

Товариство з обмеженою відповідальністю «С.І.Т»

Засіб криптографічного захисту інформації

ЗDA CA CLIENT

Настанова користувача

версія 2.0.20

Київ 2026

Терміни та скорочення

Ключ – особистий ключ;

Сертифікат – сертифікат відкритого ключа;

ЗНКІ – захищений носій ключової інформації

ПЗ – програмний засіб

СВС – список відкликаних сертифікатів

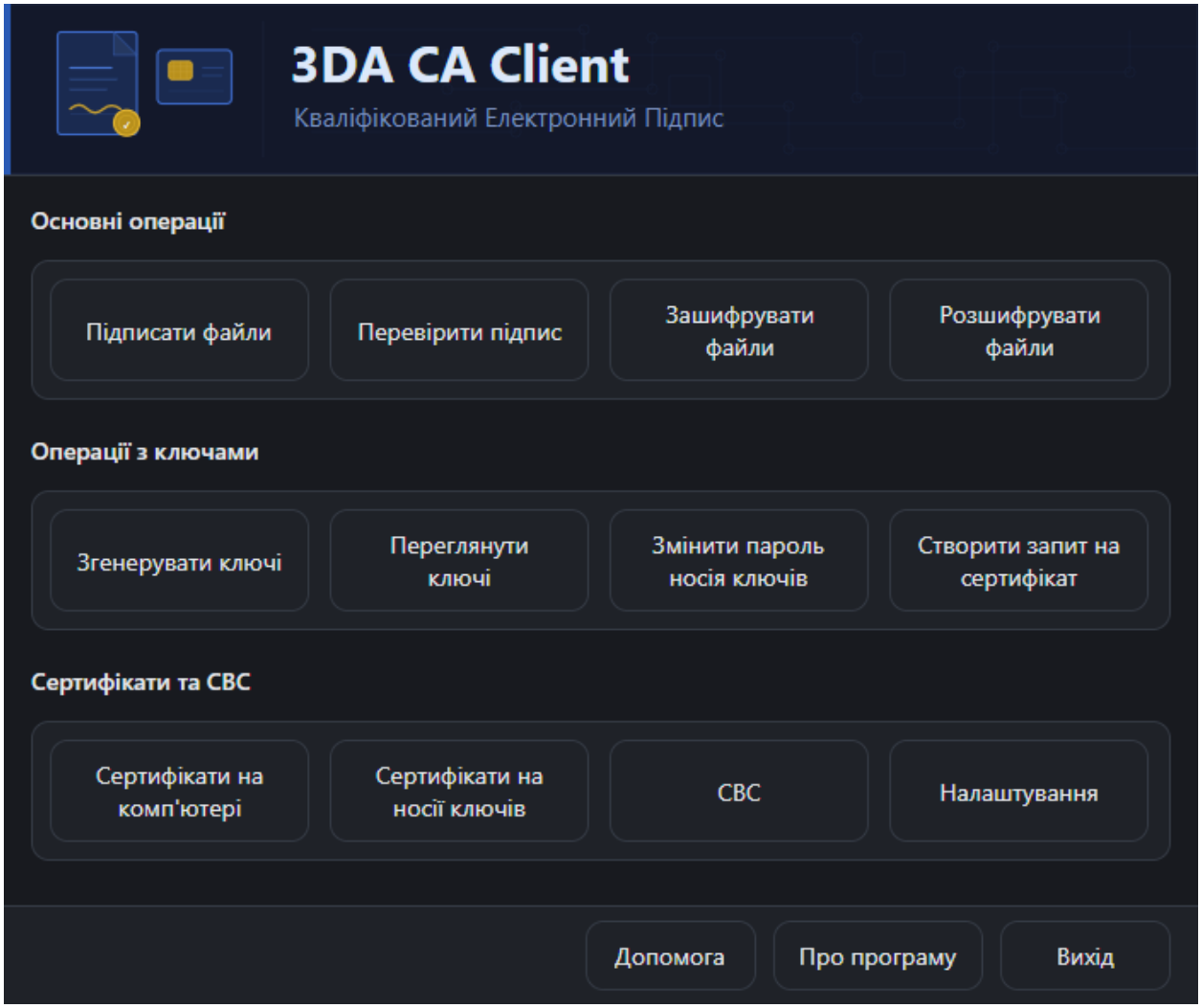
КНЕДП – кваліфікований надавач електронних довірчих послуг

КЕДП – кваліфіковані електронні довірчі послуги

API – Application Programming Interface (прикладний програмний інтерфейс)

