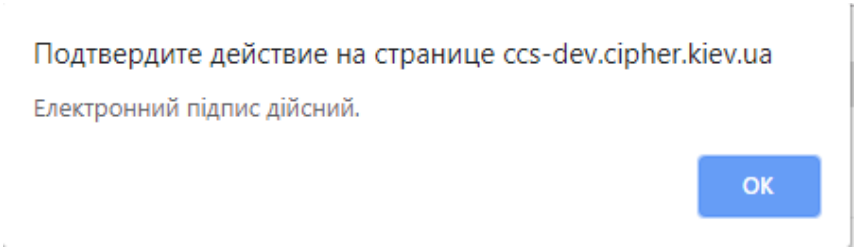

Рис. 21. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з’являється інформація про дійсність підпису, вказується інформація про підписанта та дату підпису, Рис. 22. За необхідності зберегти первинні дані (без підпису), натиснувши на кнопку «Зберегти підписані дані». Після чого, натискаємо кнопку «Очистити форму».

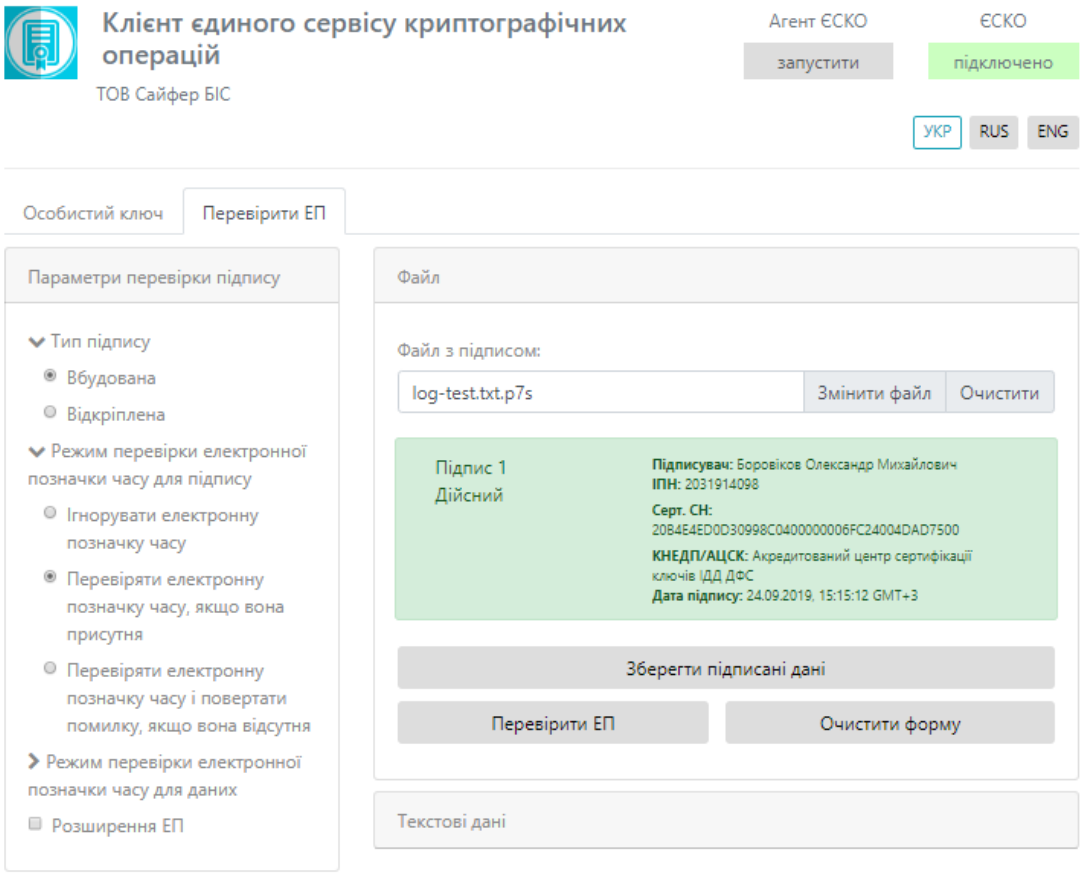

Рис. 22. Результат перевірки

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. 23Рис. 20.

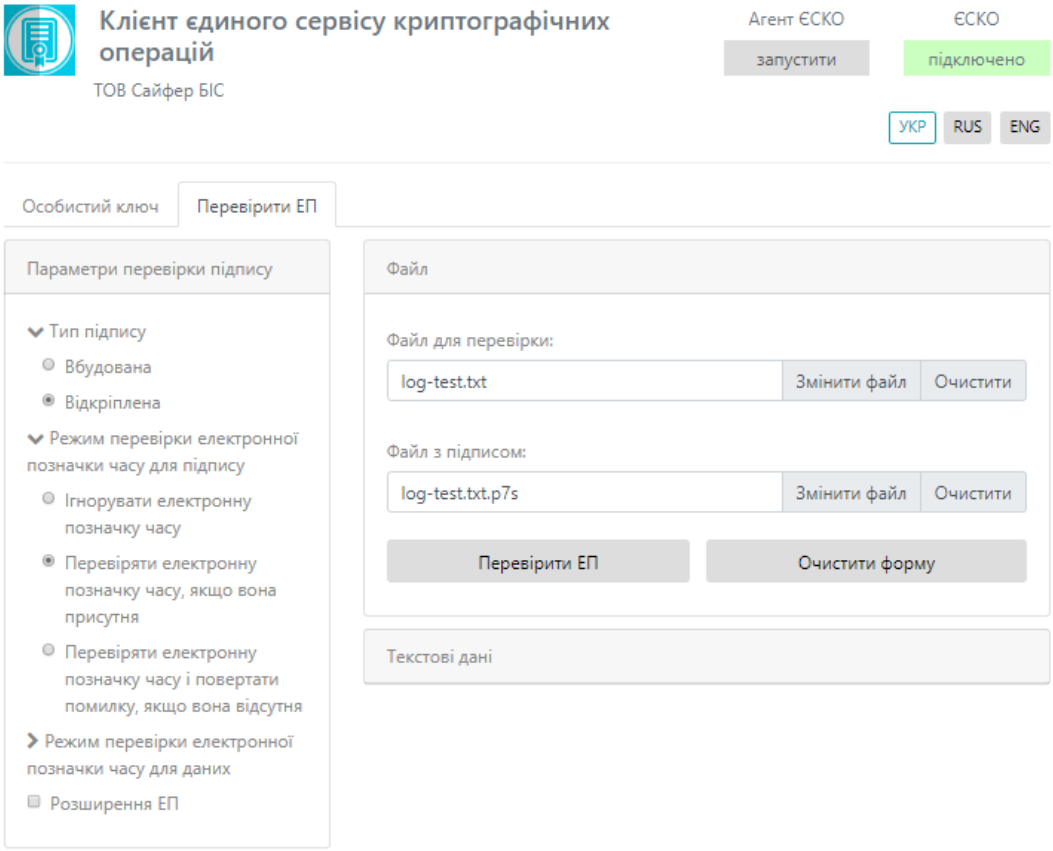

Рис. 23. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 24.

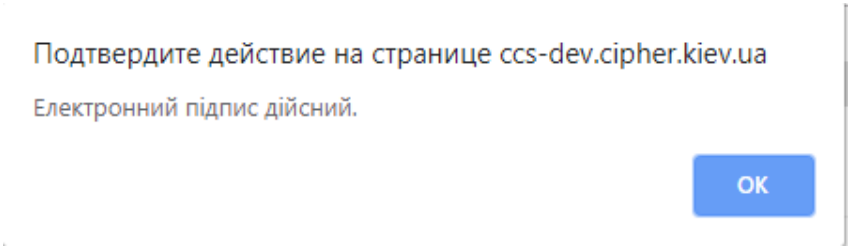

Рис. 24. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дата підпису, Рис. 25. Після чого, натискаємо кнопку «Очистити форму».

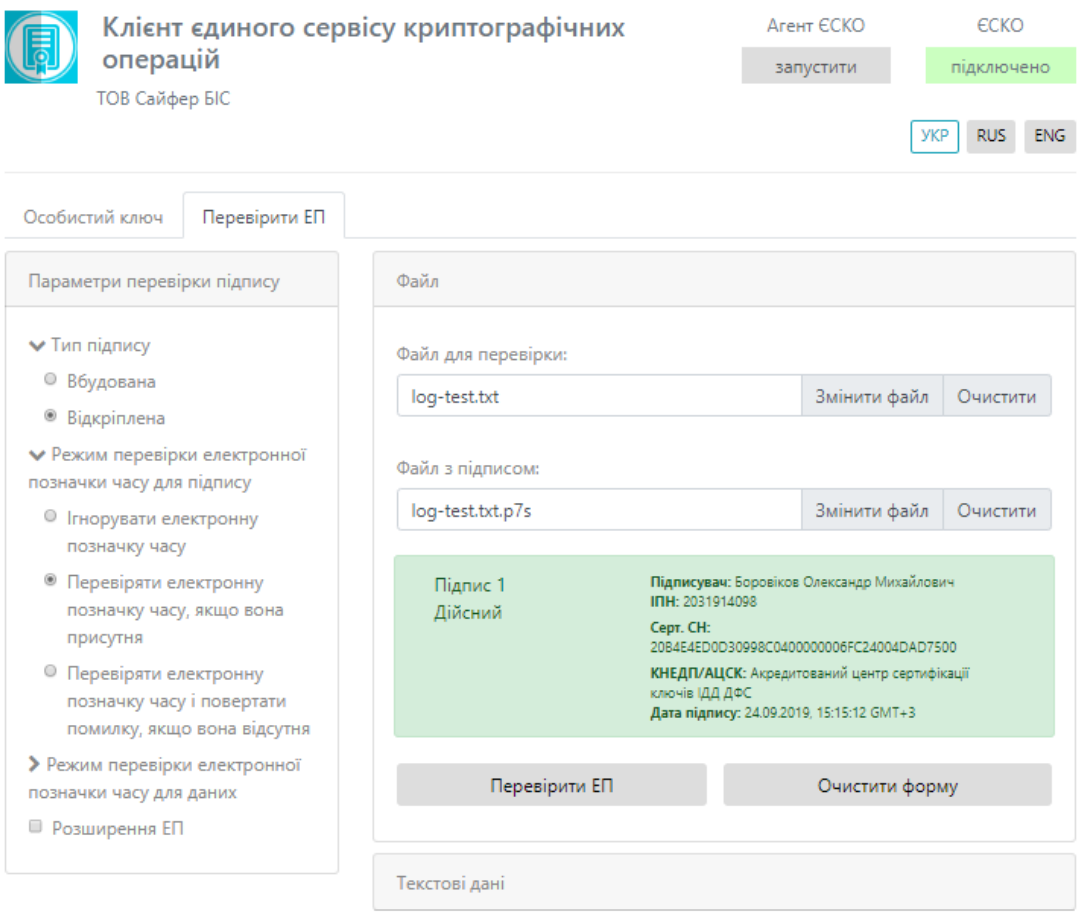

Рис. 25. Результат перевірки

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. 26.

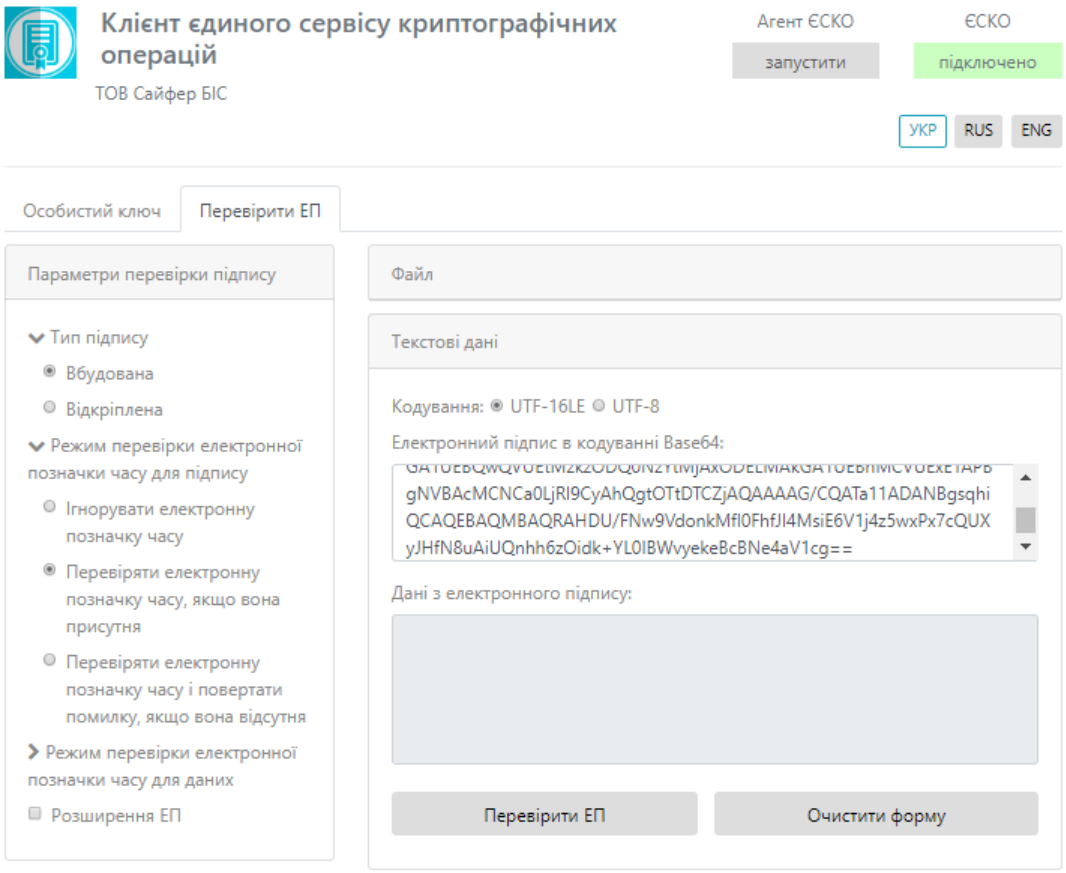

Рис. 26. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з’являється повідомлення з результатами перевірки електронного підпису, Рис. 27.

