
Єдиний Криптографічний Центр

Настанова з установки та експлуатації Агенту ЄКЦ (Java)

ЗМІСТ

ВСТУП	3
СИСТЕМНІ ВИМОГИ	3
ПІДГОТОВКА РОБОЧОГО МІСЦЯ ДЛЯ РОБОТИ З СЕРВІСОМ	4
ВВЕДЕННЯ	4
ПІДТРИМКА ЗАХИЩЕНИХ НОСІЇВ	5
AVTOR SECURE TOKEN – 337	6
РОБОТА З АГЕНТОМ ЄДИНОГО КРИПТОГРАФІЧНОГО ЦЕНТРУ	7
ЗАПУСК	7
СЛУЖБОВІ ФУНКЦІЇ ТА ОПЦІЇ ЄКЦ	10
ВИБІР КЛЮЧА ЕП – ФАЙЛ	14
ВИБІР КЛЮЧА ЕП – ЗАХИЩЕНИЙ НОСІЙ	18
СТВОРЕННЯ ЕП	22
Створення ЕП за типом «Вбудована» на файл	23
Створення ЕП за типом «Відкріплена» на файл	25
Створення ЕП за типом «Вбудована» на текстові дані	27
Створення ЕП за типом «Відкріплена» на текстові дані	30
ПЕРЕВІРКА ЕП	32
Перевірка ЕП за типом «Вбудована», файл	35
Перевірка ЕП за типом «Відкріплена», файл	37
Перевірка ЕП за типом «Вбудована», текстові дані	38
Перевірка ЕП за типом «Відкріплена», текстові дані	40
Перевірка базового ЕП	42
Розширення ЕП	44
ЗАШИФРУВАТИ	50
Операція зашифрування файлу	52
Операція зашифрування текстових даних	54
РОЗШИФРУВАТИ	56
Операція розшифрування файлу	57
Операція розшифрування текстових даних	59

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 «Диспетчері устроїв». Для перевірки необхідно перейти «Пуск»->«Панель управління»->«Диспетчер устроїв»->«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 Агента ЄКЦ

- 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.

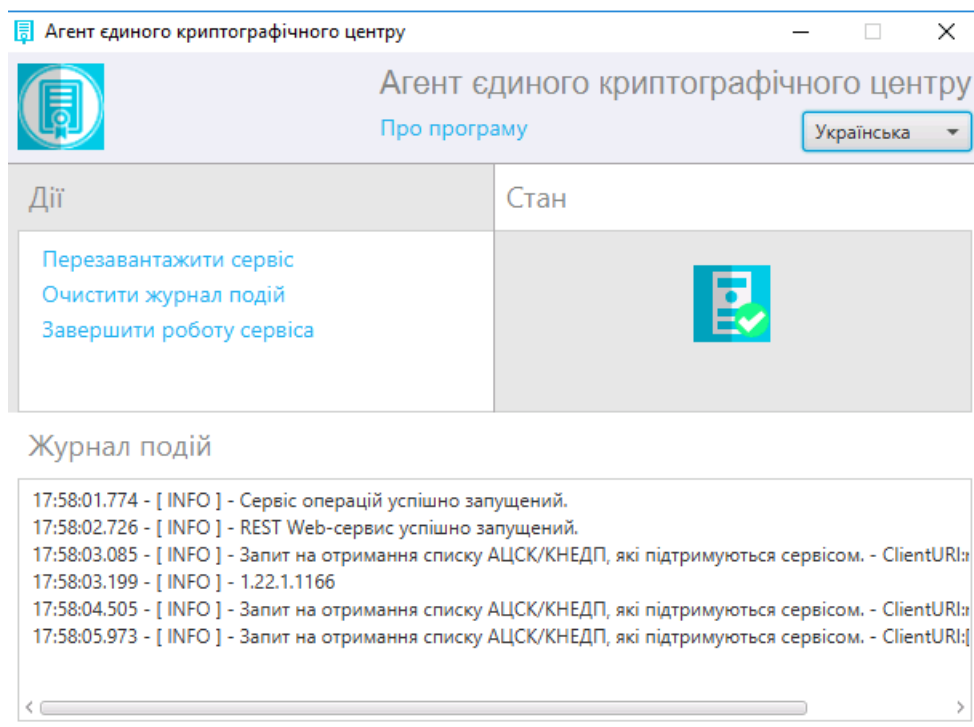


Рис. 3. Вікно «Агенту єдиного криптографічного центру»

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

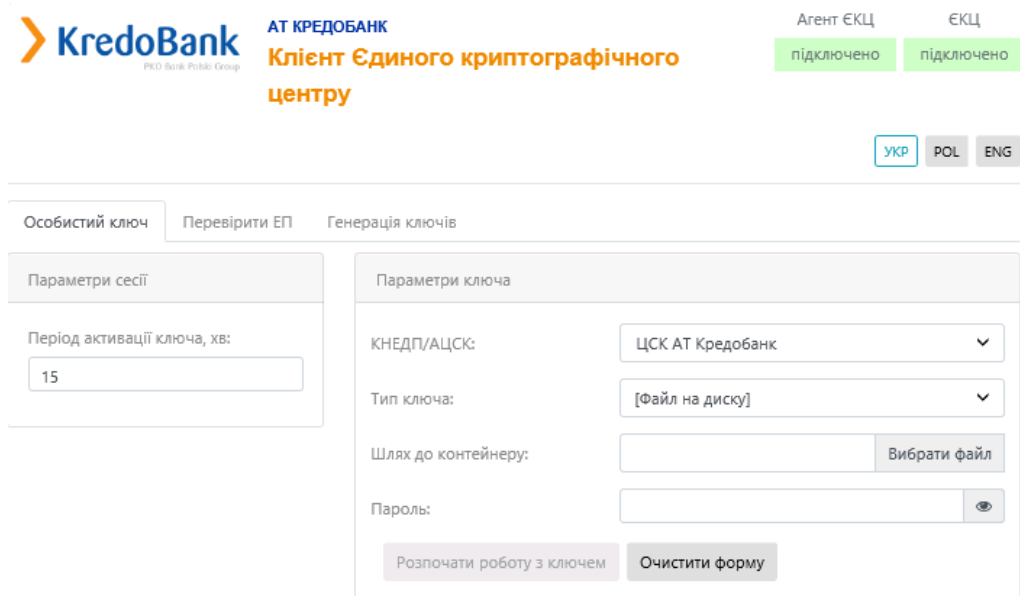


Рис. 4. Стартове вікно Агент ЄКЦ

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

The screenshot shows the KredoBank website interface. At the top left is the KredoBank logo with the text 'AT КРЕДОБАНК' and 'Клієнт Єдиного криптографічного центру'. At the top right, there are two green buttons labeled 'Агент ЕКЦ підключено' and 'ЕКЦ підключено'. Below these are language selection buttons for 'УКР', 'POL', and 'ENG'. The main content area has three tabs: 'Особистий ключ', 'Перевірити ЕП', and 'Генерація ключів'. The 'Генерація ключів' tab is active, showing a form titled 'Параметри ключа'. The form has four main sections: 'КНЕДП/АЦСК:' with a dropdown menu set to 'ЦСК АТ Кредобанк'; 'Тип ключа:' with a dropdown menu set to '[Файл на диску]'; 'Шлях до контейнеру:' with a text input field containing 'C:\Users\skovtun\Desktop\key-2' and a 'Вибрати файл' button; and 'Пароль:' with a masked password input field. At the bottom of the form are two buttons: 'Розпочати роботу з ключем' and 'Очистити форму'. To the left of the main form is a 'Параметри сесії' section with a 'Період активації ключа, хв:' field set to '15'.

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 Агенті ЕКЦ, Рис. 6.

Особистий ключ Перевірити ЕП Створити ЕП Зашифрувати Розшифрувати Генерація ключів

Дії

Загальна інформація

Сертифікат ключа підпису

Сертифікат ключа шифрування

Завершити роботу з ключем

Загальна інформація про ключ ЕП

Повне ім'я	Кочоркова Ліора Даниліївна
Серійний номер сертифікату	C964124DC661EA78
Початок дії	21.09.2019 14:46:33
Закінчення дії	20.09.2020 00:00:00
Посилений	Ні
Стартовий	Ні

Загальна інформація про ключ шифрування

Повне ім'я	Кочоркова Ліора Даниліївна
Серійний номер сертифікату	F72C6E6826965C72
Початок дії	21.09.2019 14:46:46
Закінчення дії	20.09.2020 00:00:00
Посилений	Ні
Стартовий	Ні

Рис. 6. Робоча область Агента 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).

The screenshot shows the KredoBank interface for the Agent EEC. At the top, there is the KredoBank logo and the text 'АТ КРЕДОБАНК Клієнт Єдиного криптографічного центру'. On the right, there are two green buttons labeled 'підключено' (connected) for 'Агент ЕКЦ' and 'ЕКЦ'. Below the header, there is a navigation bar with tabs: 'Особистий ключ', 'Перевірити ЕП', 'Створити ЕП', 'Зашифрувати', 'Розшифрувати', and 'Генерація ключів'. The 'Дії' (Actions) menu is open, showing options: 'Загальна інформація' (highlighted), 'Сертифікат ключа підпису', 'Сертифікат ключа шифрування', and 'Завершити роботу з ключем'. The main content area displays two key details sections:

Загальна інформація про ключ ЕП	
Повне ім'я	Кочоркова Ліора Даниліївна
Серійний номер сертифікату	C964124DC661EA78
Початок дії	21.09.2019 14:46:33
Закінчення дії	20.09.2020 00:00:00
Посилений	Ні
Стартовий	Ні

Загальна інформація про ключ шифрування	
Повне ім'я	Кочоркова Ліора Даниліївна
Серійний номер сертифікату	F72C6E6826965C72
Початок дії	21.09.2019 14:46:46
Закінчення дії	20.09.2020 00:00:00
Посилений	Ні
Стартовий	Ні

Рис. 7. Робоча область Агента ЕКЦ

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 (CAAdES-X Long).
- «Файл». Включає в себе 2 поля:
 - 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/файли для зашифрування.
- «Текстові дані».
 - Кодування UTF-16LE та UTF-8.
 - «Текст для зашифрування». Поле, де слід вказати текст для зашифрування.
 - «Зашифровані дані у кодуванні 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 кодуванні 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.