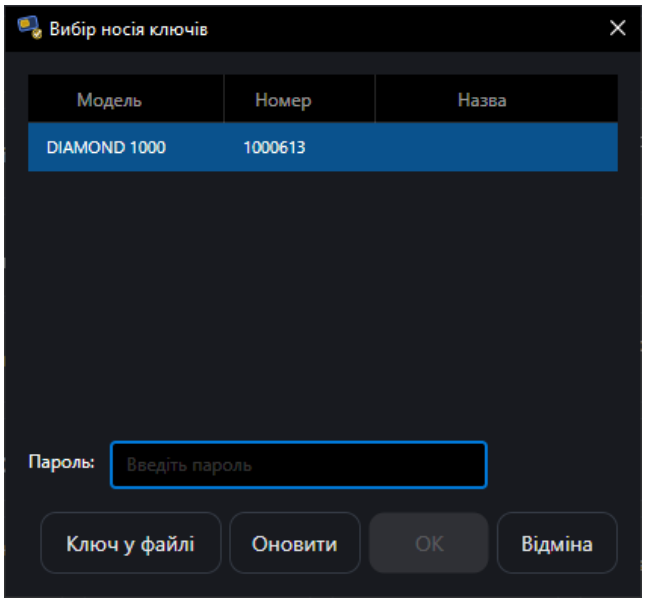
Загальні відомості

Програмний засіб «3DA CA CLIENT» призначений для роботи з ЗНКІ, генерації та знищення ключів, накладання та перевірки підпису, зашифрування та розшифрування файлів. Головне вікно програми має наступний вигляд:



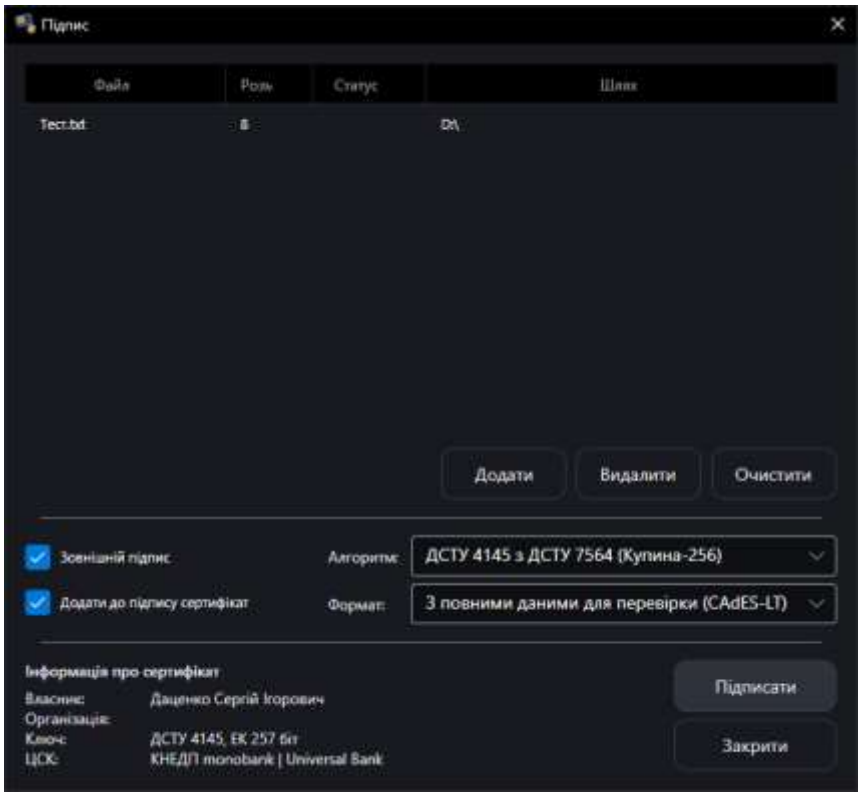
Підпис файлів

Для накладання електронного підпису на електронні документи у вигляді файлів натисніть кнопку «Підписати файли» у головному вікні програми. Після цього оберіть ЗНКІ, введіть пароль до нього та натисніть кнопку «ОК».



У наступному діалоговому вікні, за допомогою кнопки «Додати» або перетягуванням потрібно додати файл (и) для підпису, а також обрати параметри підпису, а саме:

1. Алгоритм підпису
2. Формат підпису
3. Інші параметри

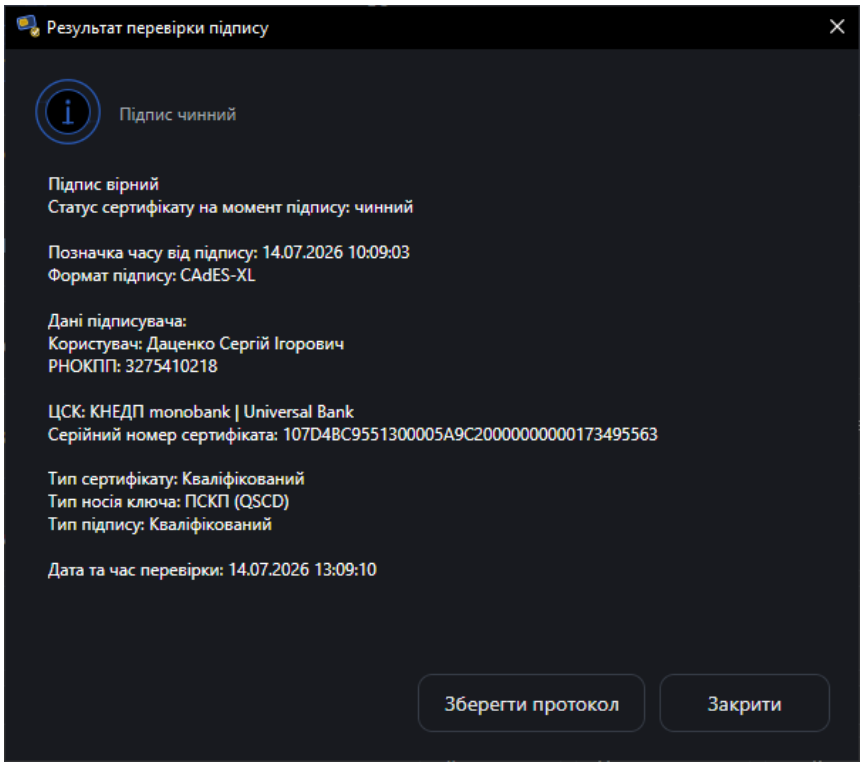


Після завантаження файлу (ів) та вибору всіх необхідних параметрів потрібно натиснути кнопку «Підписати».