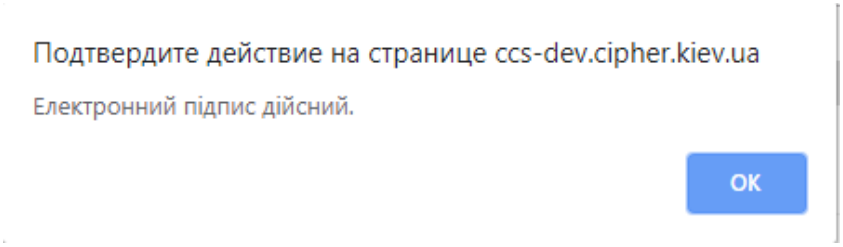

Рис. 27. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з’являється інформація про дійсність підпису, вказується інформація про підписанта та дату підпису, Рис. 28. Після чого, натискаємо кнопку «Очистити форму».

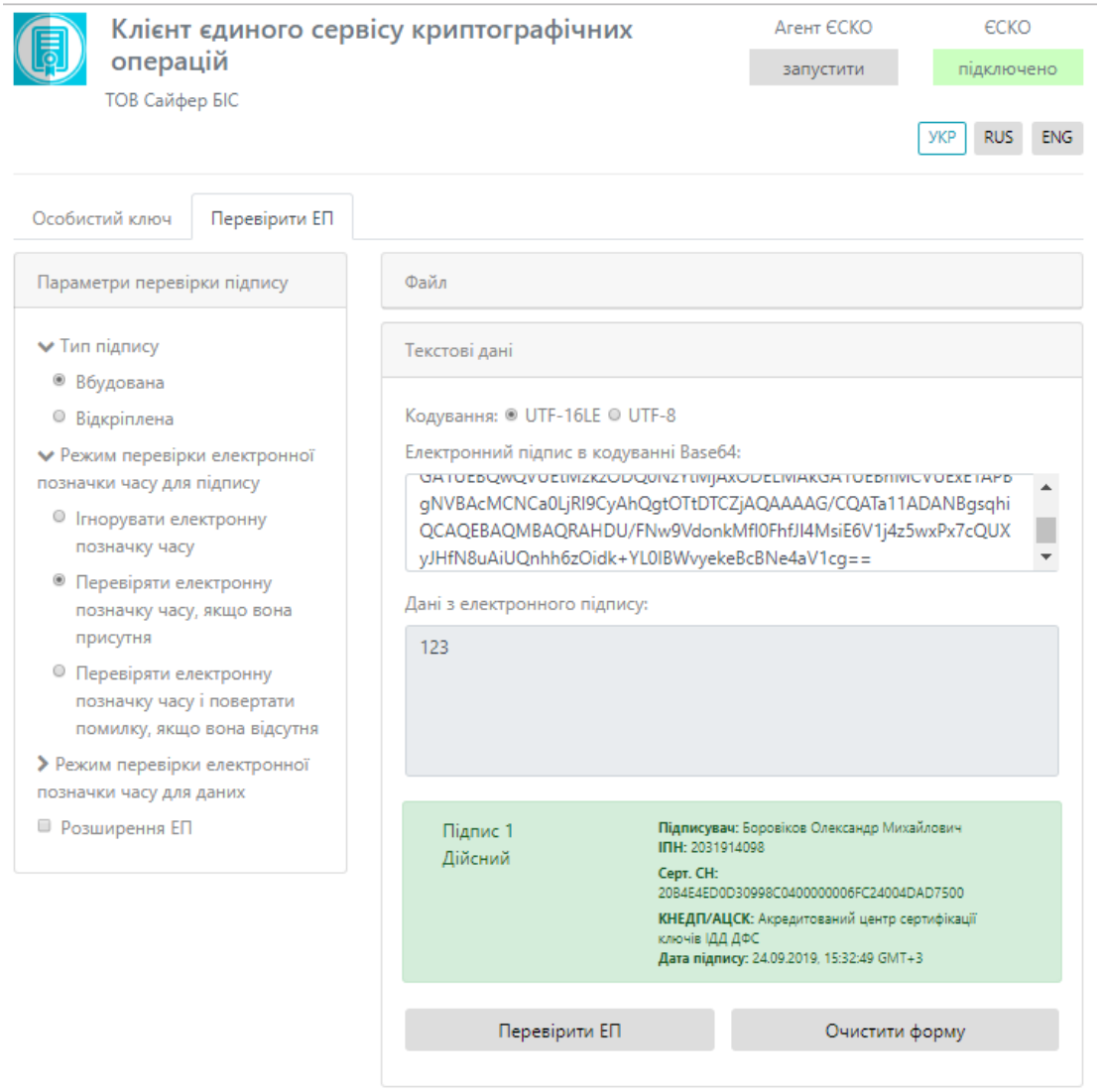

Рис. 28. Результат перевірки

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. 29.

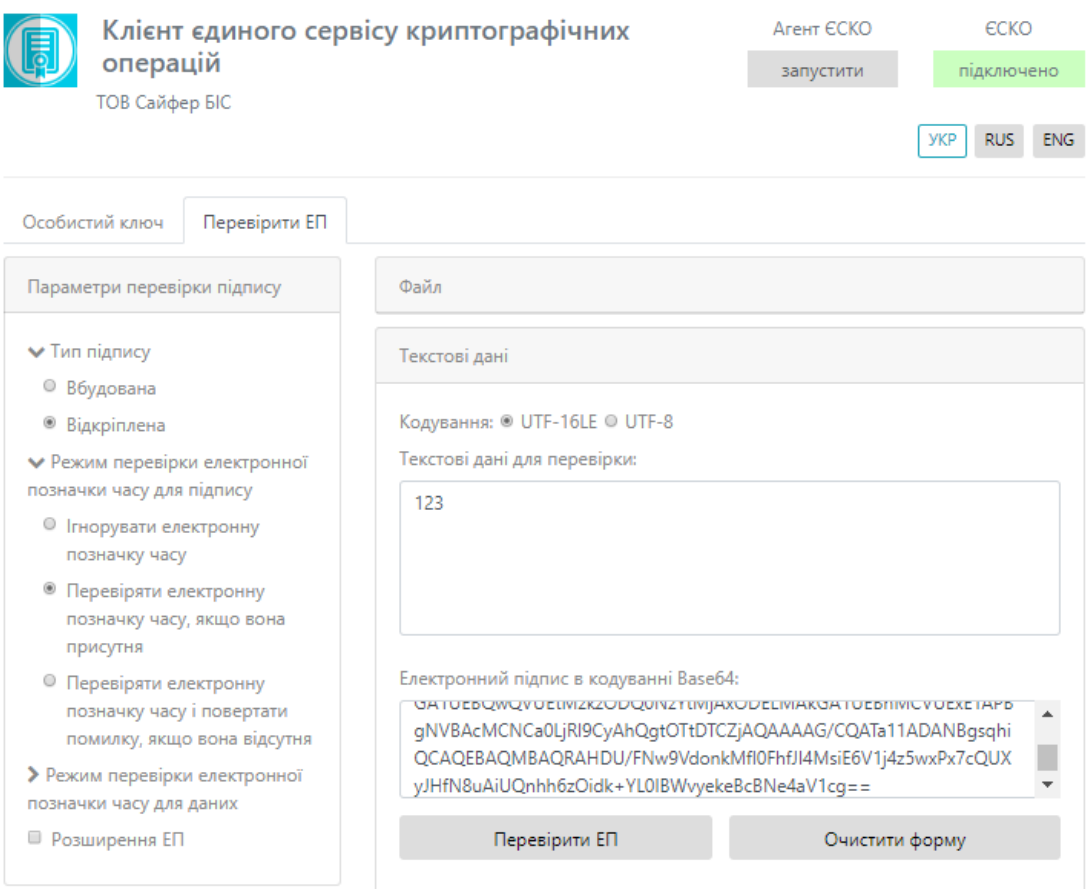

Рис. 29. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з’являється повідомлення з результатами перевірки електронного підпису, Рис. 30.

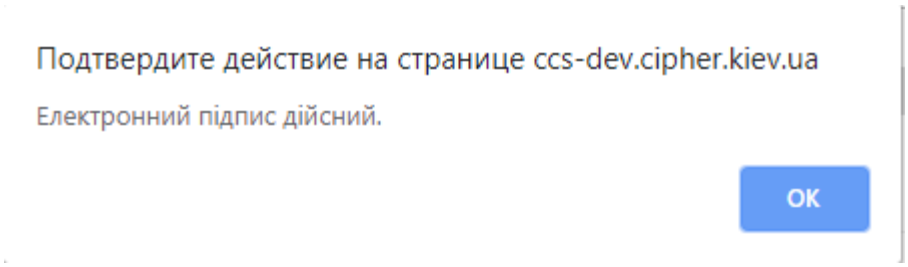

Рис. 30. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з’являється інформація про дійсність підпису, вказується інформація про підписанта та дата підпису, Рис. 31. Після чого, натискаємо кнопку «Очистити форму».

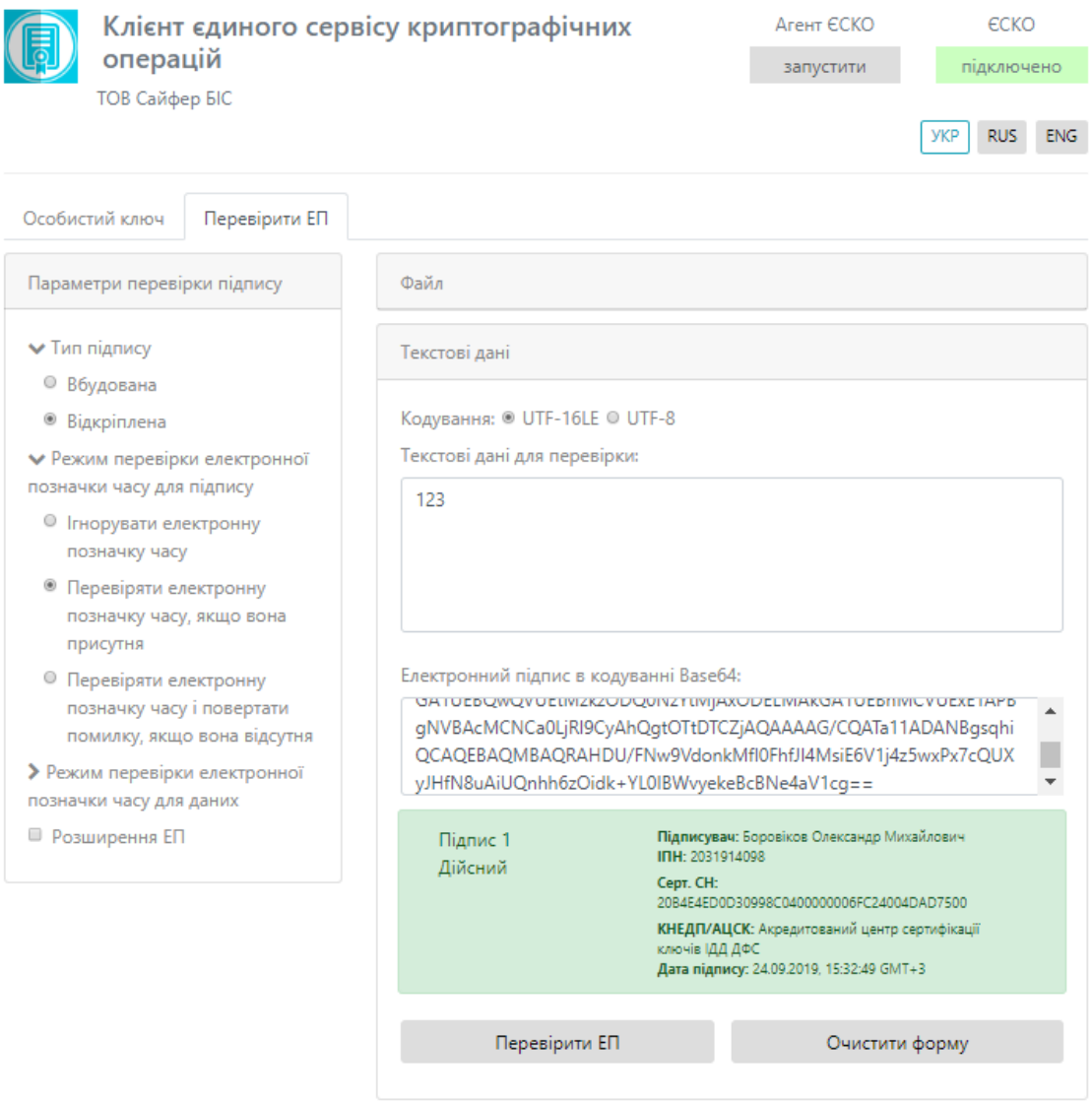

Рис. 31. Результат перевірки

Розширення ЕП

Вкладка «Перевірити ЕП» містить додаткову позначку «Розширити ЕП», при її вказівці, зовнішній вигляд сторінки видозмінюється та стають доступні нові кнопки, Рис. 32.