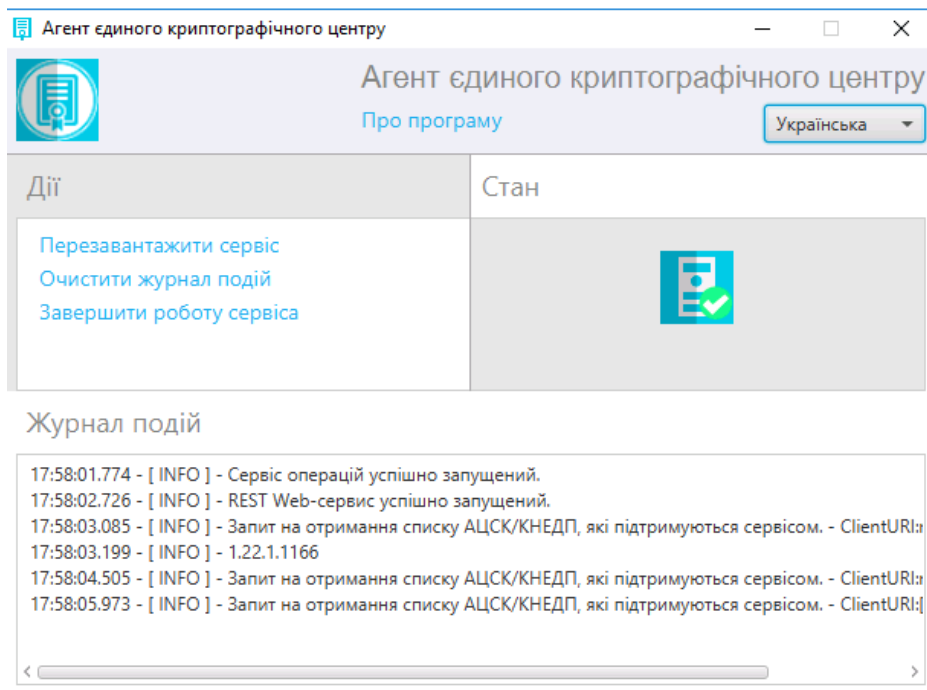


Рис. 8. Агент єдиного криптографічного центру

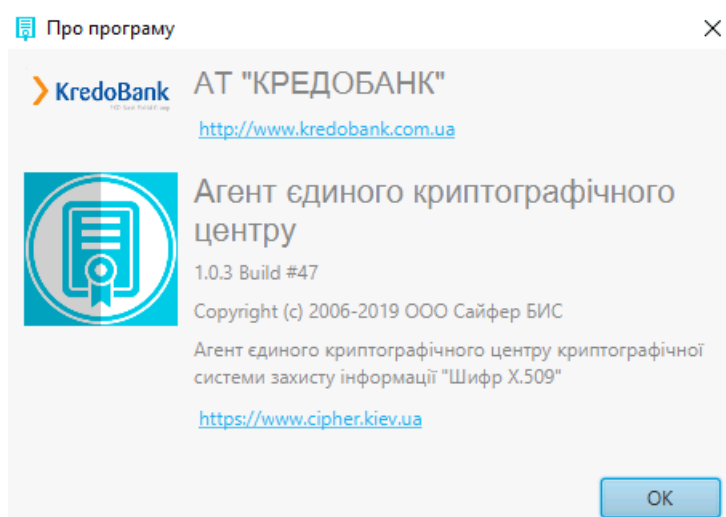


Рис. 9. Вікно «Про програму»

Вибір ключа ЕП – файл

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

Рис. 10. Стартове вікно ЕКЦ

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

Особистий ключ Перевірити ЕП

Параметри сесії

Період активації ключа, хв:

Параметри ключа

КНЕДП/АЦСК:

Тип ключа:

Шлях до контейнеру:

Пароль:

Рис. 11. Запуск Агента ЄКЦ

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

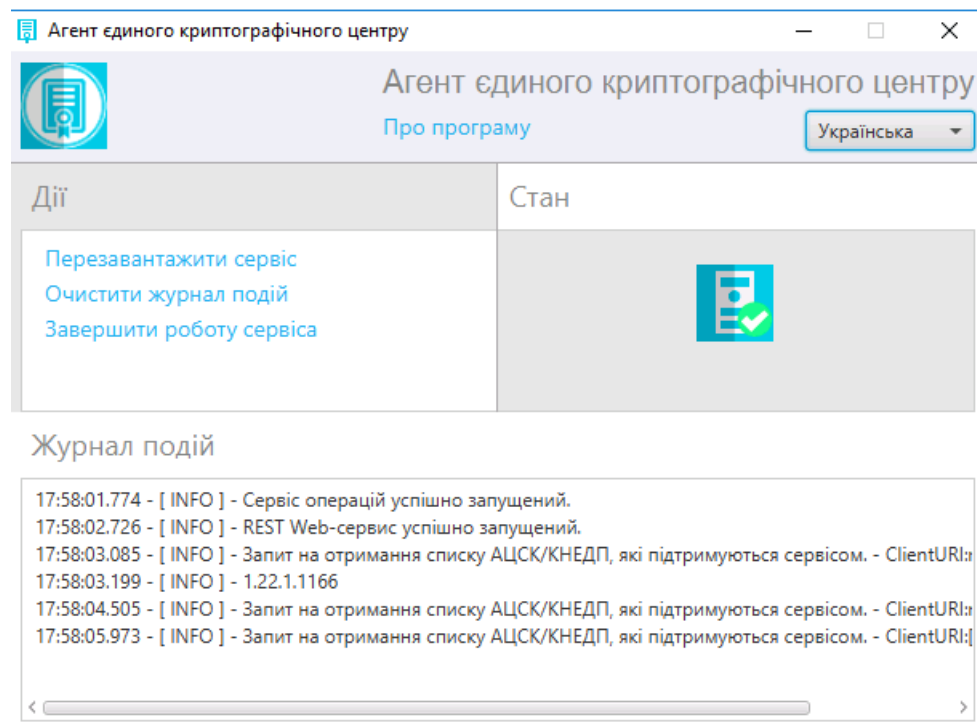


Рис. 12. Агент Єдиного Криптографічного Центру

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

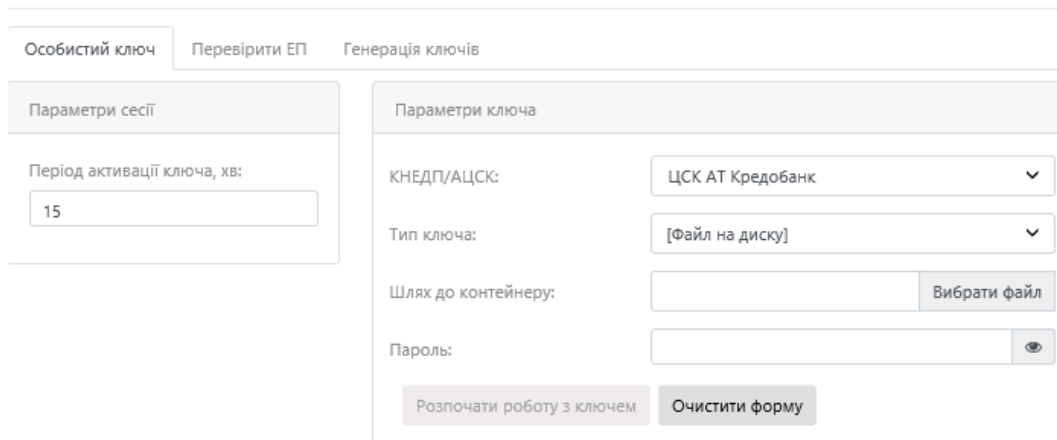


Рис. 13. Стартове вікно Агент ЄКЦ

5. На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвиликах 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 «ДІА»;
 - 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.

Особистий ключ Перевірити ЕП Генерація ключів

Параметри сесії

Період активації ключа, хв:

Параметри ключа

КНЕДП/АЦСК:


Тип ключа:

Шлях до контейнеру:

Пароль:

Рис. 14. Заповнення розділу «Параметри ключа»

- 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 ЕКЦ, Рис. 15.


AT КРЕДОБАНК
Клієнт Єдиного криптографічного центру

Агент ЕКЦ підключено ЕКЦ підключено

00:14:57 УКР POL ENG

Особистий ключ Перевірити ЕП Створити ЕП Зашифрувати Розшифрувати Генерація ключів

Дії

Загальна інформація про ключ ЕП

Повне ім'я	Кочоркова Ліора Данилівна
Серійний номер сертифікату	C964124DC661EA78
Початок дії	21.09.2019 14:46:33
Закінчення дії	20.09.2020 00:00:00
Посилений	Ні
Стартовий	Ні

Загальна інформація про ключ шифрування

Повне ім'я	Кочоркова Ліора Данилівна
Серійний номер сертифікату	F72C6E6826965C72
Початок дії	21.09.2019 14:46:46
Закінчення дії	20.09.2020 00:00:00
Посилений	Ні
Стартовий	Ні

Рис. 15. Робоча область Агенту ЕКЦ

Вибір ключа ЕП – захищений носій

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

Кредобанк
AT КРЕДОБАНК
Клієнт Єдиного криптографічного центру

Агент ЕКЦ ЕКЦ
запустити підключено

УКР POL ENG

Особистий ключ Перевірити ЕП

Параметри сесії

Період активації ключа, хв:
15

Параметри ключа

КНЕДП/АЦСК: ЦСК АТ Кредобанк

Тип ключа: [Файл на диску]

Шлях до контейнеру: Вибрати файл

Пароль: [password input]

Розпочати роботу з ключем Очистити форму

Рис. 16. Стартове вікно ЕКЦ

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

Кредобанк
AT КРЕДОБАНК
Клієнт Єдиного криптографічного центру

Агент ЕКЦ ЕКЦ
запустити підключено

УКР POL ENG

Особистий ключ Перевірити ЕП

Параметри сесії

Період активації ключа, хв:
15

Параметри ключа

КНЕДП/АЦСК: ЦСК АТ Кредобанк

Тип ключа: [Файл на диску]

Шлях до контейнеру: Вибрати файл

Пароль: [password input]