У разі успіху буде сформовано підпис (и) у файлі (ах) з додатковим розширенням p7s у тих же каталогах, де знаходилися файли для підпису.

Перевірка підпису

Для перевірки електронного підпису натисніть кнопку «Перевірити підпис» , та у стандартному діалозі вибору файлу, виберіть файл підпису з розширенням p7s, який необхідно перевірити. У діалоговому вікні буде відображено результати перевірки підпису чи можливу помилку, якщо операцію здійснити не можливо.

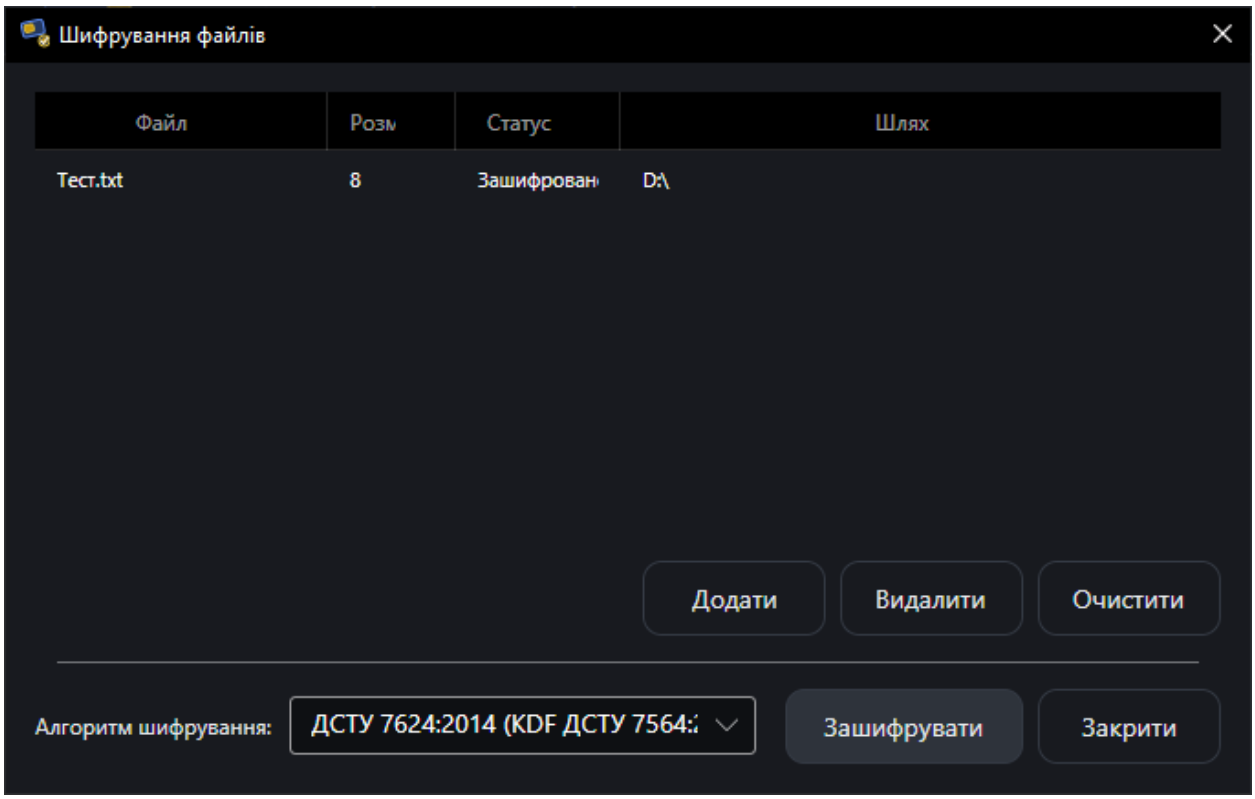


У разі використання підпису з інкапсульованими даними, в каталозі, в якому знаходиться відповідний файл підпису, після його перевірки буде створено файл, що містить інкапсульовані дані без розширення p7s.