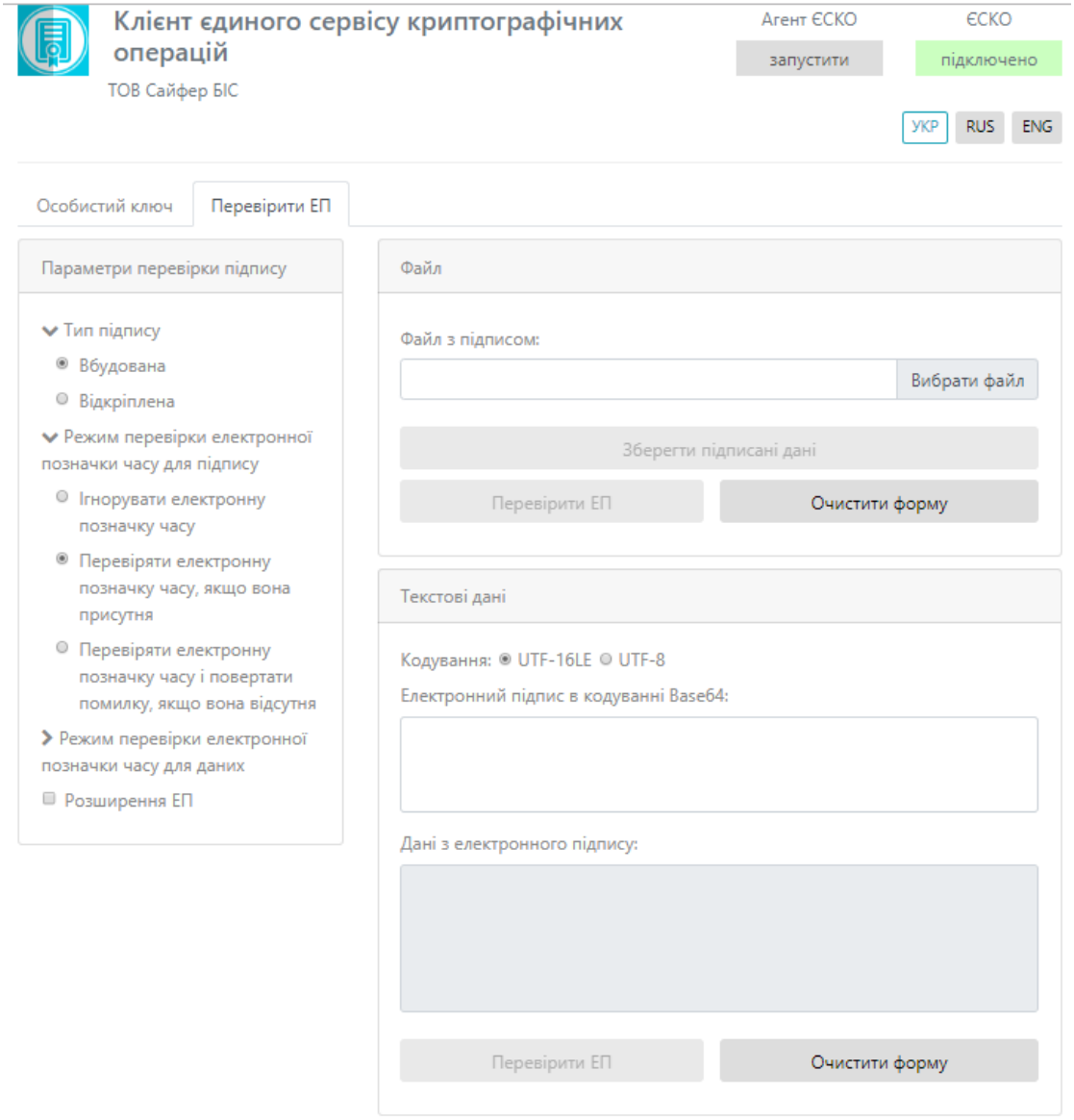

Рис. 32. Вкладка «Перевірити ЕП» з позначкою «Розширення ЕП»

Розширення ЕП для файлу

Відеоінструкція знаходиться за посиланням.

На прикладі вбудованого електронного підпису, який отримано раніше. Слід обрати файл та натиснути кнопку «Перевірити ЕП», Рис. 33.

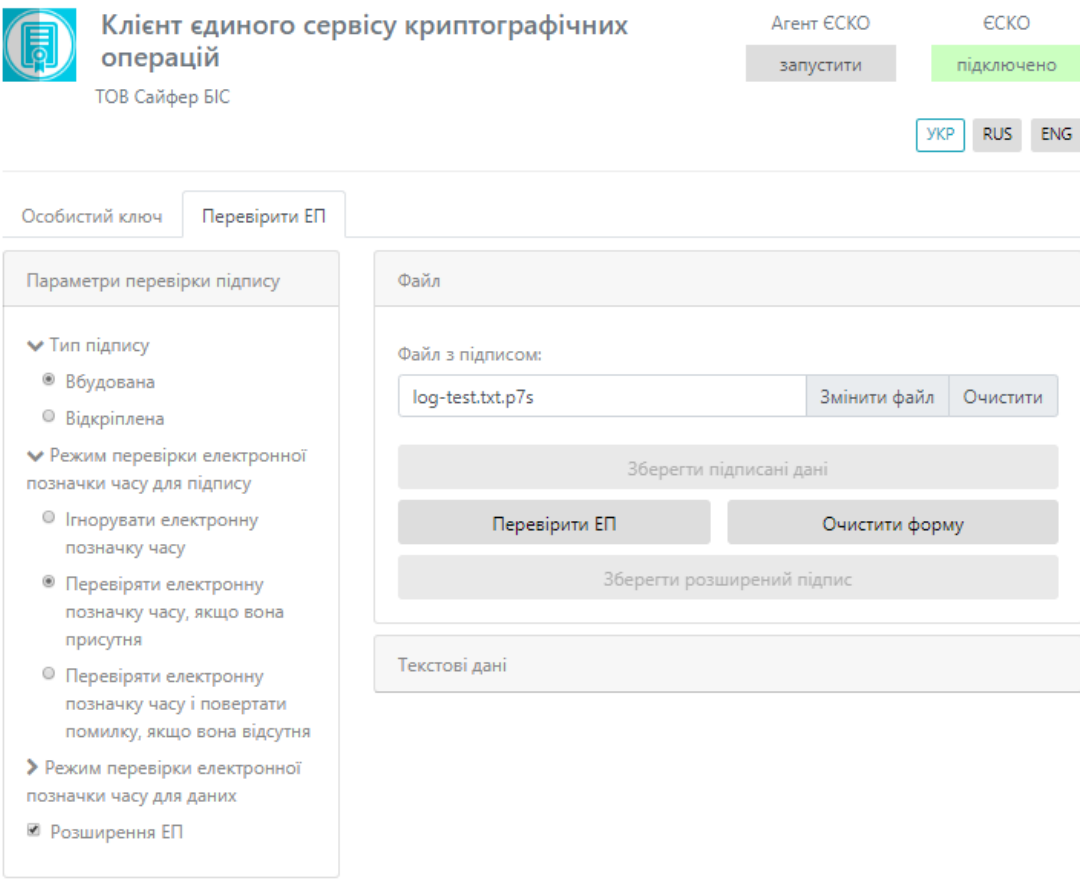

Рис. 33. Розширення вбудованого ЕП

Отримати повідомлення про успішне розширення підпису, Рис. 34.

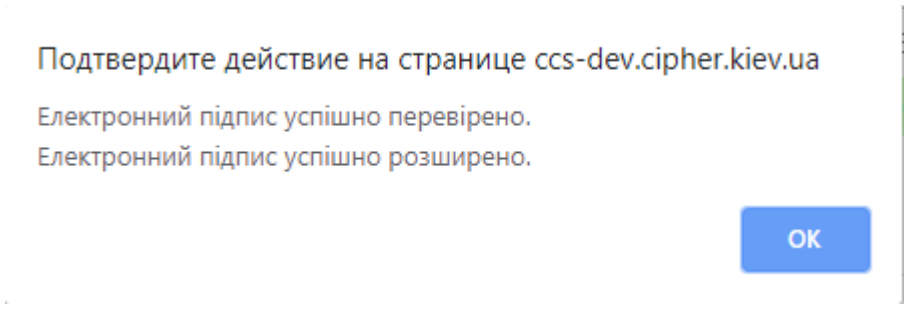

Рис. 34. Повідомлення про результат перевірки та розширення ЕП

Отримати результат перевірки електронного підпису та зберегти файл натиснувши відповідну кнопку, Рис. 35.

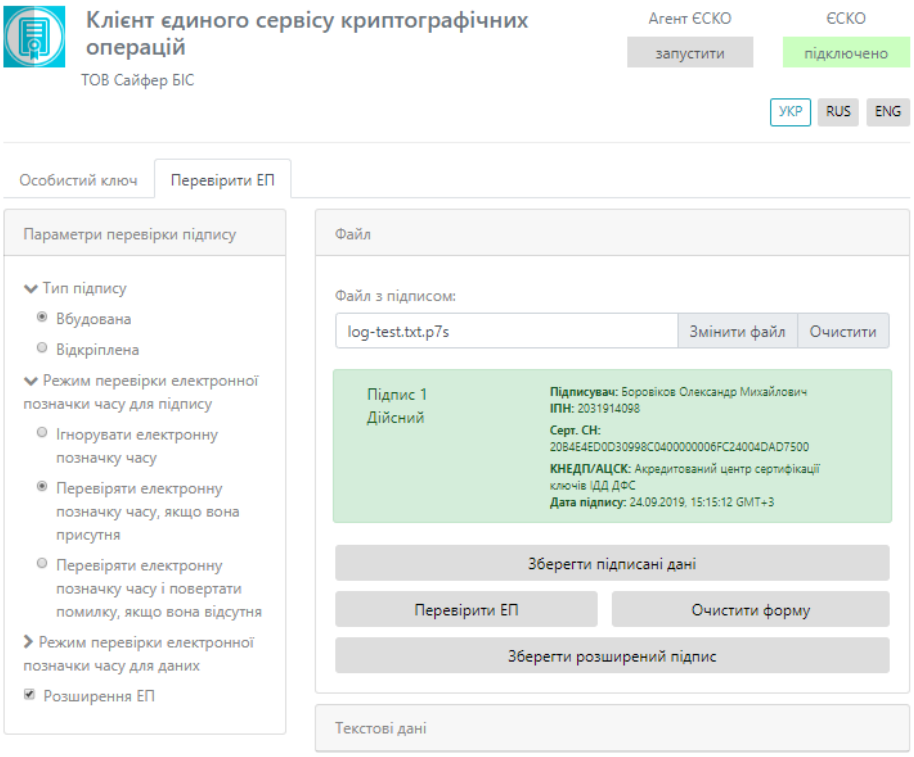

Рис. 35. Розширення вбудованого ЕП

За умови, якщо було завантажено файл вже з повними даними для перевірки, то з’явиться повідомлення про це, Рис. 36.