Розпочати роботу з ключем Очистити форму

Рис. 17. Запуск Агента ЕКЦ

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

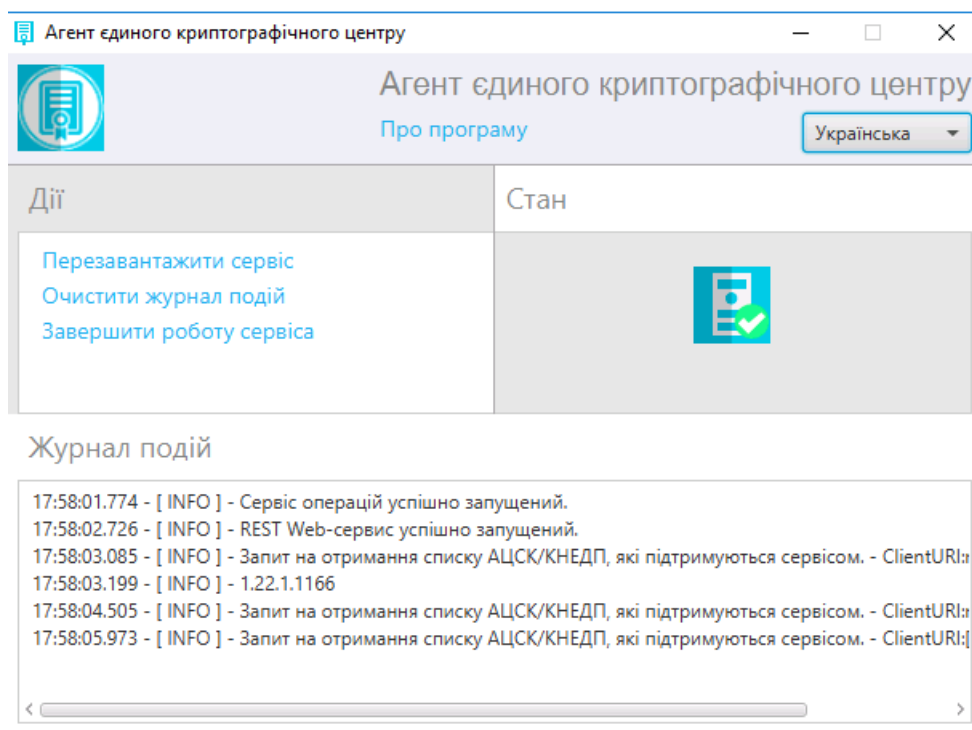


Рис. 18. Агент Єдиного Криптографічного Центру

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

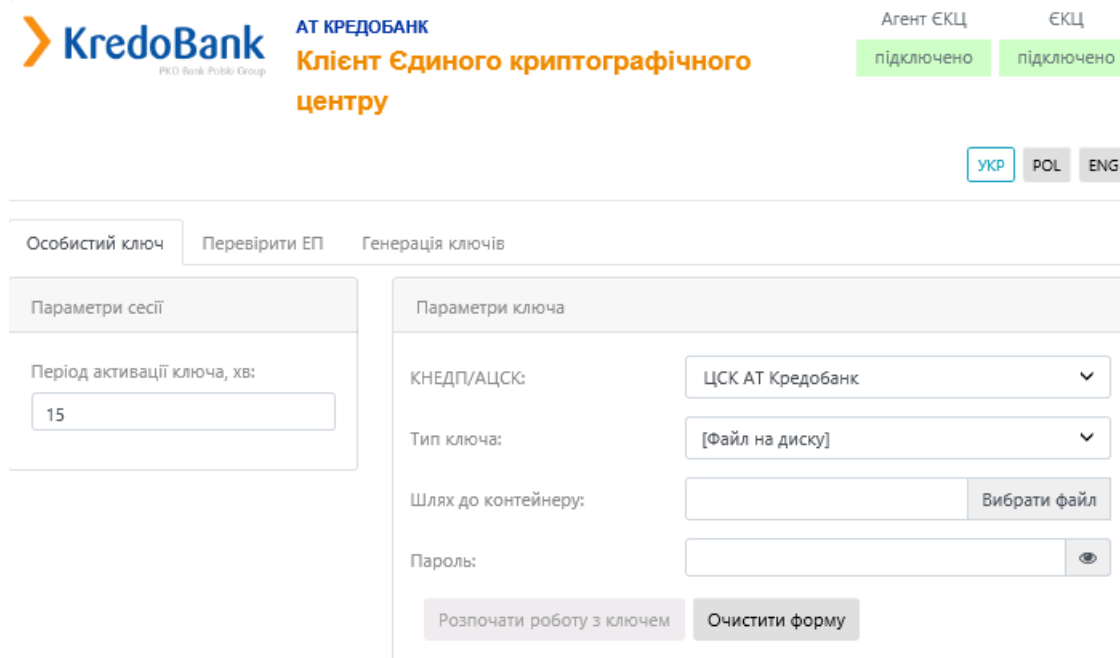


Рис. 19. Стартове вікно Агент ЄКЦ

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;

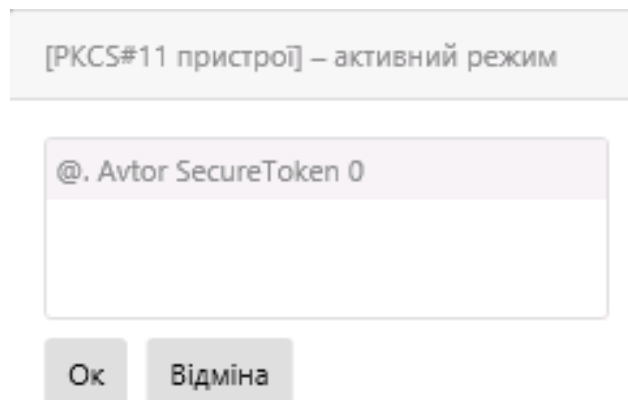


Рис. 20. Вказівка «Шлях до контейнера»

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

Особистий ключ Перевірити ЕП Генерація ключів

Параметри сесії

Період активації ключа, хв:

Параметри ключа

КНЕДП/АЦСК:

Тип ключа:

Шлях до контейнеру:

Пароль:

Рис. 21. Форма «Агент ЕКЦ»

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.

00:14:58

Агент ЕКЦ ЕКЦ

підключено підключено

УКР POL ENG

Особистий ключ Перевірити ЕП Створити ЕП Зашифрувати Розшифрувати Генерація ключів

Дії

Загальна інформація про ключ ЕП

Повне ім'я	Ковалинський Данило Ігорович
Серійний номер сертифікату	67FAFE98F7299F09
Початок дії	21.09.2019 14:46:22
Закінчення дії	20.09.2020 00:00:00
Посилений	Ні
Стартовий	Ні

Загальна інформація про ключ шифрування

Повне ім'я	Ковалинський Данило Ігорович
Серійний номер сертифікату	DB18DF297705C52C
Початок дії	21.09.2019 14:46:37
Закінчення дії	20.09.2020 00:00:00
Посилений	Ні
Стартовий	Ні

Рис. 22. Робоча область Агента ЕКЦ

Створення ЕП

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

The screenshot shows the 'Створити ЕП' (Create Certificate) interface. At the top, there is a navigation bar with the KredoBank logo, 'AT КРЕДОБАНК', and 'Клієнт Єдиного криптографічного центру'. On the right, there are status indicators for 'Агент ЕКЦ' and 'ЕКЦ', both marked as 'підключено'. Below the navigation bar, there are language selection buttons for 'УКР', 'POL', and 'ENG'. The main interface has a top menu with options: 'Особистий ключ', 'Перевірити ЕП', 'Створити ЕП', 'Зашифрувати', 'Розшифрувати', and 'Генерація ключів'. The 'Створити ЕП' section is active and contains three sub-sections: 1. 'Параметри створення ЕП' (Parameters of certificate creation) with a tree view: 'Тип підпису' (Signature type) with radio buttons for 'Вбудована' (Embedded) and 'Відкріплена' (Detached), and a checkbox for 'Додати підпис до вже існуючого' (Add signature to existing); 'Формат підпису' (Signature format) with a radio button for 'З повними даними для перевірки (CAAdES-X Long)'. 2. 'Файл' (File) with a large empty box for file upload, a 'Додати файл(файли)' (Add file(s)) button, and 'Створити ЕП' (Create Certificate) and 'Очистити форму' (Clear form) buttons. 3. 'Текстові дані' (Text data) with a 'Кодування:' (Encoding) dropdown set to 'UTF-16LE', a 'Текстові дані для підпису:' (Text data for signature) input field, a 'Додатковий опис:' (Additional description) input field, and 'Створити ЕП' (Create Certificate) and 'Очистити форму' (Clear form) buttons. At the bottom, there is a 'Підпис у кодуванні Base64:' (Signature in Base64 encoding) output area.

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.

Особистий ключ Перевірити ЕП **Створити ЕП** Зашифрувати Розшифрувати Генерація ключів

Параметри створення ЕП

▼ Тип підпису

Вбудована

Відкріплена

Додати підпис до вже існуючого

▼ Формат підпису

З повними даними для перевірки (CAAdES-X Long)

Файл

Белый Бим Черное ухо.pdf	🗑️
Алые паруса.pdf	🗑️
Госпожа Бовари.pdf	🗑️

Додати файл(файли)

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.

Агент єдиного криптографічного центру ×

Ресурс понапе запитує дозвіл на використання ЕП в кількості 1 раз(у,ів). ?

Інформація про дані, що підписуються:

Алые паруса.pdf

Щоб дати дозвіл на використання особистого ключа натисніть кнопку "Ок".
У разі відмови натисніть кнопку "Відміна".

Рис. 25. Дозвіл на використання ЕП

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

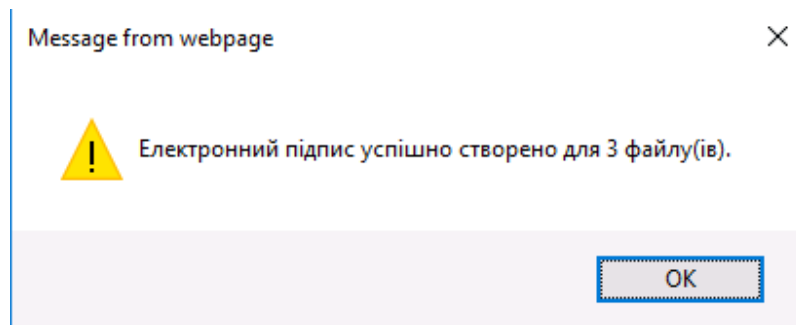


Рис. 26. Повідомлення про створення електронного підпису

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.