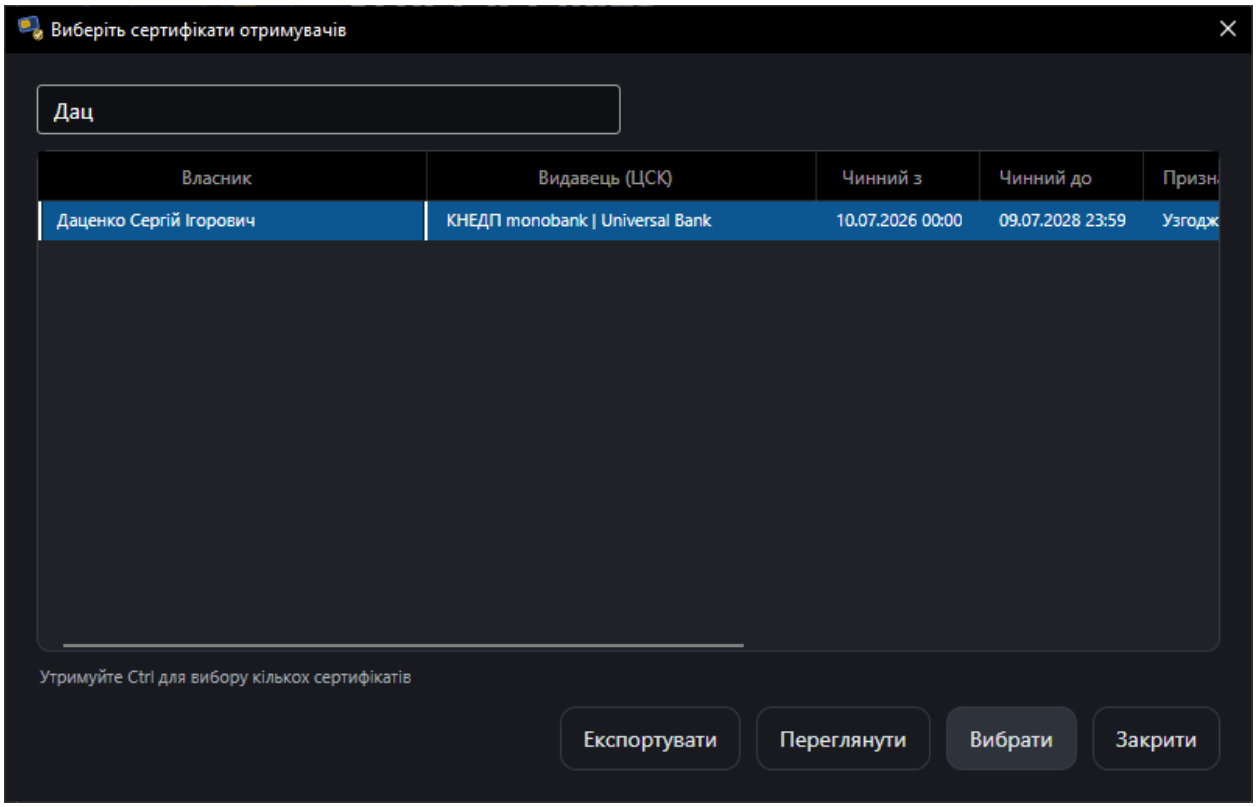
У разі необхідності збереження результатів перевірки підпису, необхідно натиснути кнопку «Зберегти протокол».

Зашифрування файлу

Для зашифрування файлу натисніть кнопку «Зашифрувати файл». У наступному діалоговому вікні, за допомогою кнопки «Додати» або перетягуванням потрібно додати файл (и) для підпису, а також обрати алгоритм шифрування та натиснути кнопку «Зашифрувати».



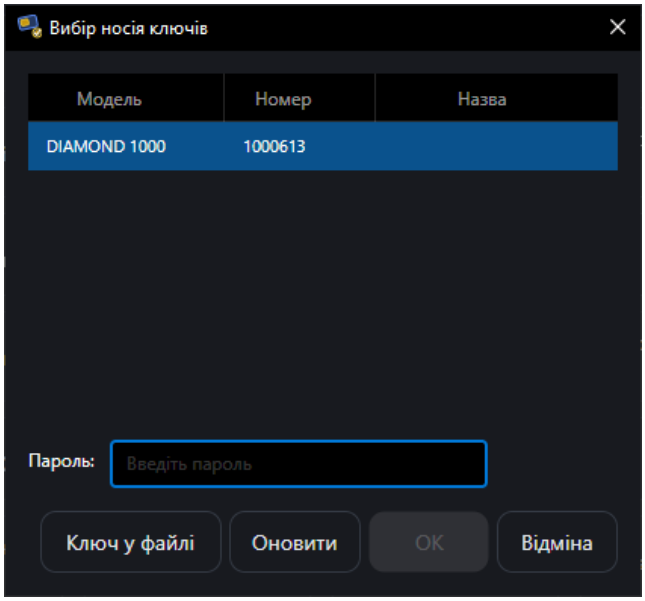
Після цього, у вікні вибору сертифікату отримувача виберіть сертифікат отримувача.



Зашифрований файл буде збережено у тому ж каталозі, що і вхідний файл з додатковим розширенням p7e.