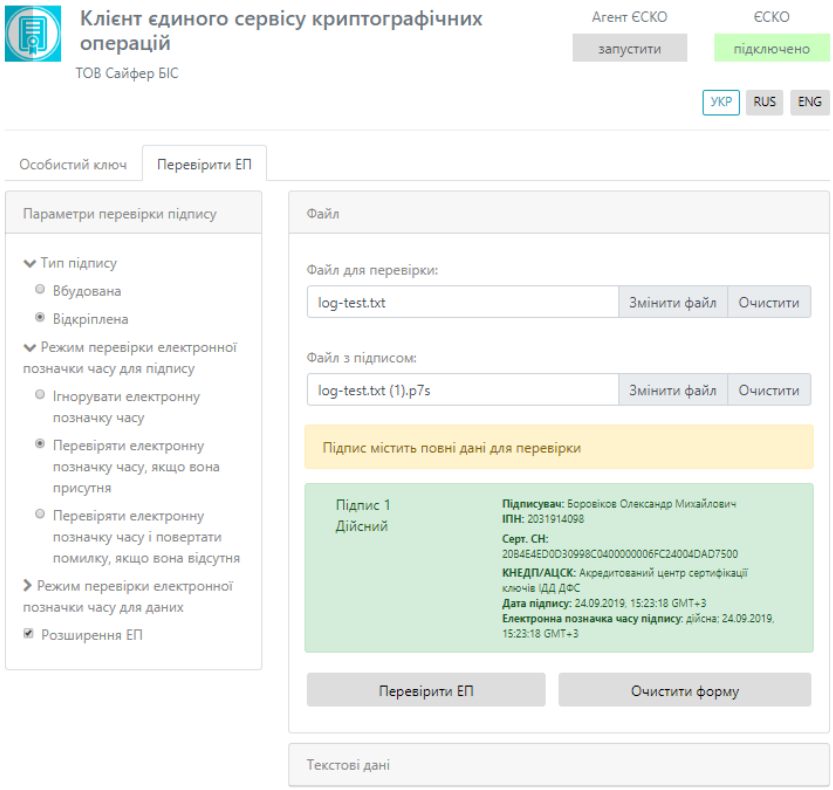

Рис. 36. Результати розширення підпису з повними даними для перевірки

Розширення ЕП для текстових даних

Відеоінструкція знаходиться за посиланням.

На прикладі відкріпленого електронного підпису, який отримано раніше. Слід вказати підписані дані та натиснути кнопку «Перевірити ЕП», Рис. 37.

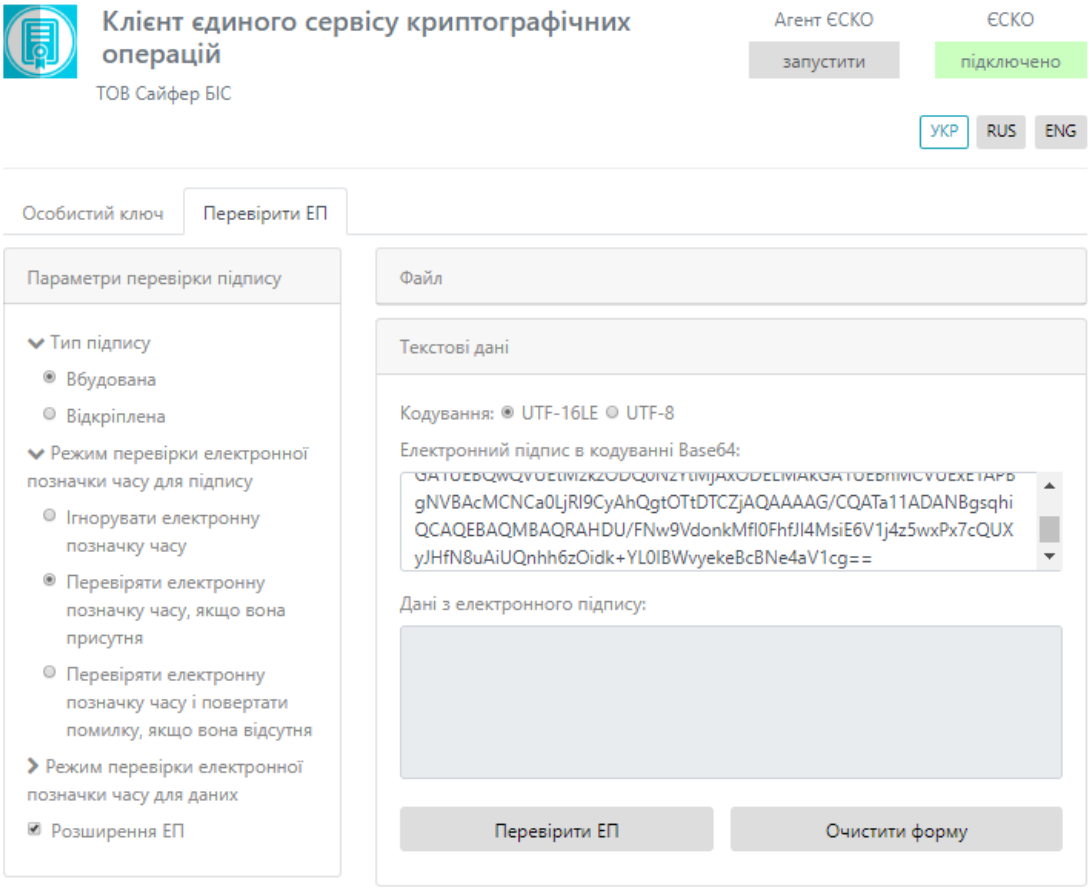

Рис. 37. Розширення вбудованого ЕП

Отримати повідомлення про успішне розширення підпису, Рис. 38.

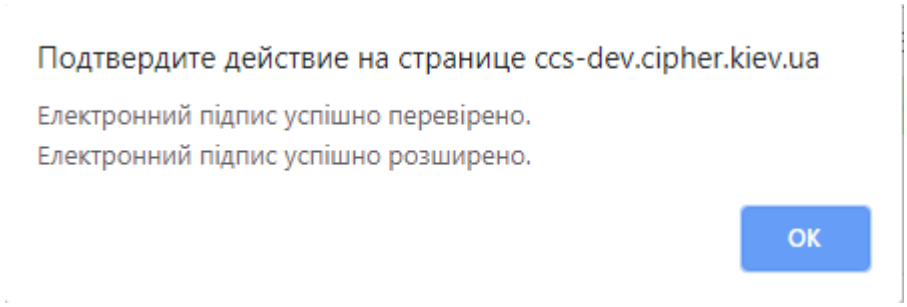

Рис. 38. Повідомлення про перевірку та розширення підпису

Отримати результат перевірки електронного підпису, Рис. 39.

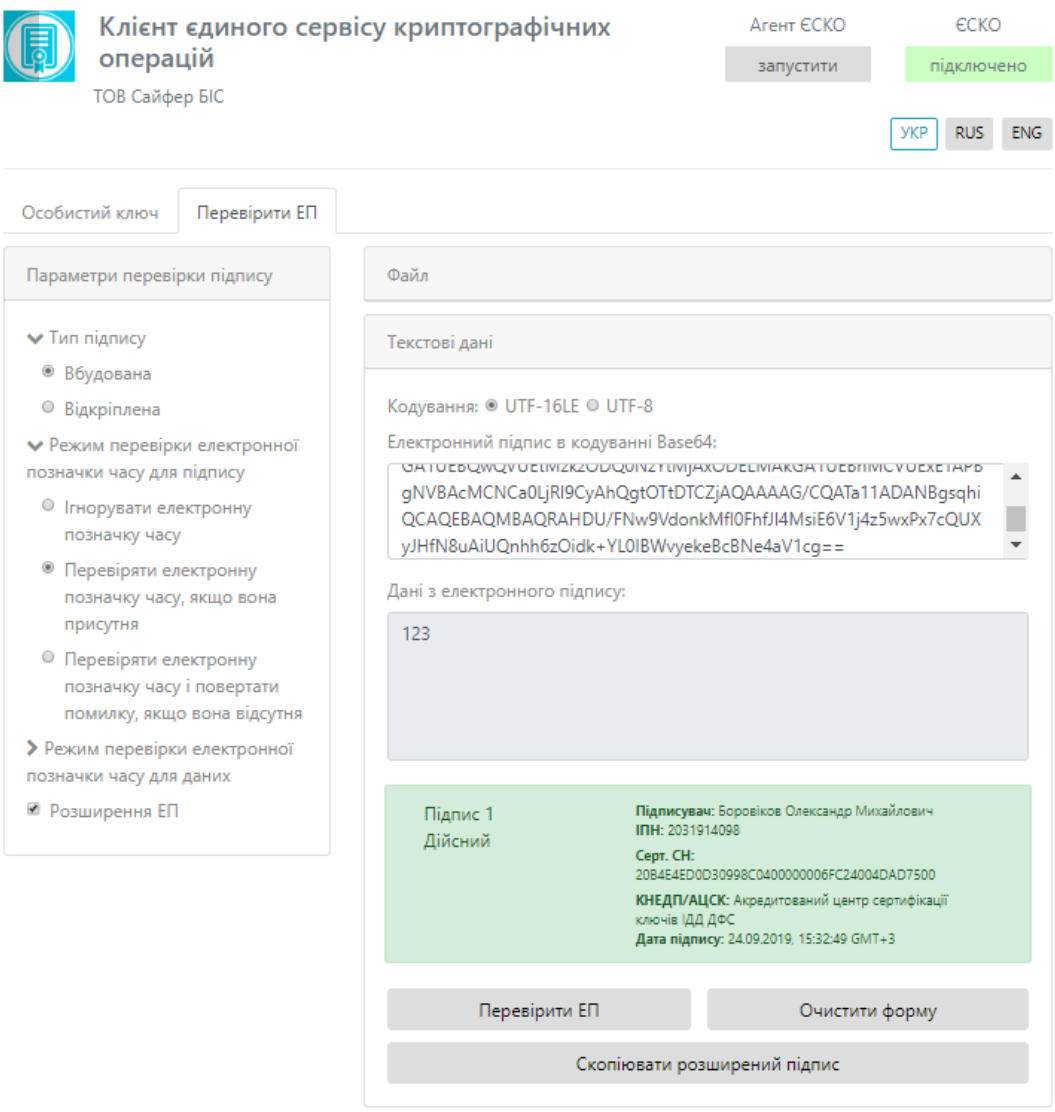

Рис. 39. Результат розширення та перевірки ЕП

За умови, якщо було завантажено текстові дані вже з повними даними для перевірки, то з’явиться повідомлення про це, Рис. 40.