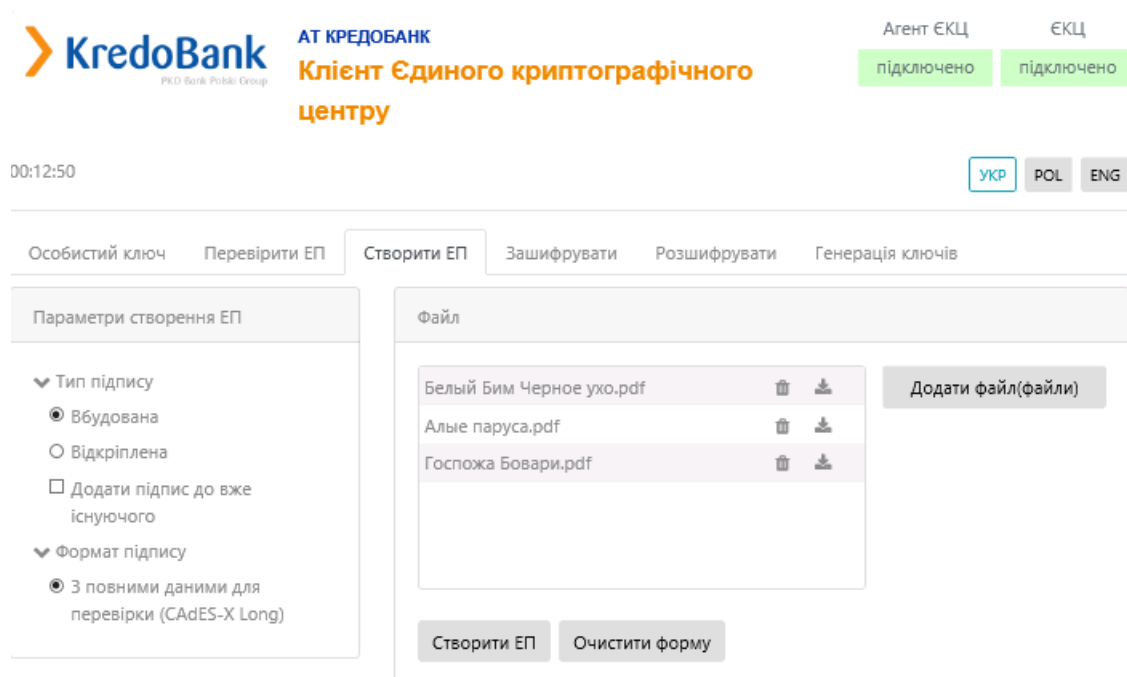


Рис. 27. Збереження підпису у файл



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.

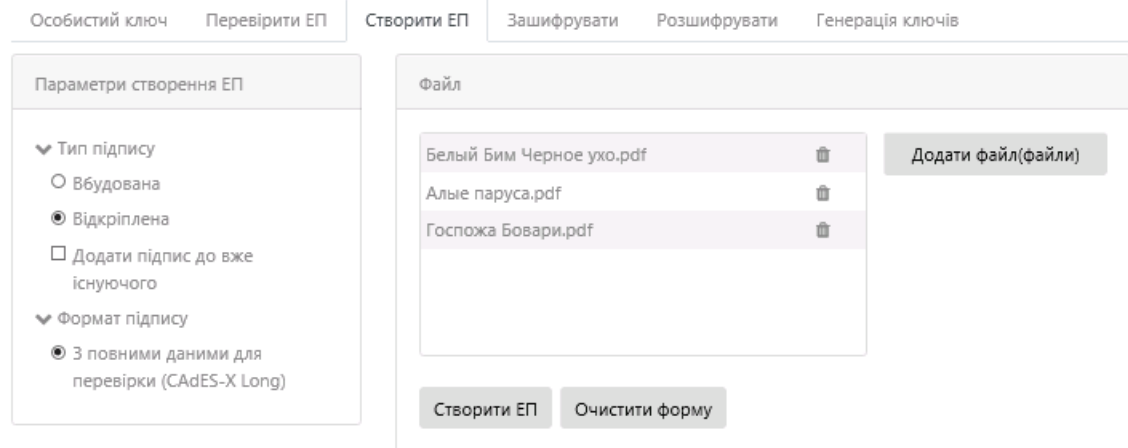


Рис. 29. Створення ЕП

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.

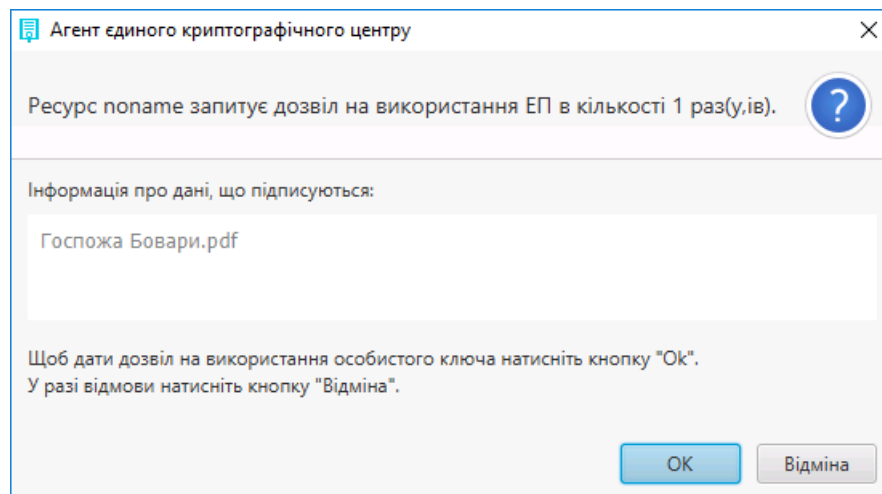


Рис. 30. Дозвіл на використання ЕП

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

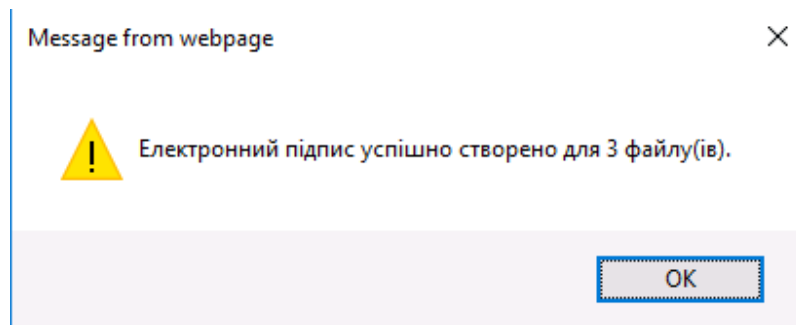


Рис. 31. Повідомлення про створення електронного підпису

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 очищуємо форму.

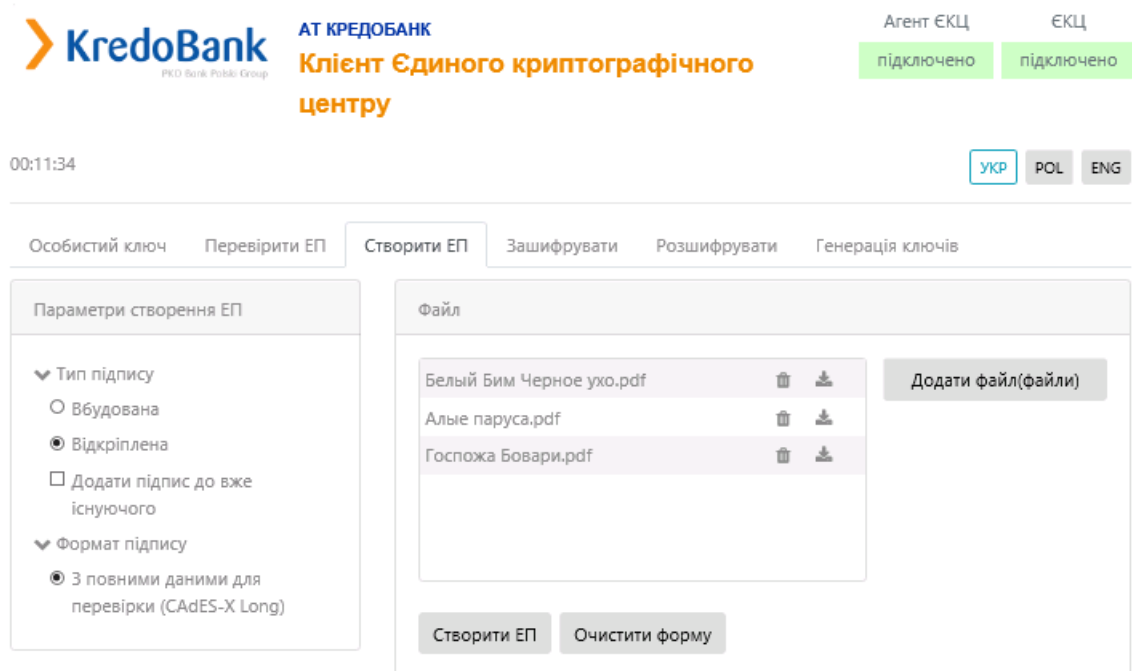


Рис. 32. Збереження підпису у файл

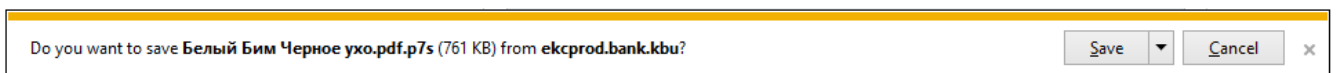


Рис. 33. Збереження файлу

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 (CAAdES-X Long), тип кодування, вказується текст для підпису, натискаємо кнопку «Створити ЕП», Рис. 34.

Особистий ключ Перевірити ЕП **Створити ЕП** Зашифрувати Розшифрувати Генерація ключів

Параметри створення ЕП

▼ Тип підпису

Вбудована

Відкріплена

Додати підпис до вже існуючого

▼ Формат підпису

З повними даними для перевірки (CAAdES-X Long)

Файл

Додати файл(файли)

Створити ЕП Очистити форму

Текстові дані

Кодування: UTF-16LE UTF-8

Текстові дані для підпису:

123

Додатковий опис:

Створити ЕП Очистити форму

Підпис у кодуванні Base64:

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.