Розшифрування файлу

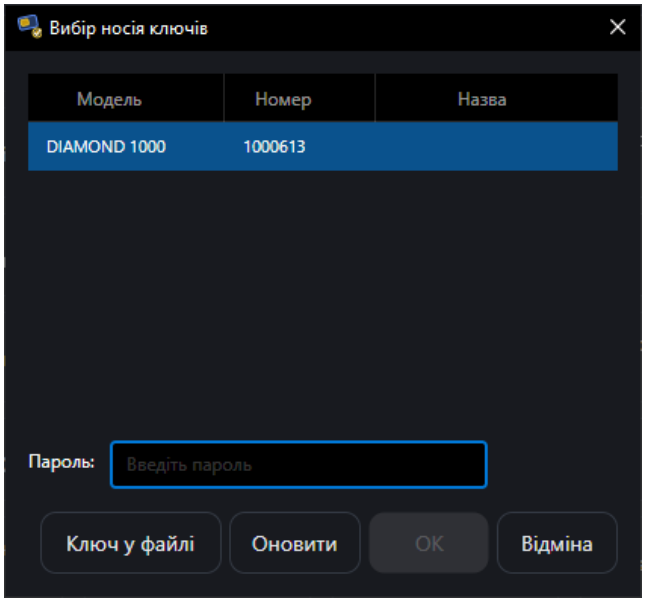
Для розшифрування файлу натисніть кнопку «Розшифрувати файл», та у стандартному діалозі вибору файлу, виберіть файл з розширенням p7e, який необхідно розшифрувати. Після цього оберіть ЗНКІ, на котрому зберігається ключ розшифрування, введіть пароль до нього та натисніть кнопку «ОК».



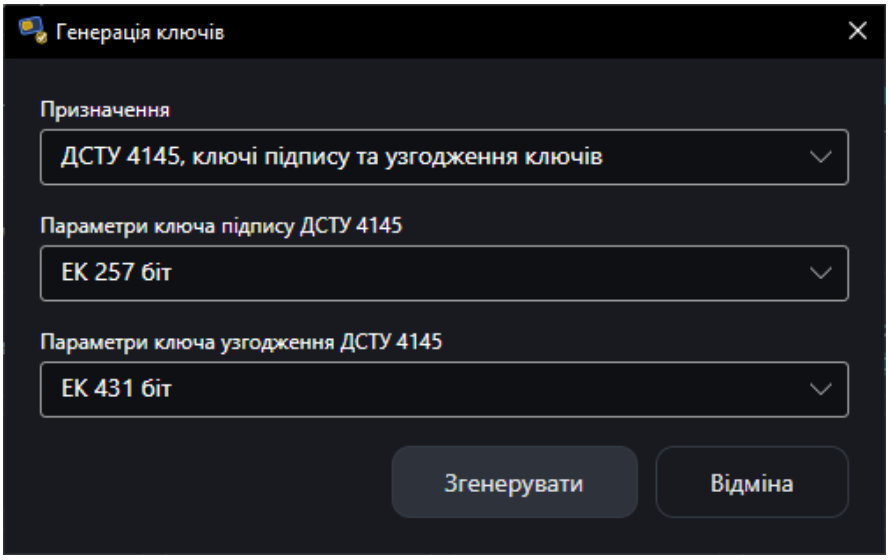
Розшифрований файл буде збережено у тому ж каталозі, що і вхідний файл без розширення p7e.

Генерація ключів

Для того, щоб згенерувати нові ключі натисніть кнопку «Згенерувати ключі». Після цього, оберіть ЗНКІ, введіть пароль до нього та натисніть кнопку «ОК».

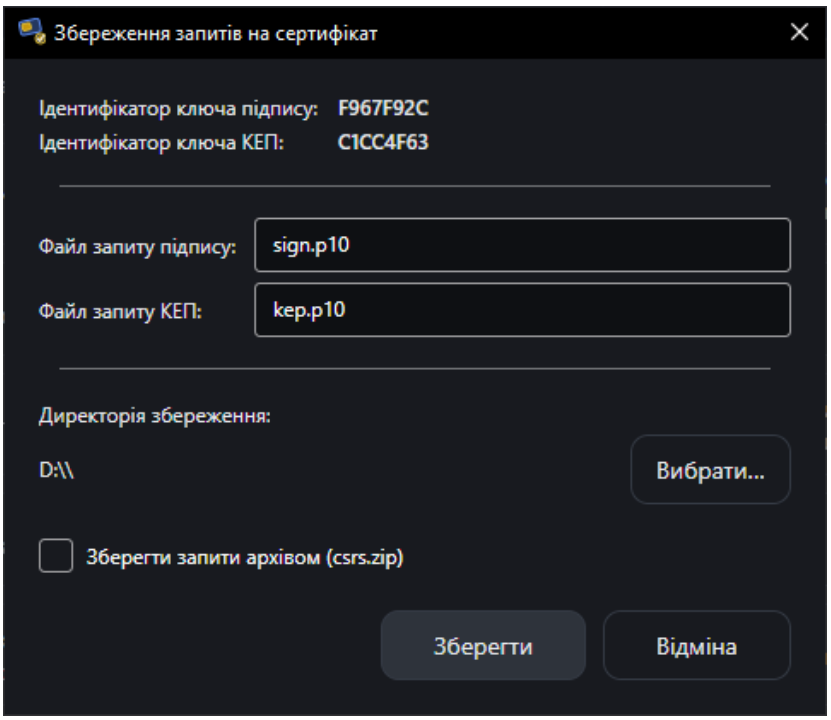


У наступному діалоговому вікні необхідно обрати призначення ключа для генерації:
- ДСТУ 4145, ключі підпису та узгодження ключів;
- ДСТУ 4145, тільки ключ підпису;
- ДСТУ 4145, тільки ключ протоколу узгодження ключів;
- ECDSA, тільки ключ підпису;
- RSA, тільки ключ підпису;