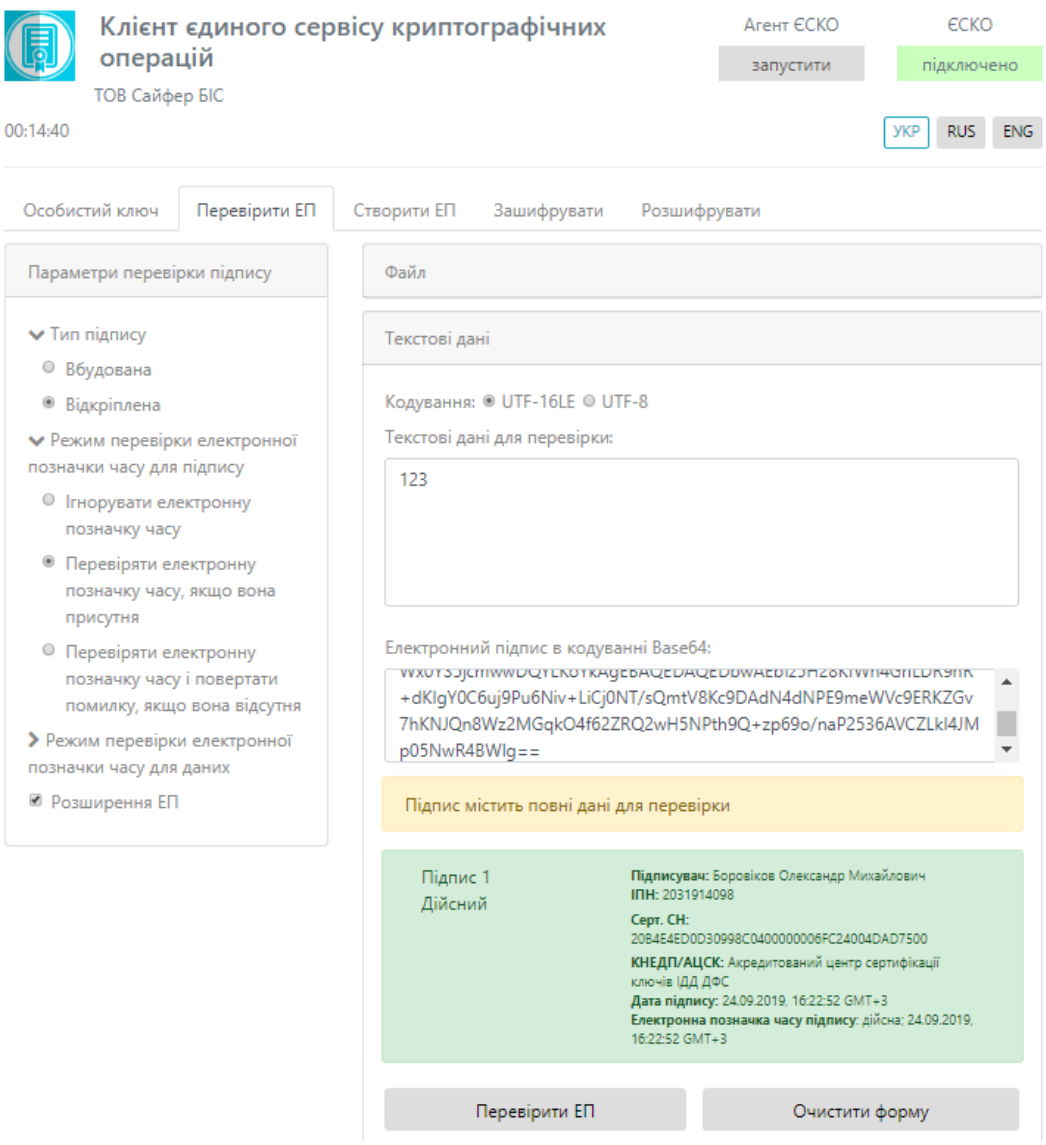

Рис. 40. Результати розширення підпису з повними даними для перевірки

Зашифрувати

Вкладка «Зашифрувати» містить такі розділи: Параметри шифрування, Сертифікат отримувача, Текстові дані та Файл, Рис. 41.

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:

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

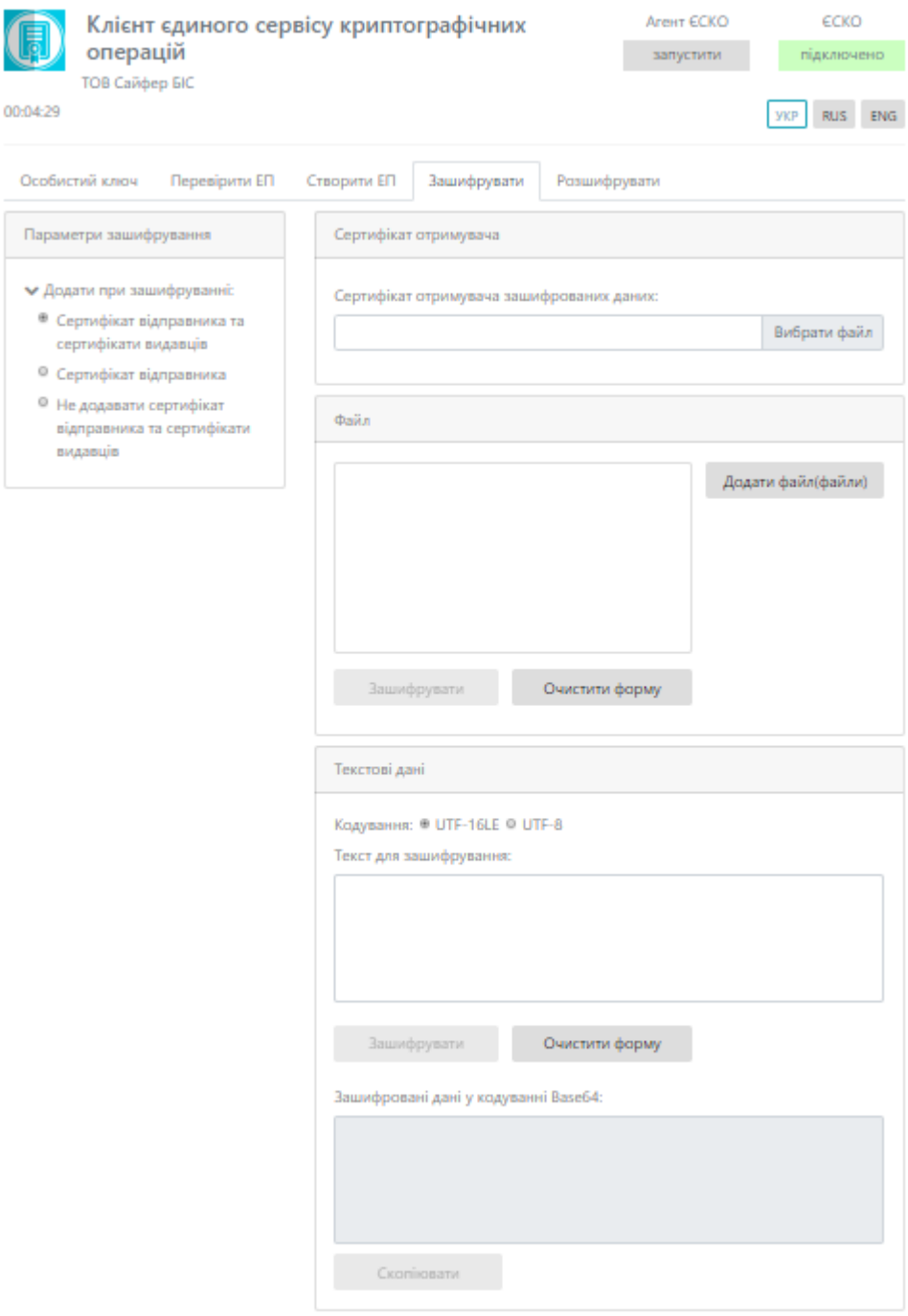

Рис. 41. Вкладка «Зашифрувати»

Розділ «Файл», який включає:

1. Поле «Файл 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».

Процес зашифрування файлу

Відеоінструкція знаходиться за посиланням.

Для того, щоб зашифрувати файл, 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. 42. За необхідності можна видалити файл натиснувши відповідну кнопку та додати ще, але слід зауважити, що максимальний об’єм всіх файлів не повинен перевищувати 100Мб.

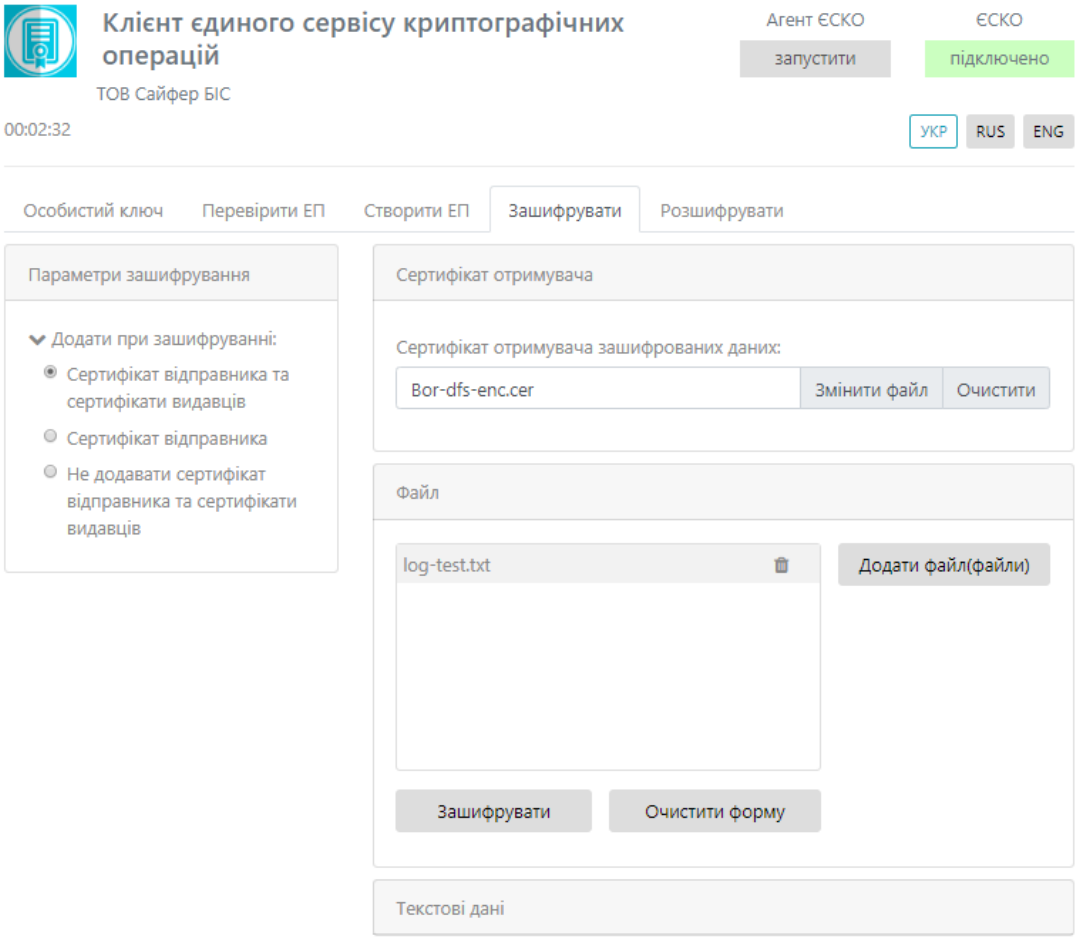

Рис. 42. Процес зашифрування

Після натискання на кнопку «Зашифрувати» з’являється вікно з повідомленням з результатом зашифрування, Рис. 43.

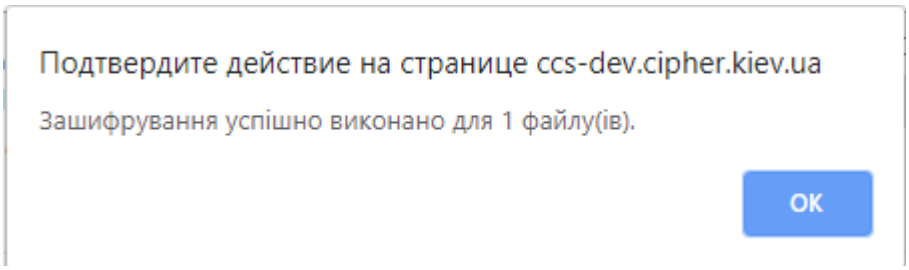

Рис. 43. Повідомлення про успішне зашифрування даних

Після, за допомогою відповідної кнопки «стрілка вниз» можна зберегти зашифрований файл та очищаємо форму, Рис. 44.

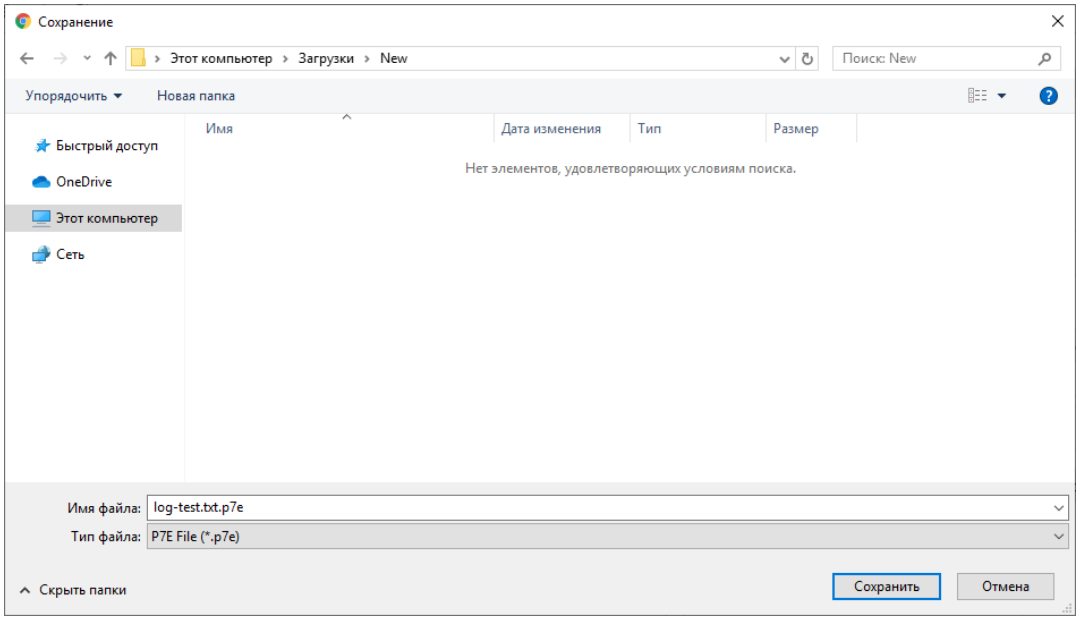

Рис. 44. Збереження зашифрованого файлу

Процес 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. 45.