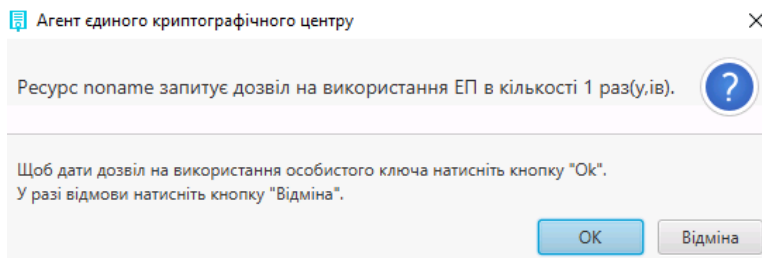


Рис. 35. Дозвіл на використання ЕП

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

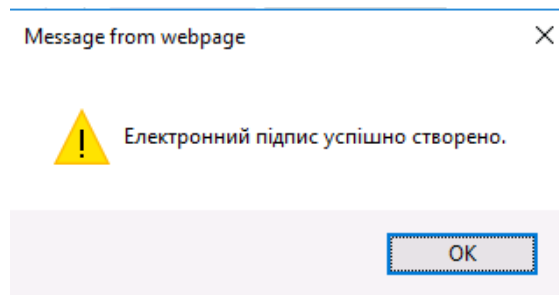


Рис. 36. Повідомлення про створення електронного підпису

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

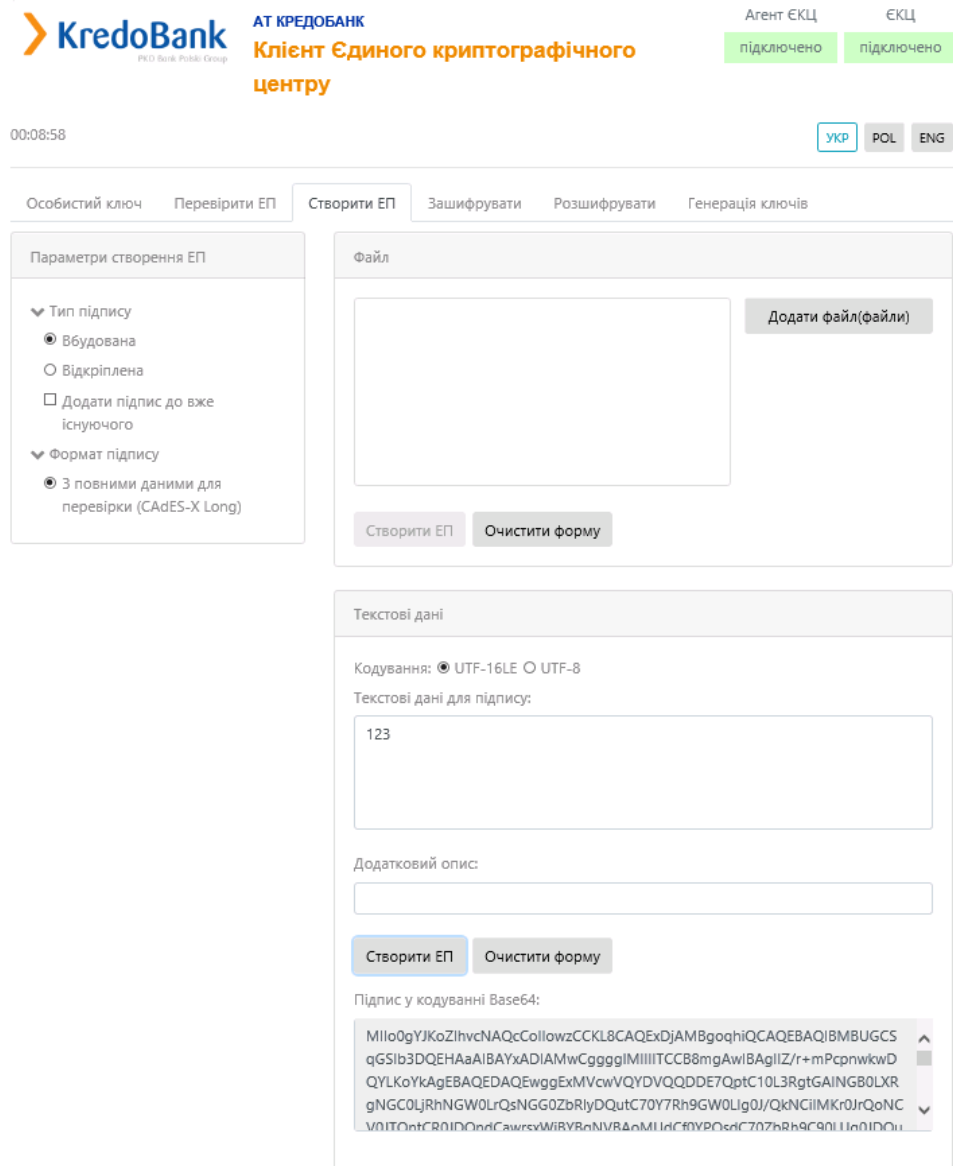


Рис. 37. Результат підпису тестових даних

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 (CAAdES-X Long), обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 38.

00:08:31

Агент ЕКЦ підключено ЕКЦ підключено

УКР POL ENG

Особистий ключ Перевірити ЕП **Створити ЕП** Зашифрувати Розшифрувати Генерація ключів

Параметри створення ЕП

▼ Тип підпису

- Вбудована
- Відкріплена
- Додати підпис до вже існуючого

▼ Формат підпису

- З повними даними для перевірки (CAAdES-X Long)

Файл

Додати файл(файли)

Створити ЕП Очистити форму

Текстові дані

Кодування: UTF-16LE UTF-8

Текстові дані для підпису:

123

Додатковий опис:

Створити ЕП Очистити форму

Підпис у кодуванні Base64:

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.

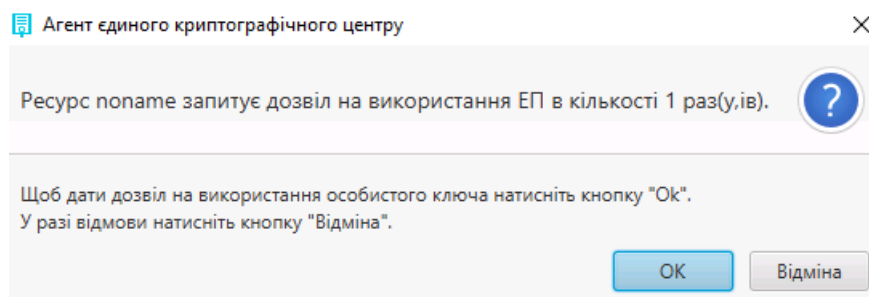


Рис. 39. Дозвіл на використання ЕП

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

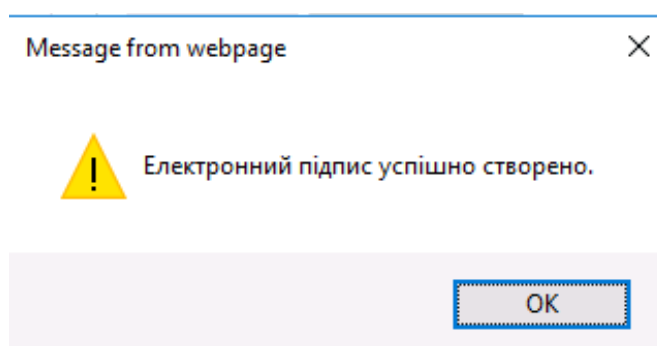


Рис. 40. Повідомлення про створення електронного підпису

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

Особистий ключ Перевірити ЕП **Створити ЕП** Зашифрувати Розшифрувати Генерація ключів

Параметри створення ЕП

▼ Тип підпису

Вбудована

Відкріплена

Додати підпис до вже існуючого

▼ Формат підпису

З повними даними для перевірки (CAAdES-X Long)

Файл

Додати файл(файли)

Створити ЕП **Очистити форму**

Текстові дані

Кодування: UTF-16LE UTF-8

Текстові дані для підпису:

Додатковий опис:

Створити ЕП **Очистити форму**

Підпис у кодуванні Base64:

```
MIloYAYJKoZiHvcNAQcCollouTCCKLUCAQExDjAMBgoqhiQCAQEBAQIBMAsgCSq
GSib3DQEHAaCCCCUwggghMIIHyaADAgECAghn+v6Y9ymfCTANBgsqhiQCAQEB
AQMBATCCATEXVzBVBgNVBAMMTtCm0LXQvdGCOYAg0YHQtdGA0YLUQuNGE0Z
bQutCw0YbRltGXINC60LvRjtGH0ZbQsiDQn9CQ0KlgwqvQmtCg0JXQINCe0JHQk
NCd0lrCuzFaMEFCA1UEFCcyR0I/Rn9Cyx0LvRlHGh0I.3O+SDOkNC60YbRltC+0I.3Otd
```

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»

Особистий ключ **Перевірити ЕП** Створити ЕП Зашифрувати Розшифрувати Генерація ключів

Параметри перевірки підпису

▼ Тип підпису

Вбудована

Відкріплена

➤ Режим перевірки електронної позначки часу для підпису

➤ Режим перевірки електронної позначки часу для даних

Розширення ЕП

Файл

Файл для перевірки:

 Вибрати файл

Файл з підписом:

 Вибрати файл

Перевірити ЕП Очистити форму

Зберегти розширений підпис

Текстові дані

Кодування: UTF-16LE UTF-8

Текстові дані для перевірки:

Електронний підпис в кодуванні Base64:

Перевірити ЕП Очистити форму

Розширений підпис у кодуванні Base64:

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 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/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.

Особистий ключ **Перевірити ЕП** Створити ЕП Зашифрувати Розшифрувати Генерація ключів

Параметри перевірки підпису

▼ Тип підпису

Вбудована

Відкріплена

➤ Режим перевірки електронної позначки часу для підпису

➤ Режим перевірки електронної позначки часу для даних

Розширення ЕП

Файл

Файл з підписом:

18822049.pdf.p7s [Змінити файл](#) [Очистити](#)

Зберегти підписані дані

[Перевірити ЕП](#) [Очистити форму](#)

Текстові дані

Кодування: UTF-16LE UTF-8

Електронний підпис в кодуванні Base64:

Дані з електронного підпису:

[Перевірити ЕП](#) [Очистити форму](#)

Рис. 44. Перевірка ЕП

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

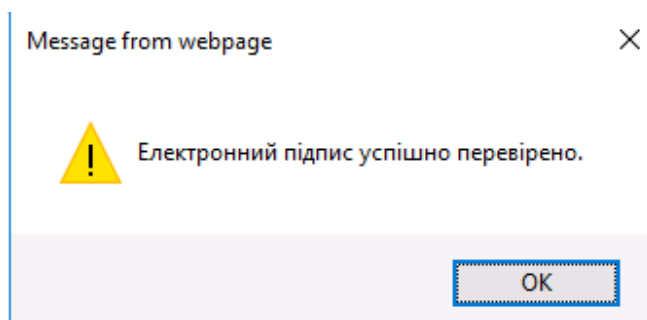


Рис. 45. Повідомлення про дійсність електронного підпису

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».