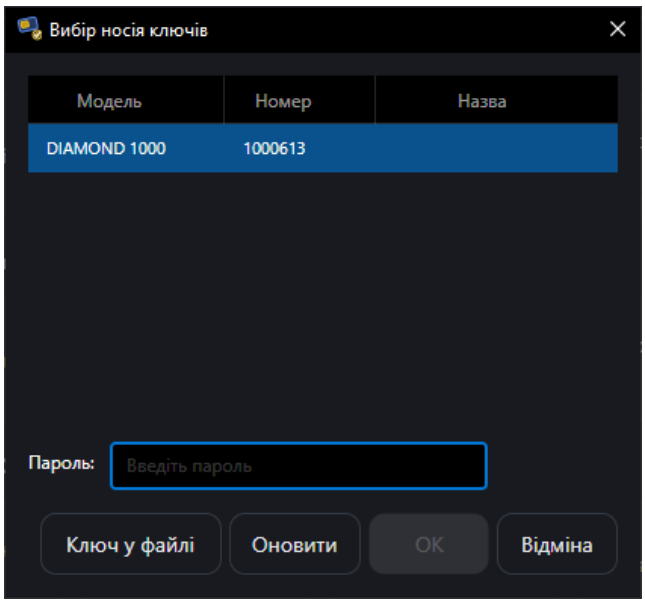
Додатково потрібно обрати параметри необхідних ключів і натиснути кнопку «Згенерувати» або «Відміна» для скасування операції.

Наступне діалогове вікно відображає інформацію про згенеровані ключі, а також дає можливість задати імена запитів на формування сертифікатів та вибору директорії для збереження запитів. Додатково можна встановити прапорець «Зберегти запити архівом (csrs.zip)» для збереження запитів в одному архіві. Після вибору необхідних параметрів необхідно натиснути кнопку «Зберегти» або «Відміна» для скасування операції.