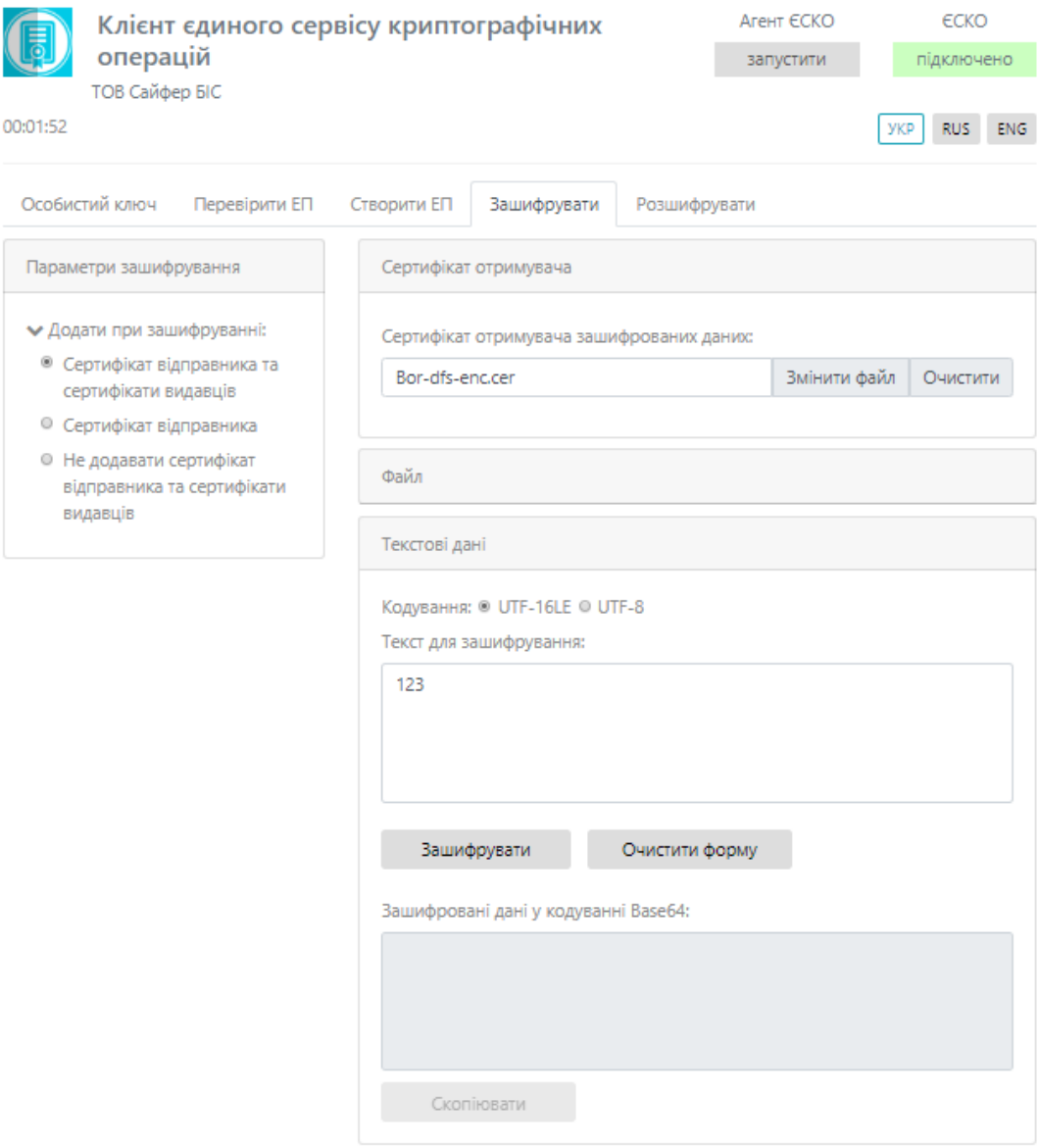

Рис. 45. Процес зашифрування

Після натискання на кнопку «Зашифрувати» з’являється у полі «Зашифровані дані у кодуванні Base64», Рис. 46.

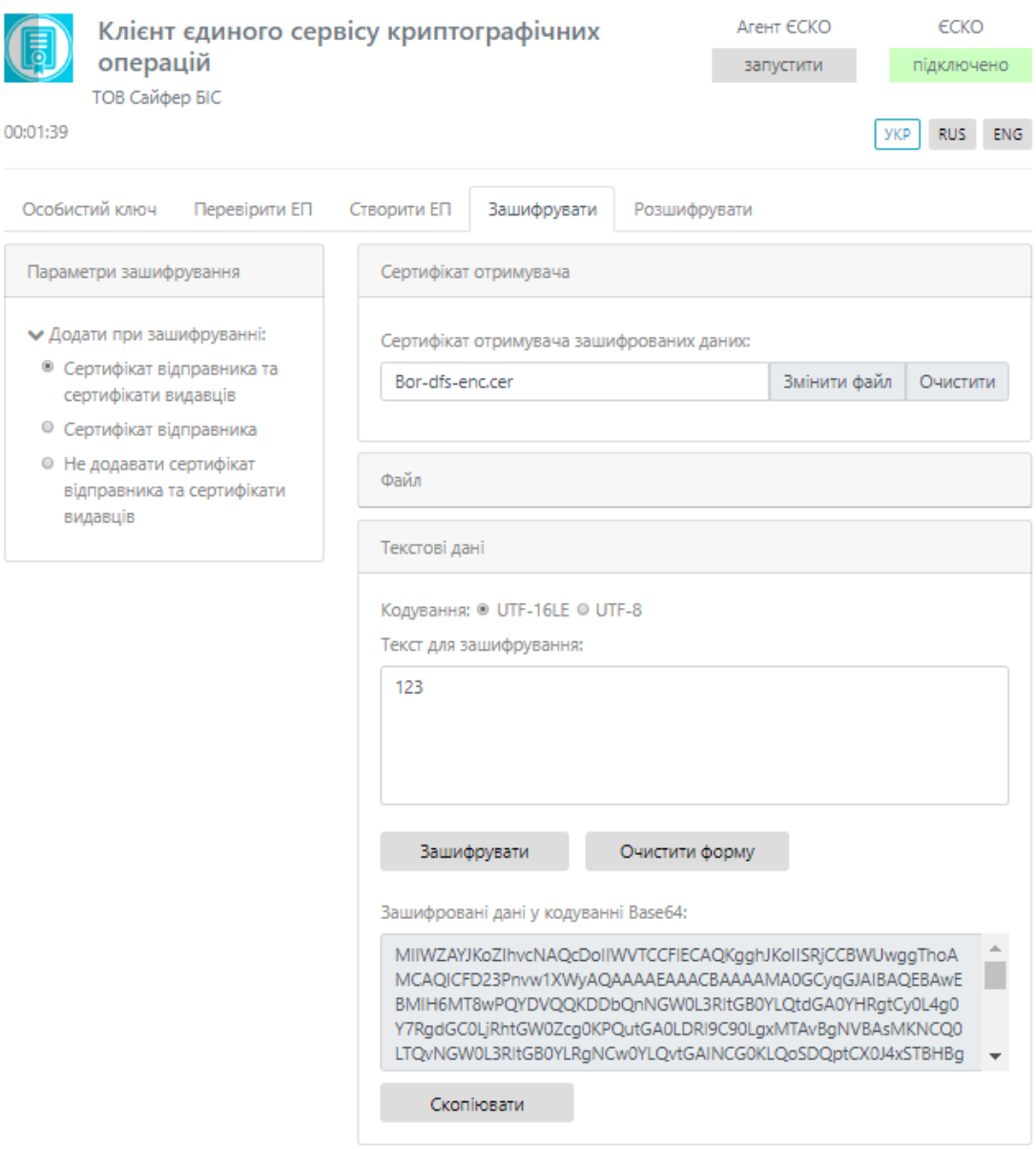

Рис. 46. Повідомлення про успішне зашифрування даних

Розшифрувати

Дана вкладка містить розділ Файл та Текстові дані.

Розділ «Файл», який включає, Рис. 47:

1. Поле «Файл для розшифрування» (обирається файл, який необхідно розшифрувати);
2. Кнопка «Розшифрувати» (Здійснює дешифрування файлу);
3. Кнопка «Зберегти розшифровані дані у файл» (здійснює збереження розшифрованих даних 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. 47:

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.

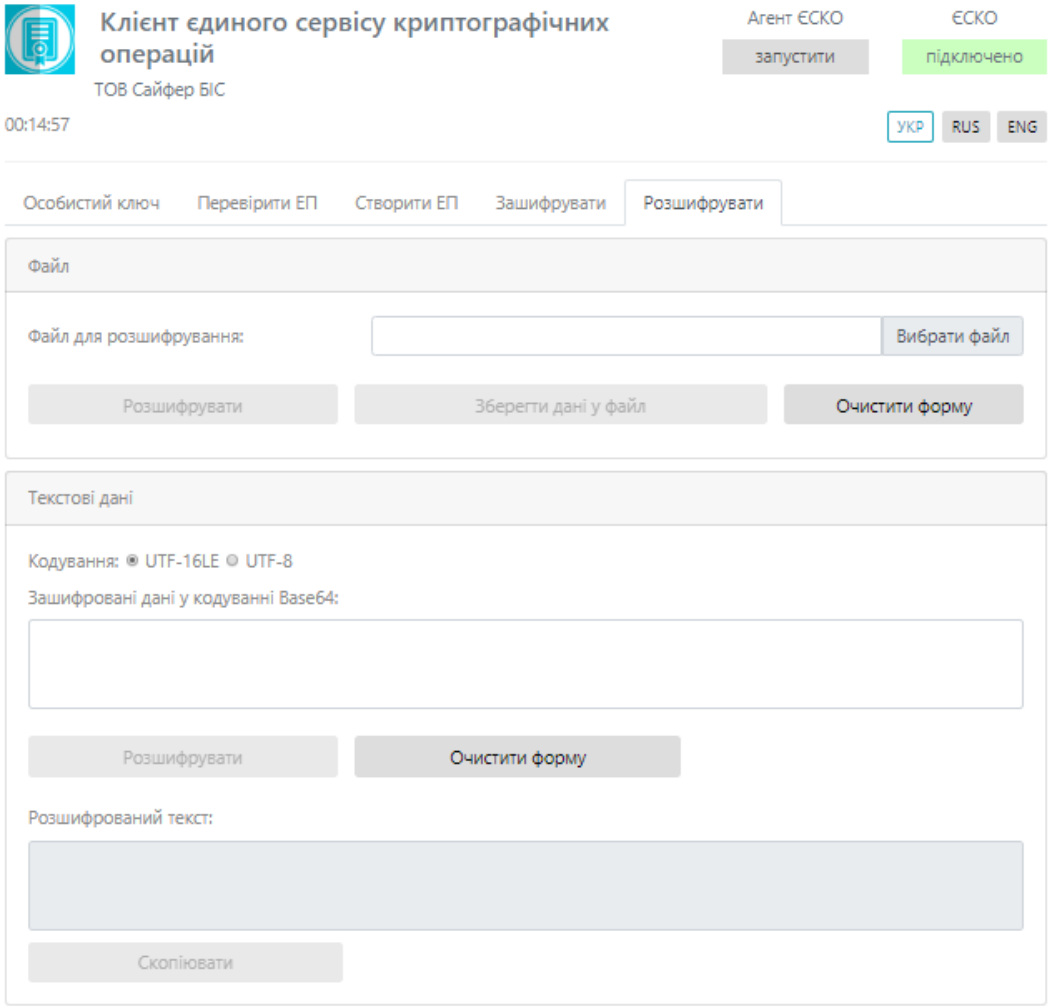

Рис. 47. Вкладка «Розшифрувати», розділ «Файл»

Процес розшифрування файлу

Відеоінструкція знаходиться за посиланням.

Для того, щоб розшифрувати файл, у розділі «Файл», необхідно вказати файл для розшифрування та натиснути кнопку «Розшифрувати», Рис. 48.