Особистий ключ **Перевірити ЕП** Створити ЕП Зашифрувати Розшифрувати Генерація ключів

Параметри перевірки підпису

▼ Тип підпису

Вбудована

Відкріплена

➤ Режим перевірки електронної позначки часу для підпису

➤ Режим перевірки електронної позначки часу для даних

Розширення ЕП

Файл

Файл з підписом:

18822049.pdf.p7s Змінити файл Очистити

Підпис 1
Дійсний

Підписувач: КОВТУН СВІТЛАНА ЮРІВНА
ІПН: 3504904142
Серт. СН: 2B6C7DF9A3B91DA10400000FAD3300061951601
КНЕДП/АЦСК: АЦСК АТ КБ «ПРИВАТБАНК»
Дата підпису: 29.08.2019 17:41:55
Електронна позначка часу підпису: дійсна; 29.08.2019 17:41:55

Зберегти підписані дані

Перевірити ЕП 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.

АТ КРЕДОБАНК Клієнт Єдиного криптографічного центру

Агент ЕКЦ ЕКЦ
підключено підключено

00:12:11 УКР POL ENG

Особистий ключ **Перевірити ЕП** Створити ЕП Зашифрувати Розшифрувати Генерація ключів

Параметри перевірки підпису

▼ Тип підпису

Вбудована

Відкріплена

➤ Режим перевірки електронної позначки часу для підпису

➤ Режим перевірки електронної позначки часу для даних

Розширення ЕП

Файл

Файл для перевірки:

crt-crypt-AB.txt Змінити файл Очистити

Файл з підписом:

crt-crypt-AB.txt (1).p7s Змінити файл Очистити

Перевірити ЕП Очистити форму

Рис. 47. Перевірка ЕП

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

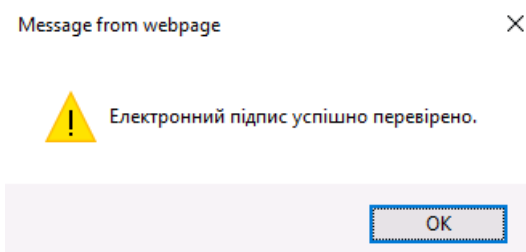


Рис. 48. Повідомлення про дійсність електронного підпису

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

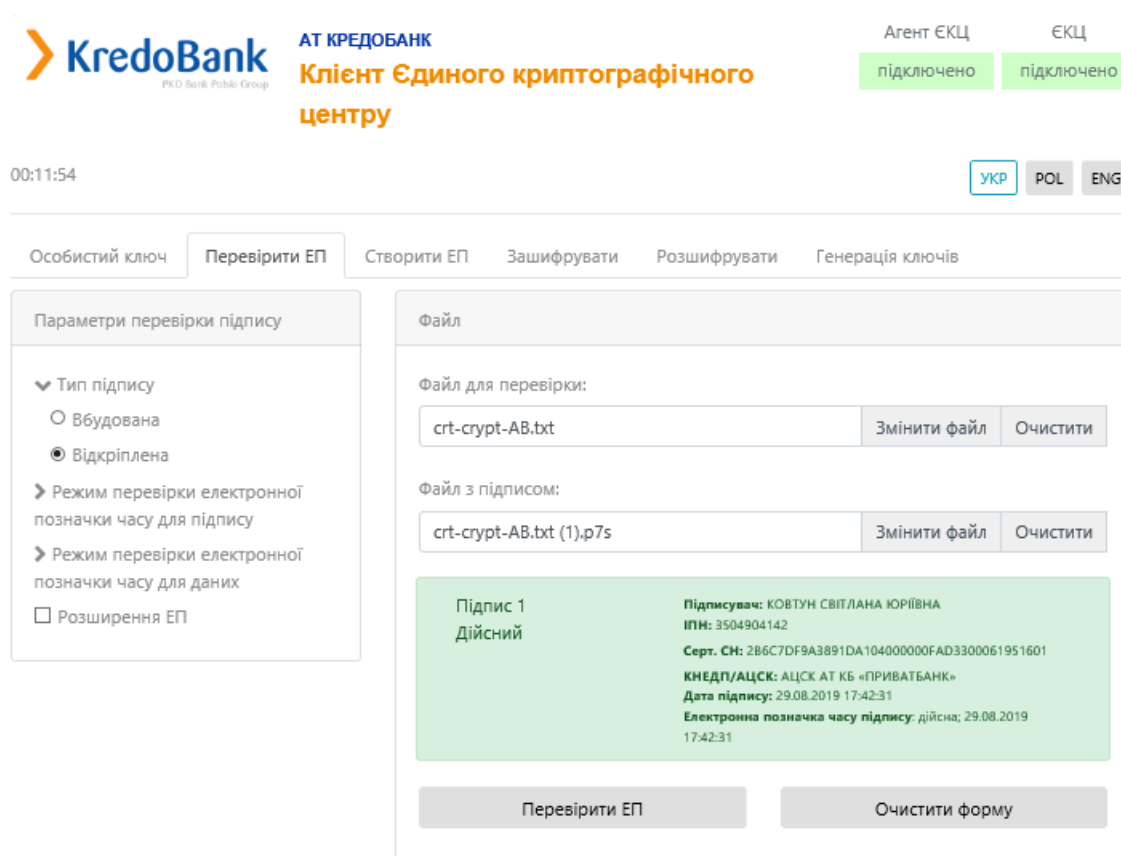


Рис. 49. Результат перевірки

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.

Особистий ключ **Перевірити ЕП** Створити ЕП Зашифрувати Розшифрувати Генерація ключів

Параметри перевірки підпису

- Тип підпису
 - Вбудована
 - Відкріплена
- Режим перевірки електронної позначки часу для підпису
- Режим перевірки електронної позначки часу для даних
- Розширення ЕП

Файл

Файл з підписом:

Текстові дані

Кодування: UTF-16LE UTF-8

Електронний підпис в кодуванні Base64:

Дані з електронного підпису:

Рис. 50. Перевірка ЕП

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

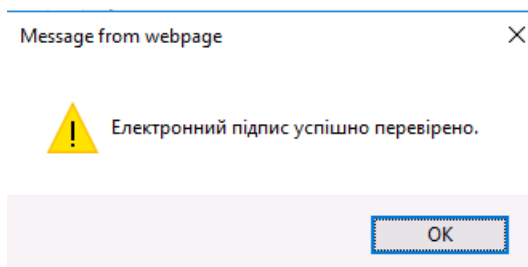


Рис. 51. Повідомлення про дійсність електронного підпису

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

Особистий ключ
Перевірити ЕП
Створити ЕП
Зашифрувати
Розшифрувати
Генерація ключів

Параметри перевірки підпису

▼ Тип підпису

Вбудована

Відкріплена

➤ Режим перевірки електронної позначки часу для підпису

➤ Режим перевірки електронної позначки часу для даних

Розширення ЕП

Файл

Файл з підписом:

Вибрати файл

Зберегти підписані дані

Перевірити ЕП
Очистити форму

Текстові дані

Кодування: UTF-16LE UTF-8

Електронний підпис в кодуванні Base64:

A1UEBwwl0JrQuNGX0LICFDO2y3v3lbnOBAAAALH6JQAbvVsAMA0GCyqGJAIBAQ
 EBAwEBBEDFJDHo/8grRG96BZ6uaFCsYcLGThp2dZBX7PA6jc+wfgQFN1P63whiKA
 Oe265wkQopzKt6ZxWhUZNXCrj19Un

Дані з електронного підпису:

123

Підпис 1
Дійсний

Підписувач: Ковтун Світлана Юріана
ІПН: 3504904142
ЄДРПОУ: 3504904142
Серт. СН: 33B6CB7BF721B9CE0400000B1FA25001BBD5B00
КНЕДП/АЦСК: Акредитований центр сертифікації ключів ЦДД
 ДФС
Дата підпису: 22.09.2019 18:39:35

Перевірити ЕП
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.

Особистий ключ | **Перевірити ЕП** | Створити ЕП | Зашифрувати | Розшифрувати | Генерація ключів

Параметри перевірки підпису

- ▼ Тип підпису
 - Вбудована
 - Відкріплена
- Режим перевірки електронної позначки часу для підпису
- Режим перевірки електронної позначки часу для даних
- Розширення ЕП

Файл

Файл для перевірки:

 Вибрати файл

Файл з підписом:

 Вибрати файл

Перевірити ЕП Очистити форму

Текстові дані

Кодування: UTF-16LE UTF-8

Текстові дані для перевірки:

Електронний підпис в кодуванні Base64:

```
QsgIU7bLe/chuc4EAAAAsfolABu9WwAwDQYLKoYkAgEBAQEDAQEEQEMs+SIX
pIFvU+B4QwwqheOLYPRbpuroMIP7PLNKtThTPJmoXoCmA4WGz3HiXkPtc+jLfXq
bmsCJPJaUsqEclik=
```

Перевірити ЕП Очистити форму

Рис. 53. Перевірка ЕП

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

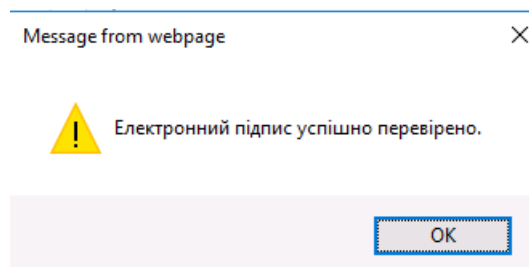


Рис. 54. Повідомлення про дійсність електронного підпису

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

Особистий ключ **Перевірити ЕП** Створити ЕП Зашифрувати Розшифрувати Генерація ключів

Параметри перевірки підпису

▼ Тип підпису

Вбудована

Відкріплена

➤ Режим перевірки електронної позначки часу для підпису

➤ Режим перевірки електронної позначки часу для даних

Розширення ЕП

Файл

Файл для перевірки:

 Вибрати файл

Файл з підписом:

 Вибрати файл

Перевірити ЕП Очистити форму

Текстові дані

Кодування: UTF-16LE UTF-8

Текстові дані для перевірки:

Електронний підпис в кодуванні Base64:

```
QsglUM7bLe/chuc4EAAAAsfolABu9WwAwDQYLKoYkAgEBAQEDAQEEQEMs+SIX
plFvU+B4QwwqheOLYPRbpuroMIP7PLNKtThTPJmoXoCmA4WGz3HIXkPtc+jLfxQ
bmsCJPJaUsqEclik=
```

Підпис 1
Дійсний

Підписувач: Ковтун Світлана Юріївна
ІПН: 3504904142
ЄДРПОУ: 3504904142
Серт. СН: 33B6CB78F721B9CE040000081FA250018BD5800
КНЕДП/АЦСК: Акредитований центр сертифікації ключів ІДД
ДФС
Дата підпису: 22.09.2019 18:40:38

Перевірити ЕП 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.