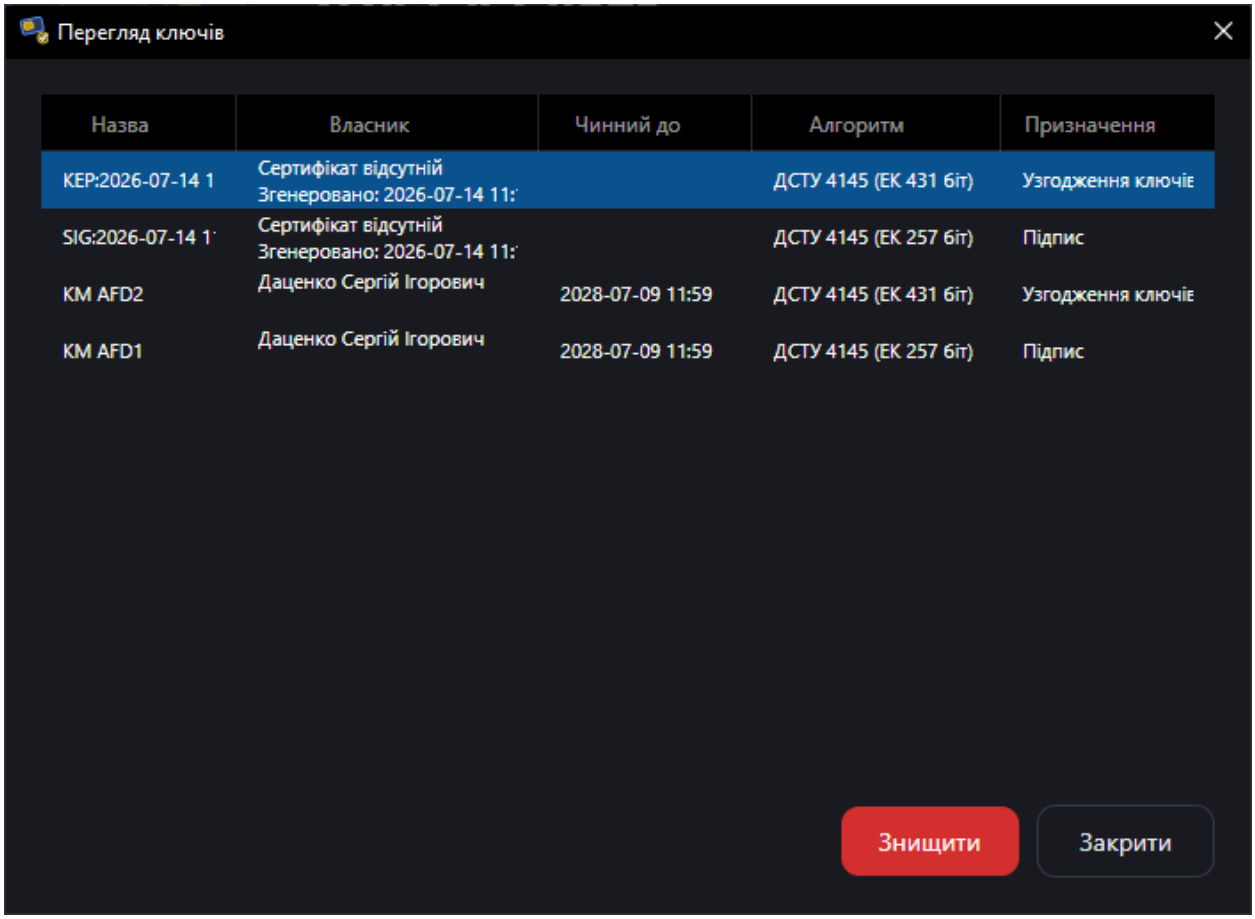


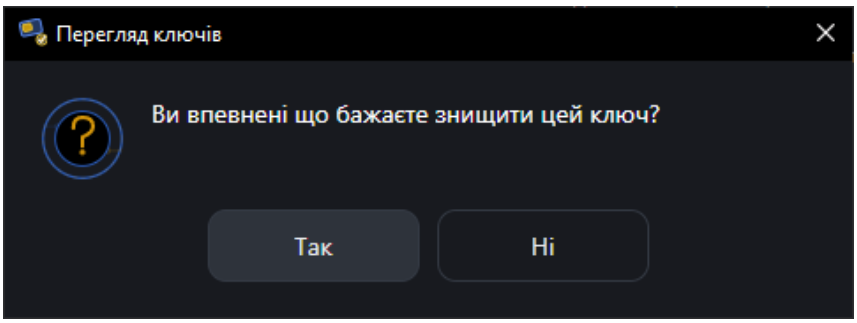
Перегляд та знищення ключів

Для перегляду ключів на ЗНКІ натисніть кнопку «Ключі на носії». Після цього, оберіть ЗНКІ, введіть пароль до нього та натисніть кнопку «ОК».



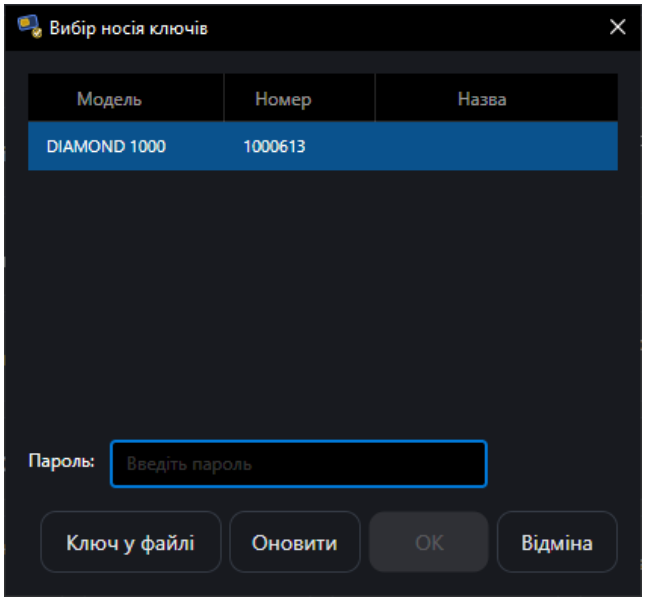
Для знищення ключів у наступному діалоговому вікні потрібно обрати ключ, який необхідно знищити і натиснути кнопку «Знищити», після чого підтвердити вибір натиснувши кнопку «Так» або кнопку «Ні» для скасування операції.



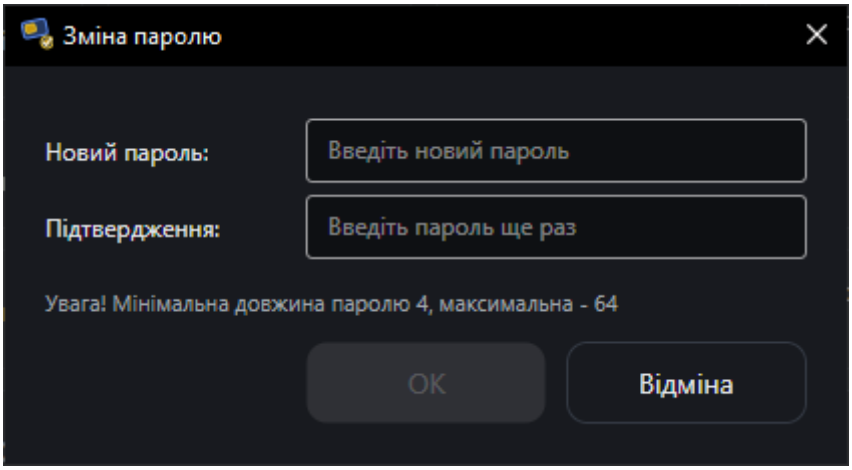


Зміна паролю доступу до носія ключів

Для зміни паролю доступу до ЗНКІ натисніть кнопку «Змінити пароль носія ключів». Після цього, оберіть ЗНКІ, введіть пароль до нього та натисніть кнопку «ОК».