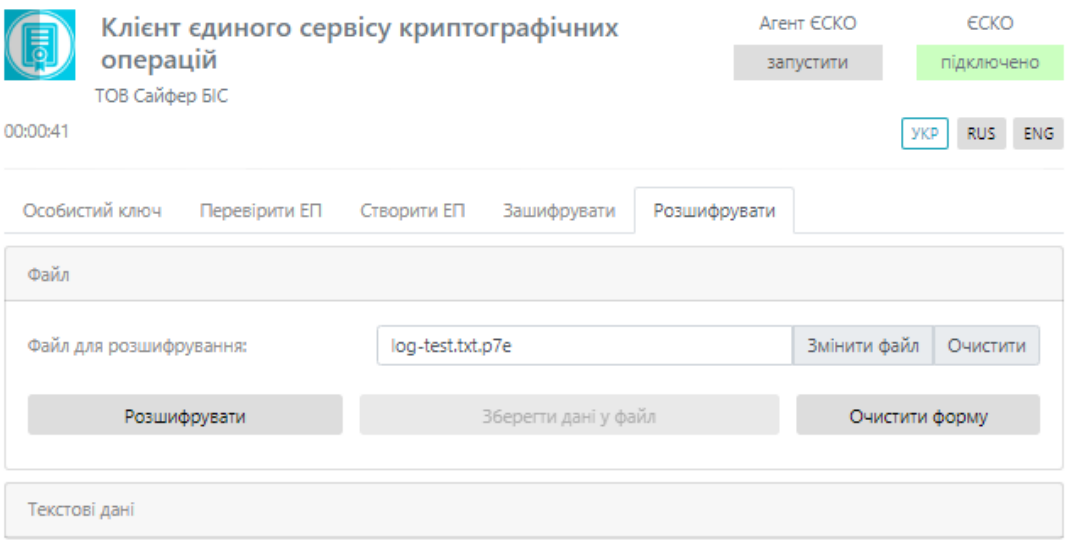

Рис. 48. Процес розшифрування

Після натискання на кнопку «Розшифрувати» з'являється вікно з повідомленням з результатом зашифрування, Рис. 49, та для збереження розшифрованих даних необхідно натиснути кнопку «Зберегти розшифровані дані у файл», Рис. 50.

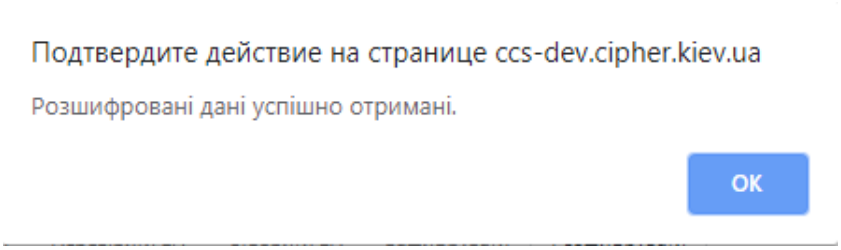

Рис. 49. Повідомлення про успішне розшифрування даних

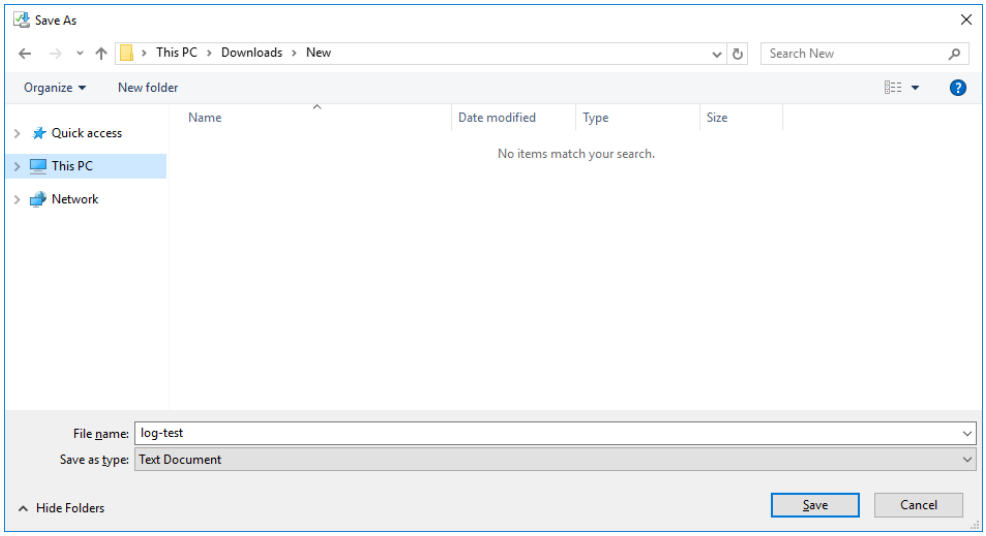

Рис. 50. Збереження розшифрованих даних

Процес 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. 51.

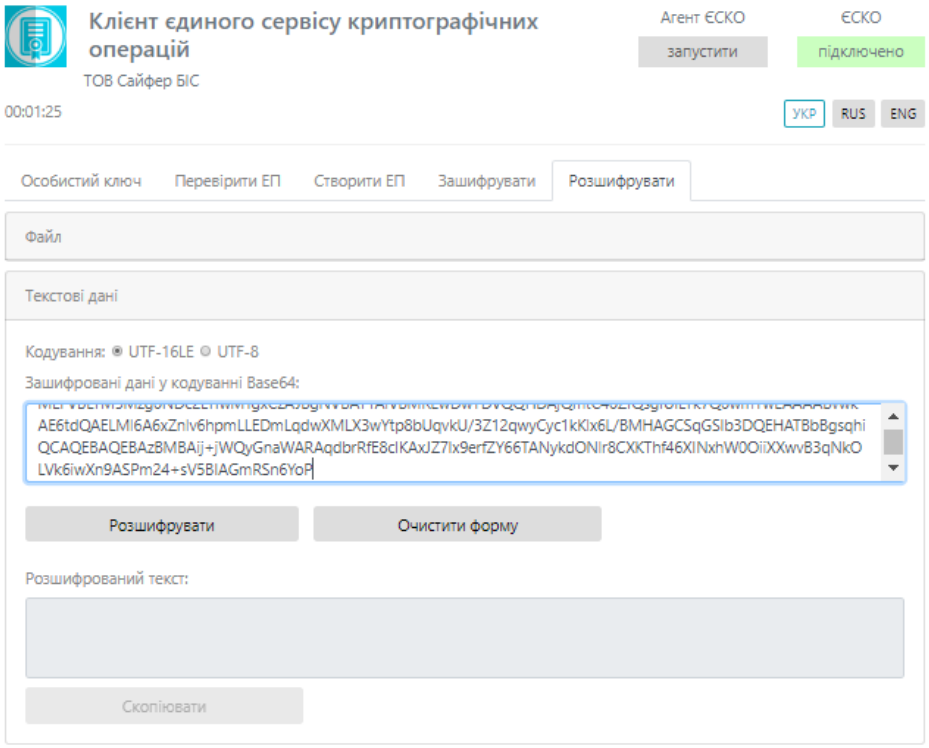

Рис. 51. Процес розшифрування

Після натискання на кнопку «Розшифрувати» з’являється розшифровані текстові дані у полі «Розшифрований текст», Рис. 52 та очистити форму.

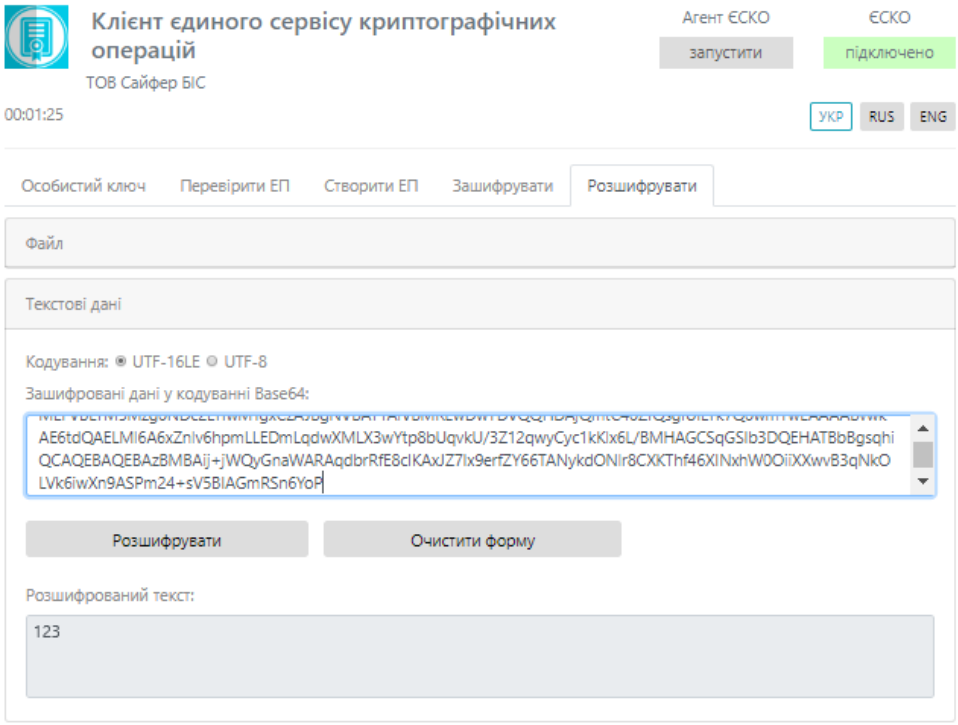

Рис. 52. Розшифровані текстові дані

MobileID

Відеоінструкція знаходиться за посиланням.

Для авторизації з ключем, який знаходиться на SIM-карті в ЄСКО, необхідно змінити «Тип ключа» на «Мобільний ЕП (MobileID)», Рис. 53.

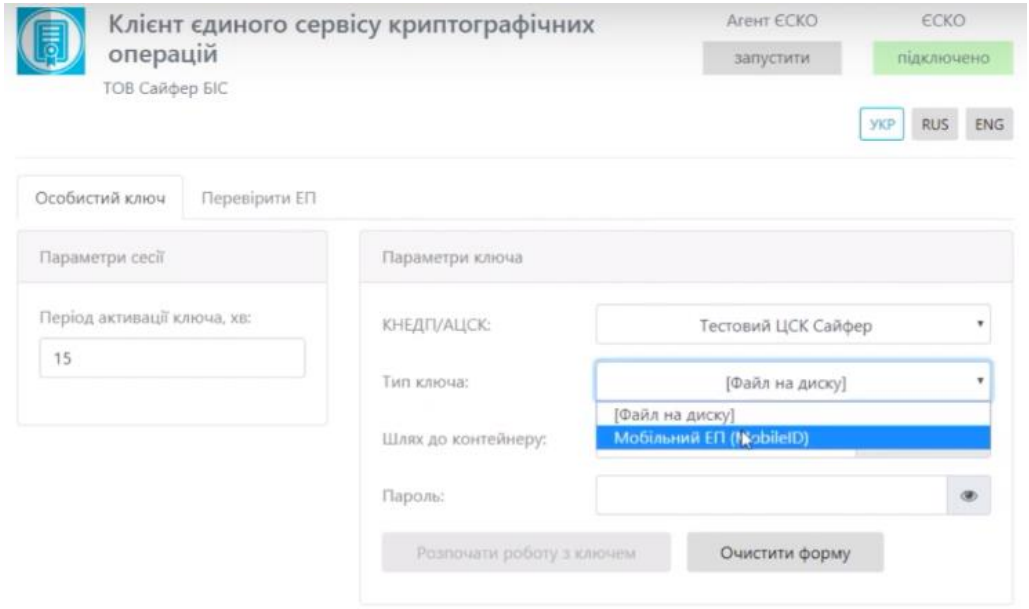

Рис. 53. Вибір «Мобільного ЕП»

Після зміни типу ключа, видозмінюється вікно «Параметри ключа», де слід вказати оператора та номер телефону, Рис. 54-Рис. 55.