Особистий ключ

Перевірити ЕП

Генерація ключів

Параметри перевірки підпису

▼ Тип підпису

 Вбудована Відкріплена➤ Режим перевірки електронної
позначки часу для підпису➤ Режим перевірки електронної
позначки часу для даних Розширення ЕП

Файл

Файл з підписом:

att-base.p7s

Змінити файл

Очистити

Зберегти підписані дані

Перевірити ЕП

Очистити форму

Рис. 56. Перевірка ЕП

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

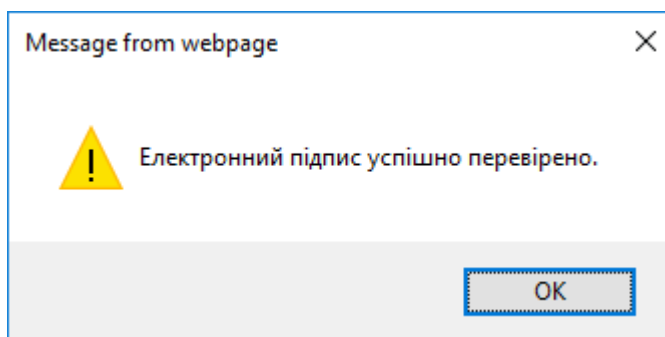


Рис. 57. Повідомлення про перевірку електронного підпису

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».

Особистий ключ **Перевірити ЕП** Генерація ключів

Параметри перевірки підпису

- ▼ Тип підпису
 - Вбудована
 - Відкріплена
- Режим перевірки електронної позначки часу для підпису
- Режим перевірки електронної позначки часу для даних
- Розширення ЕП

Файл

Файл з підписом:

att-base.p7s
Змінити файл
Очистити

<p>Підпис 1 Дійсний</p>	<p>Підписувач: Боровіков Олександр Михайлович ІПН: 2031914098 Серт. СН: 2084E4ED0D30998C0400000006FC24004DAD7500 КНЕДП/АЦСК: Акредитований центр сертифікації ключів ІДД ДФС Дата підпису: 05.09.2019 12:15:02 Електронна позначка часу підпису: відсутня</p>
------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Шановний користувач!

Звертаємо Вашу увагу на те, що із набуттям чинності від 07.11.2018 Закону України «Про електронні довірчі послуги» та відповідно до частини четвертої статті 26 цього Закону, використання електронної позначки часу для постійного зберігання електронних даних є обов'язковим.

Даний документ не містить електронної позначки часу і не може зберігатися з гарантованою можливістю перевірки електронного підпису.

Зберегти підписані дані

Перевірити ЕП
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.

Особистий ключ **Перевірити ЕП** Створити ЕП Зашифрувати Розшифрувати Генерація ключів

Параметри перевірки підпису

▼ Тип підпису

Вбудована

Відкріплена

➤ Режим перевірки електронної позначки часу для підпису

➤ Режим перевірки електронної позначки часу для даних

Розширення ЕП

Файл

Файл з підписом:

Вибрати файл

Зберегти підписані дані

Перевірити ЕП

Очистити форму

Зберегти розширений підпис

Текстові дані

Кодування: UTF-16LE UTF-8

Електронний підпис в кодуванні Base64:

Дані з електронного підпису:

Перевірити ЕП

Очистити форму

Розширений підпис у кодуванні Base64:

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.

Особистий ключ **Перевірити ЕП** Створити ЕП Зашифрувати Розшифрувати Генерація ключів

Параметри перевірки підпису

- Тип підпису
 - Вбудована
 - Відкріплена
- Режим перевірки електронної позначки часу для підпису
- Режим перевірки електронної позначки часу для даних
- Розширення ЕП

Файл

Файл з підписом:

att-base.p7s

Рис. 60. Розширення вбудованого ЕП

Отримати повідомлення про успішне розширення підпису, Рис. 61.

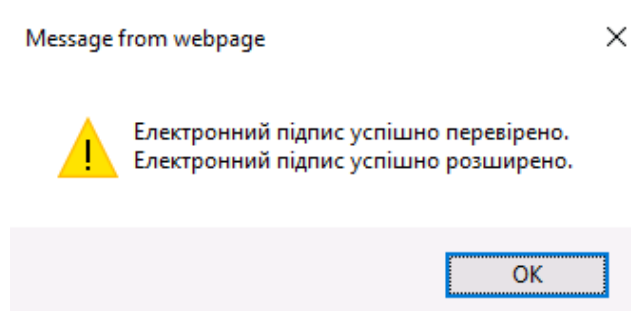


Рис. 61. Повідомлення про результат перевірки та розширення ЕП

Отримати результат перевірки електронного підпису, Рис. 62.

Особистий ключ

Перевірити ЕП

Створити ЕП

Зашифрувати

Розшифрувати

Генерація ключів

Параметри перевірки підпису

▼ Тип підпису

Вбудована

Відкріплена

► Режим перевірки електронної позначки часу для підпису

► Режим перевірки електронної позначки часу для даних

Розширення ЕП

Файл

Файл з підписом:

att-base.p7s

Змінити файл

Очистити

Підпис 1
Дійсний

Підписувач: КОВТУН СВІТЛАНА ЮРІВНА
ІПН: 3504904142
Серт. СН: 2B6C7DF9A3891DA10400000FAD3300061951601
КНЕДП/АЦСК: АЦСК АТ КБ «ПРИВАТБАНК»
Дата підпису: 05.09.2019 10:31:26

Зберегти підписані дані

Перевірити ЕП

Очистити форму

Зберегти розширений підпис

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.

Особистий ключ

Перевірити ЕП

Генерація ключів

Параметри перевірки підпису

▼ Тип підпису

Вбудована

Відкріплена

► Режим перевірки електронної позначки часу для підпису

► Режим перевірки електронної позначки часу для даних

Розширення ЕП

Файл

Файл з підписом:

att-long.p7s

Змінити файл

Очистити

Підпис містить повні дані для перевірки (CAvES-X Long). Розширювати електронний підпис не потрібно.

Підпис 1
Дійсний

Підписувач: Боровіков Олександр Михайлович
ІПН: 2031914098
Серт. СН: 2084E4ED0D30998C040000006FC24004DAD7500
КНЕДП/АЦСК: Акрредитований центр сертифікації ключів ІДД ДФС
Дата підпису: 05.09.2019 12:49:36
Електронна позначка часу підпису: дійсна: 05.09.2019 12:49:36

Зберегти підписані дані

Перевірити ЕП

Очистити форму

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.

AT КРЕДОБАНК
Клієнт Єдиного криптографічного центру

Агент ЕКЦ підключено
ЕКЦ підключено

UKR POL ENG

Особистий ключ | **Перевірити ЕП** | Генерація ключів

Параметри перевірки підпису

- Тип підпису
 - Вбудована
 - Відкріплена
- Режим перевірки електронної позначки часу для підпису
- Режим перевірки електронної позначки часу для даних
- Розширення ЕП

Файл

Файл для перевірки:

Файл з підписом:

Текстові дані

Кодування: UTF-16LE UTF-8

Текстові дані для перевірки:

Електронний підпис в кодуванні Base64:

```
QsglUM7bLe/chuc4EAAAAsfolABu9WwAwDQYLKoYkAgEBAQEDAQEEQEMs+SIX  
plFvU+B4QwwqheOLYPRbpuroMIP7PLNKtThTPJmoXoCmA4WGz3HixkPtc+jLfxq  
bmsCJPJaUsqEclik=
```

Рис. 64. Розширення відкріпленого ЕП

Отримати повідомлення про успішне розширення підпису, Рис. 65.

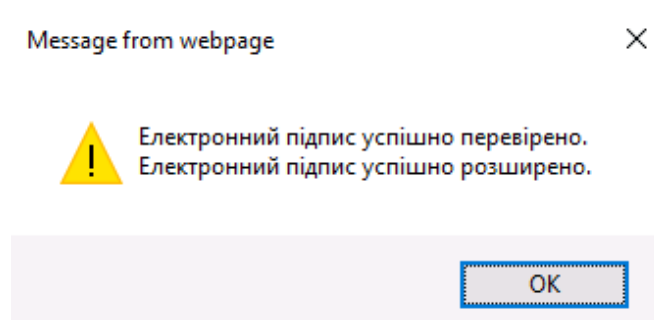


Рис. 65. Повідомлення про перевірку та розширення підпису

Отримати результат перевірки електронного підпису, Рис. 66.

KredoBank АТ КРЕДОБАНК
Клієнт Єдиного криптографічного центру

Агент ЕКЦ підключено ЕКЦ підключено

УКР POL ENG

Особистий ключ | **Перевірити ЕП** | Генерація ключів

Параметри перевірки підпису

- Тип підпису
 - Вбудована
 - Відкріплена
- Режим перевірки електронної позначки часу для підпису
- Режим перевірки електронної позначки часу для даних
- Розширення ЕП

Файл

Файл для перевірки: **Вибрати файл**

Файл з підписом: **Вибрати файл**

Перевірити ЕП **Очистити форму**

Зберегти розширений підпис

Текстові дані

Кодування: UTF-16LE UTF-8

Текстові дані для перевірки:

Електронний підпис в кодуванні Base64:

```
QsgIU7bLe/chuc4EAAAAf0IABu9WwAwDQYLKoYkAgEBAQEDAQEEQEMs+SIX  
pIFvU+B4QwwqheOLYPRbpuroMIP7PLNKtThTPJmoXoCmA4WGz3HIXkPtc+jLfXq  
bmsCJPJaUsqEclik=
```

Підпис 1
Дійсний

Підписувач: Ковтун Світлана Юрівна
ІПН: 3504904142
ЄДРПОУ: 3504904142
Серт. СН: 33B6CB7BF721B9CE0400000B1FA25001BBD5B00
КНЕДП/АЦСК: Акредитований центр сертифікації ключів ІДД
ДФС
Дата підпису: 22.09.2019 18:40:38

Перевірити ЕП **Очистити форму**

Розширений підпис у кодуванні Base64:

```
MllrnwYJKoZlhvcNAQcCollrkDCCK4wCAQExDjAMBgoqhiQCAQEBAQIBMAAsGCSq  
GSib3DQEHATGCK2gwgitikAgEBMIIlBajCCAVAXVDBS8gNVBAoMS9CGOL3RhNC+  
0YDQvNCw0YbRitC50L3Qvi3QtNC+0LLRitC00LrQvtCy0LjQuSDQtNC10L/QsNGA0
```

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.

Особистий ключ

Перевірити ЕП

Генерація ключів

Параметри перевірки підпису

▼ Тип підпису

 Вбудована

 Відкріплена

▶ Режим перевірки електронної позначки часу для підпису

▶ Режим перевірки електронної позначки часу для даних

 Розширення ЕП

Файл

Файл для перевірки:

 Вибрати файл

Файл з підписом:

 Вибрати файл

Перевірити ЕП

Очистити форму

Текстові дані

 Кодування: UTF-16LE UTF-8

Текстові дані для перевірки:

Електронний підпис в кодуванні Base64:

```
qGJAIBAQEBAwEBA28ABGzxeG8e3aw8c82AAYQd92NDEPvzeRbj5e32lcf3rFeZ+Q
14OU82al82XiAgeSRzy3G3XgqumhsL17IMm7d+M6n+yyrpb6tKxTWH1yVVhR+E4
ObDwPnwkPk9Dt+VTfO9wS4Exs+25xx/aPG548DA=
```

Підпис містить повні дані для перевірки (CAAdES-X Long). Розширювати електронний підпис не потрібно.

 Підпис 1
Дійсний

 Підписувач: Ковтун Світлана Юріївна
ІПН: 3504904142

ЄДРПОУ: 3504904142

Серт. СН: 33B6CB7BF721B9CE040000081FA25001B8D5800

 КНЕДП/АЦСК: Акредитований центр сертифікації ключів ІДД
ДФС

Дата підпису: 23.10.2019 16:18:43

 Електронна позначка часу підпису: дійсна; 23.10.2019
16:18:43

Перевірити ЕП

Очистити форму

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 Агента 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.

The screenshot displays the 'Зашифрувати' (Encrypt) tab of the KredoBank interface. At the top, the KredoBank logo and 'AT КРЕДОБАНК' are visible, along with the text 'Клієнт Єдиного криптографічного центру'. On the right, there are status indicators for 'Агент ЄКЦ' (Agent EKC) and 'ЄКЦ' (EKC), both showing 'підключено' (connected). The time '00:13:32' and language selection buttons ('УКР', 'POL', 'ENG') are also present.

The main content area is divided into several sections:

- Параметри зашифрування** (Encryption parameters): A dropdown menu 'Додати при зашифруванні:' (Add when encrypting:) with three radio button options:
 - Сертифікат відправника та сертифікати видавців (Sender certificate and issuer certificates)
 - Сертифікат відправника (Sender certificate)
 - Не додавати сертифікат відправника та сертифікати видавців (Do not add sender certificate and issuer certificates)
- Сертифікат отримувача** (Recipient certificate): A section titled 'Сертифікат отримувача зашифрованих даних:' (Recipient certificate of encrypted data:) with a text input field and a 'Вибрати файл' (Select file) button.
- Файл** (File): A section with a large empty text area and a 'Додати файл(файли)' (Add file(s)) button.
- Текстові дані** (Text data): A section with a 'Кодування:' (Encoding:) label and two radio button options: 'UTF-16LE' (selected) and 'UTF-8'. Below is a 'Текст для зашифрування:' (Text for encryption:) text input field and 'Зашифрувати' (Encrypt) and 'Очистити форму' (Clear form) buttons. At the bottom, there is a label 'Зашифровані дані у кодуванні Base64:' (Encrypted data in Base64 encoding:) and a large empty text area for the result.

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.

Особистий ключ Перевірити ЕП Створити ЕП **Зашифрувати** Розшифрувати Генерація ключів

Параметри зашифрування

▼ Додати при зашифруванні:


- Сертифікат відправника та сертифікати видавців
- Сертифікат відправника
- Не додавати сертифікат відправника та сертифікати видавців

Сертифікат отримувача

Сертифікат отримувача зашифрованих даних:

key-2-enc.crt Змінити файл Очистити

Файл

Граф Монте-Кристо.pdf  Додати файл(файли)

Зашифрувати Очистити форму

Текстові дані

Кодування: UTF-16LE UTF-8

Текст для зашифрування:

Зашифрувати Очистити форму

Зашифровані дані у кодуванні Base64:

Рис. 69. Процес зашифрування

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



Зашифрування успішно виконано для 1 файлу(ів).

OK

Рис. 70. Повідомлення про успішне зашифрування даних

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

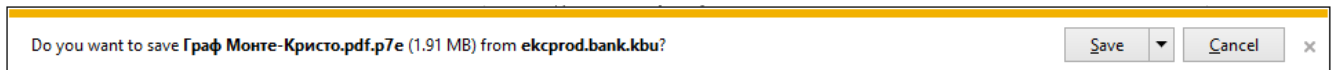


Рис. 71. Збереження зашифрованого файлу

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.

Особистий ключ Перевірити ЕП Створити ЕП **Зашифрувати** Розшифрувати Генерація ключів

Параметри зашифрування

▼ Додати при зашифруванні:

- Сертифікат відправника та сертифікати видавців
- Сертифікат відправника
- Не додавати сертифікат відправника та сертифікати видавців

Сертифікат отримувача

Сертифікат отримувача зашифрованих даних:

key-2-enc.crt Змінити файл Очистити

Файл

Додати файл(файли)

Зашифрувати Очистити форму

Текстові дані

Кодування: UTF-16LE UTF-8

Текст для зашифрування:

123

Зашифрувати Очистити форму

Зашифровані дані у кодуванні Base64:

Рис. 72. Процес зашифрування

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

Особистий ключ Перевірити ЕП Створити ЕП **Зашифрувати** Розшифрувати Генерація ключів

Параметри зашифрування

▼ Додати при зашифруванні:

- Сертифікат відправника та сертифікати видавців
- Сертифікат відправника
- Не додавати сертифікат відправника та сертифікати видавців

Сертифікат отримувача

Сертифікат отримувача зашифрованих даних:

Змінити файл Очистити

Файл

Додати файл(файли)

Зашифрувати
Очистити форму

Текстові дані

Кодування: UTF-16LE UTF-8

Текст для зашифрування:

123

Зашифрувати
Очистити форму

Зашифровані дані у кодуванні Base64:

```
MIIQRAYJKoZlhvNAQcDollQNTCCEDCAQKgggyIoIMhDCCBFswggQDoAMCA
QJCCDV/TnWs8o/dMA0GcyqGJAIBAQEBAwEBMIIIBMFXMFUGA1UEAwxO0KbQt
dC90YLRgCDRgdC10YDRgtC40YTRItC60LDRhtGW0Zcg0LrQu9GO0YfRitCylNCf0J
DQoiDCq9Ca0KDQldCU0J7QkdCQ0J3QmsK7MVowWAYDVQQKDFHqn9GD0LH
Ou9GW0YfOvdC1INCO0LrRhtGW0L7OvdC10YDQvdC1INCI0L7OstCw0YDQuNGR
```

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: UTF-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.

Файл

Файл для розшифрування: Змінити файл Очистити

Розшифрувати Зберегти розшифровані дані у файл Очистити форму

Текстові дані

Кодування: UTF-16LE UTF-8

Зашифровані дані у кодуванні Base64:

Розшифрувати Очистити форму

Розшифрований текст:

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.

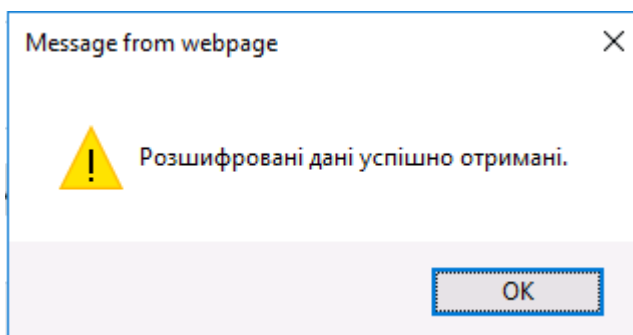


Рис. 76. Повідомлення про успішне розшифрування даних



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.

00:12:39

Агент ЕКЦ підключено ЕКЦ підключено

УКР POL ENG

Особистий ключ Перевірити ЕП Створити ЕП Зашифрувати **Розшифрувати** Генерація ключів

Файл

Файл для розшифрування: Вибрати файл

Розшифрувати Зберегти розшифровані дані у файл Очистити форму

Текстові дані

Кодування: UTF-16LE UTF-8

Зашифровані дані у кодуванні Base64:

```
RjNC60LAXCzAJBgNVBAYTAiVBMRkwFwYDVQQFEhBVQS0wOTgwNzg2Mi0wMDAyAgkA9yxuaCaWXHIELAUN0DJ2g9gHXHmLtBe  
Yv4Q/hGqM7muwkuX7bFFJ1Di0yhzkskR/O0Tz0y/LMHAGCSqGSIb3DQEHAATBbBgsqhiQCAQEBAQEBAzBMBAl6QYRZS4gdfQRAqd  
brRfE8clKAxJZ7lx9erfZY66TANykdONlr8CXKThf46XINxhW0OiiXXwvB3qNkOLV6kiwXn9ASpm24+sV5BIAg04zKh0eG
```

Розшифрувати Очистити форму

Розшифрований текст:

Рис. 78. Процес розшифрування

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

00:12:20

УКР POL ENG

Особистий ключ Перевірити ЕП Створити ЕП Зашифрувати **Розшифрувати** Генерація ключів

Файл

Файл для розшифрування: Вибрати файл

Розшифрувати Зберегти розшифровані дані у файл Очистити форму

Текстові дані

Кодування: UTF-16LE UTF-8

Зашифровані дані у кодуванні Base64:

```
RjNC60LAXCzAJBgNVBAYTAiVBMRkwFwYDVQQFEyBVS0wOTgwNzg2Mi0wMDAyAgkA9yxuaCaWXHIELAUN0DJ2g9gHXHmLtBe  
Yv4Q/hGqM7muwkuX7bFFJ1Di0yhzkskR/O0Tz0y/LMHAGCSqGSIb3DQEhATBbBgsqhiQCAQEBAQEBAzBMBAi6QYRZS4gdfQRAqd  
brRfE8clKAxJZ7lx9erfZY66TANykdONlr8CXKThf46XINxhW0OiiXxwvB3qNkOLV6iwXn9ASpm24+sV5BIAG04zKh0eG
```

Розшифрувати Очистити форму

Розшифрований текст:

123

Рис. 79. Розшифровані текстові дані