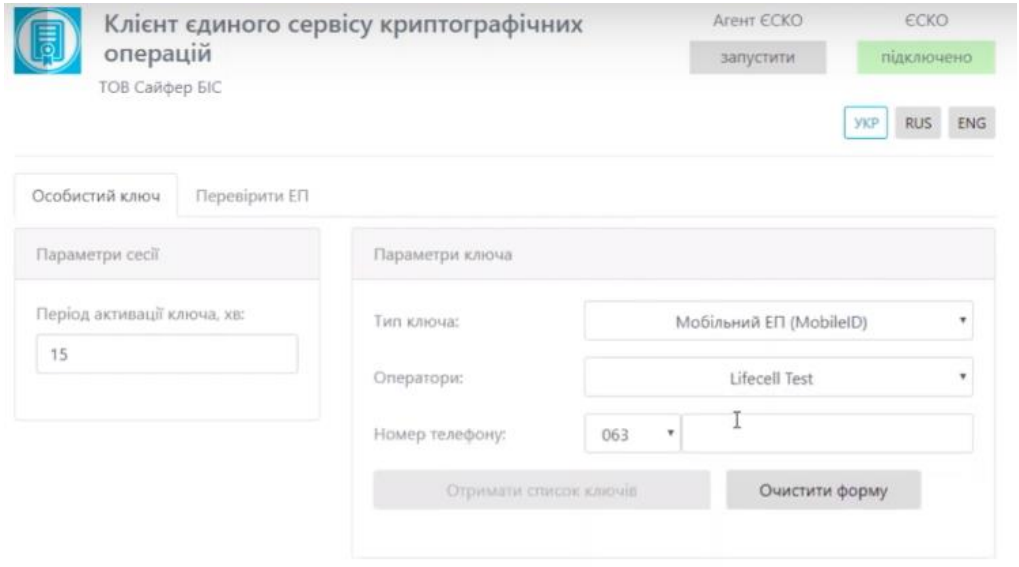

Рис. 54. Заповнення поля «Оператор»

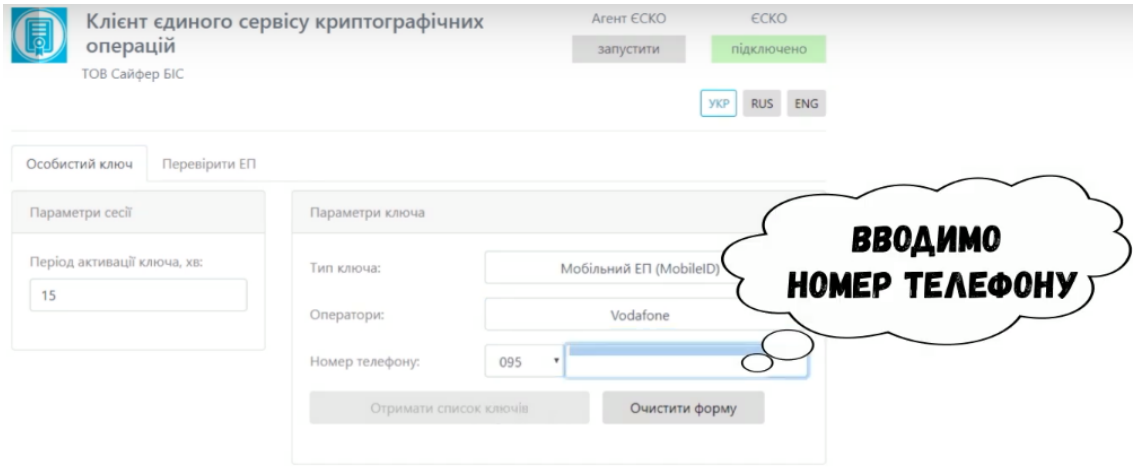

Рис. 55. Заповнення поля «Номер телефону»

Наступним кроком є отримання списку ключів, натиснувши відповідну кнопку у вікні «Параметри ключа», Рис. 56.

Одночасно на телефон приходить повідомлення про надання дозволу відображення посад додатку (Рис. 57), де необхідно «Дозволити» та ввести ПІН-код до ключа, Рис. 58.

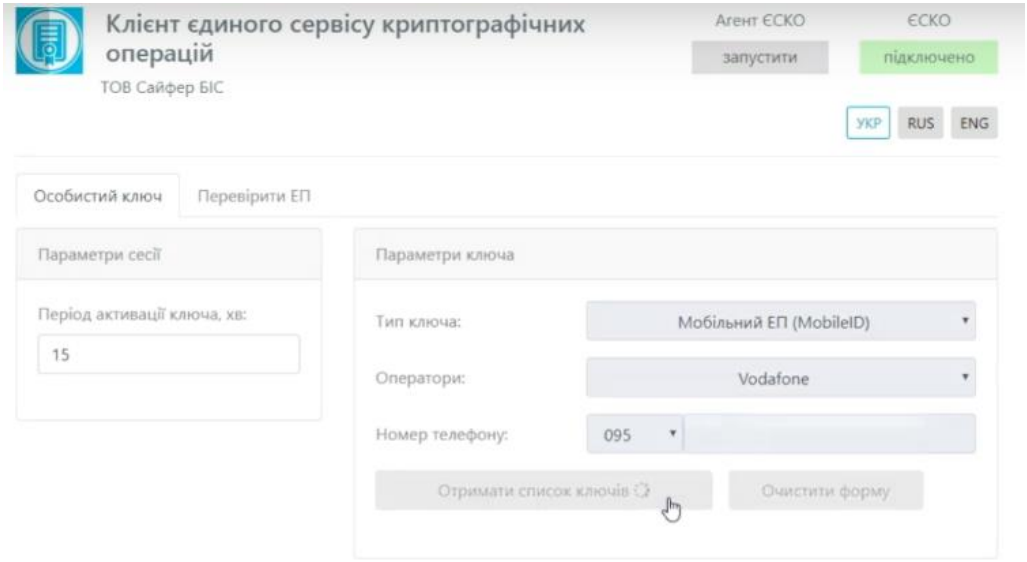

Рис. 56. Отримання списку доступних ключів

Рис. 57. Дозвіл на відображення посад додатку

Рис. 58. Введення ПІН-коду

Після успішного введення ПІН-коду, у браузері з’являється нове поле «Ключ», де необхідно обрати ключ, який необхідно використовувати (на SIM-карті може бути кілька ключів), Рис. 59.

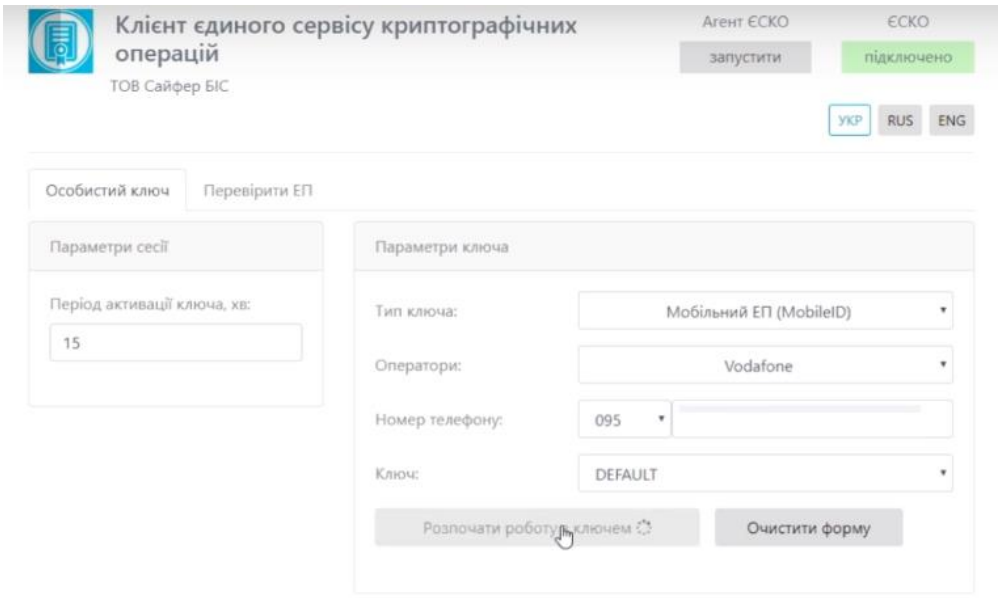

Рис. 59. Вибір ключа

Натиснувши кнопку «Розпочати роботу з ключем» створюється криптографічний контекст, де можна виконати наступні дії:

- Переглянути інформацію про сертифікат ключа ЕП, Рис. 60;
- Перевірити ЕП (доступно і без ключа);
- Створити ЕП.

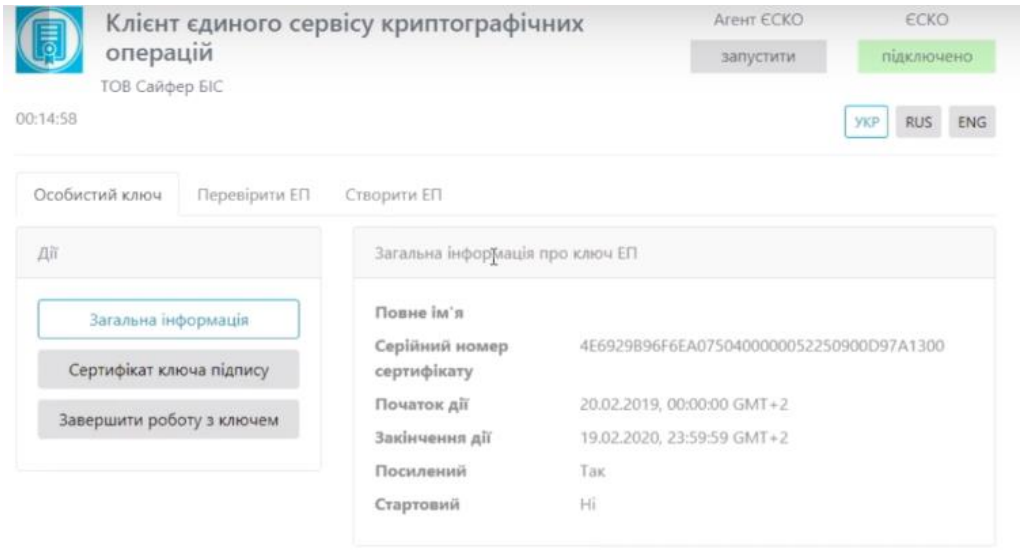

Рис. 60. Перегляд загальної інформації про ключ

Створення мобільного ЕП

За аналогією, як і при створенні звичайного підпису (за допомогою файлового контейнеру), необхідно завантажити файл/файли/текстові дані та натиснути кнопку «Створити ЕП», Рис. 61.

На телефон приходить повідомлення про підтвердження створення ЕП та введення ПІН-коду, Рис. 62-Рис. 63.

Про успішне створення мобільного ЕП повідомляється у відповідному повідомлені, Рис. 64.

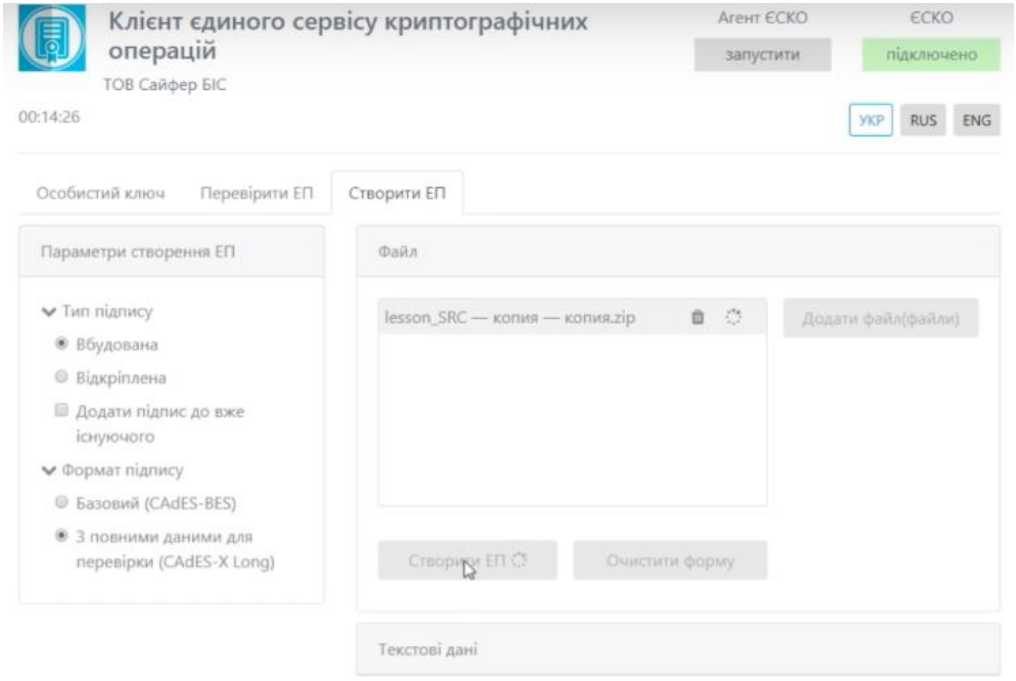

Рис. 61. Створення мобільного ЕП

Рис. 62. Підтвердження створення мобільного ЕП

Рис. 63. Введення ПІН-коду

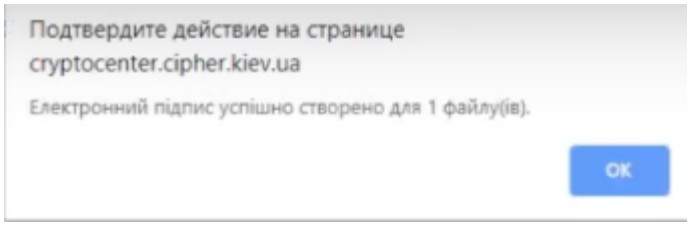

Рис. 64. Повідомлення про створення ЕП