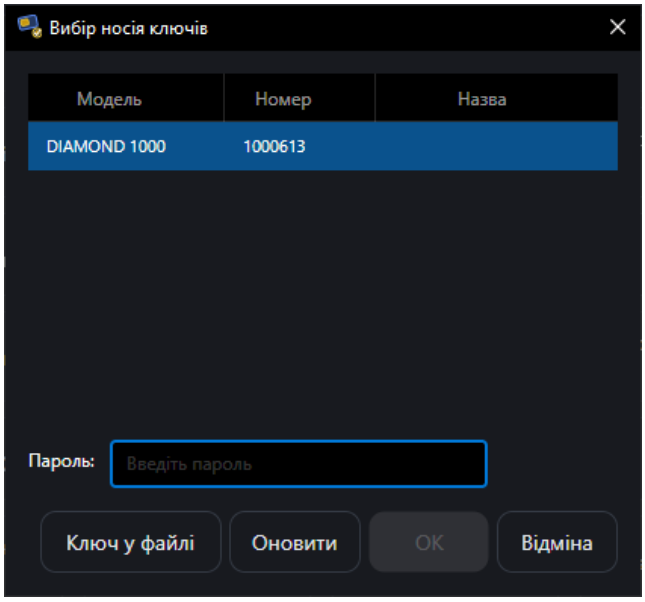


У наступному діалоговому вікні потрібно ввести новий пароль та його підтвердження і натиснути кнопку «ОК».



Створення запитів на сертифікат

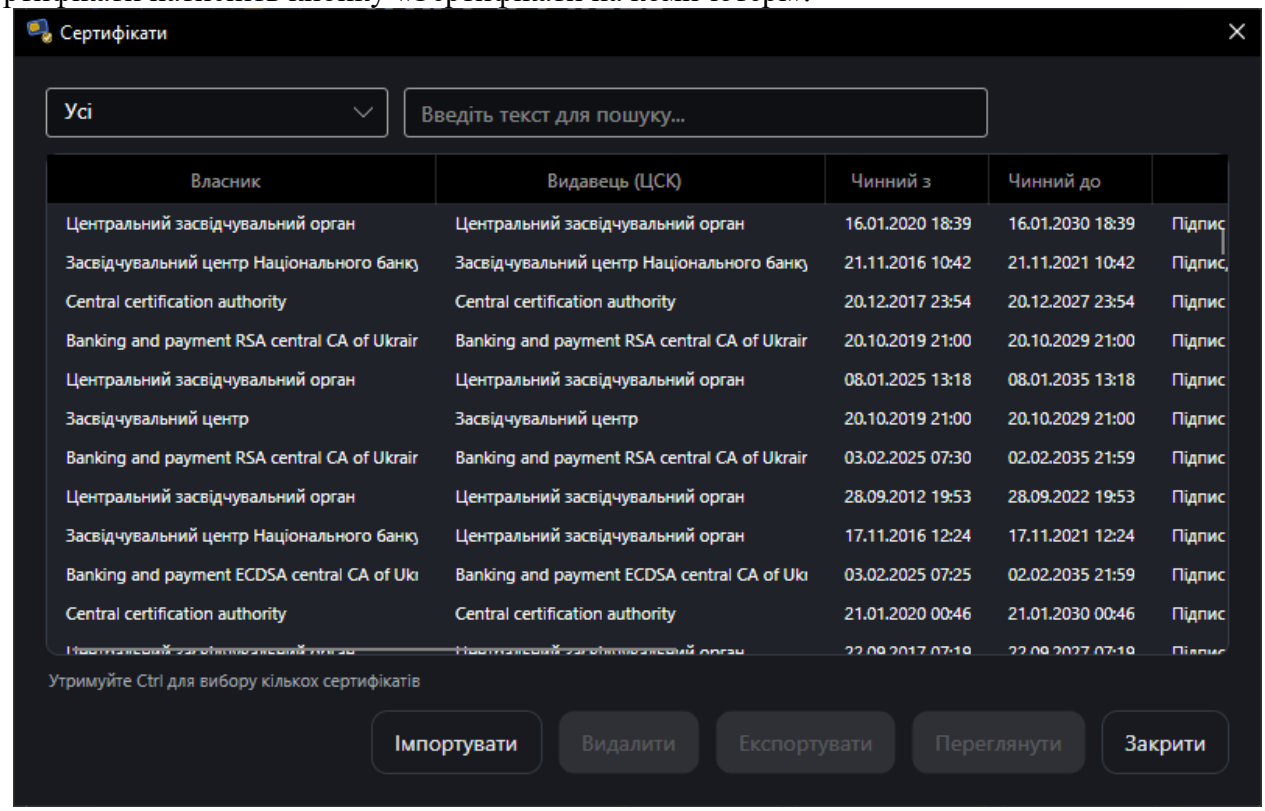
Для створення запиту на формування сертифікату натисніть кнопку «Створити запит на сертифікат». Процедура можлива лише при відсутності сертифіката відповідного ключа. Після цього, оберіть ЗНКІ, введіть пароль до нього та натисніть кнопку «ОК».



Для одного або двох ключів будуть сформовані запити на сертифікат та відкрито діалог збереження запитів на сертифікат аналогічний такому при генерації ключів.

Операції з сертифікатами на комп’ютері

Для відображення списку сертифікатів, що знаходяться у локальному сховищі, на комп’ютері, їх імпорту, експорту, видалення та перегляду детальної інформації про сертифікати натисніть кнопку «Сертифікати на комп’ютері».



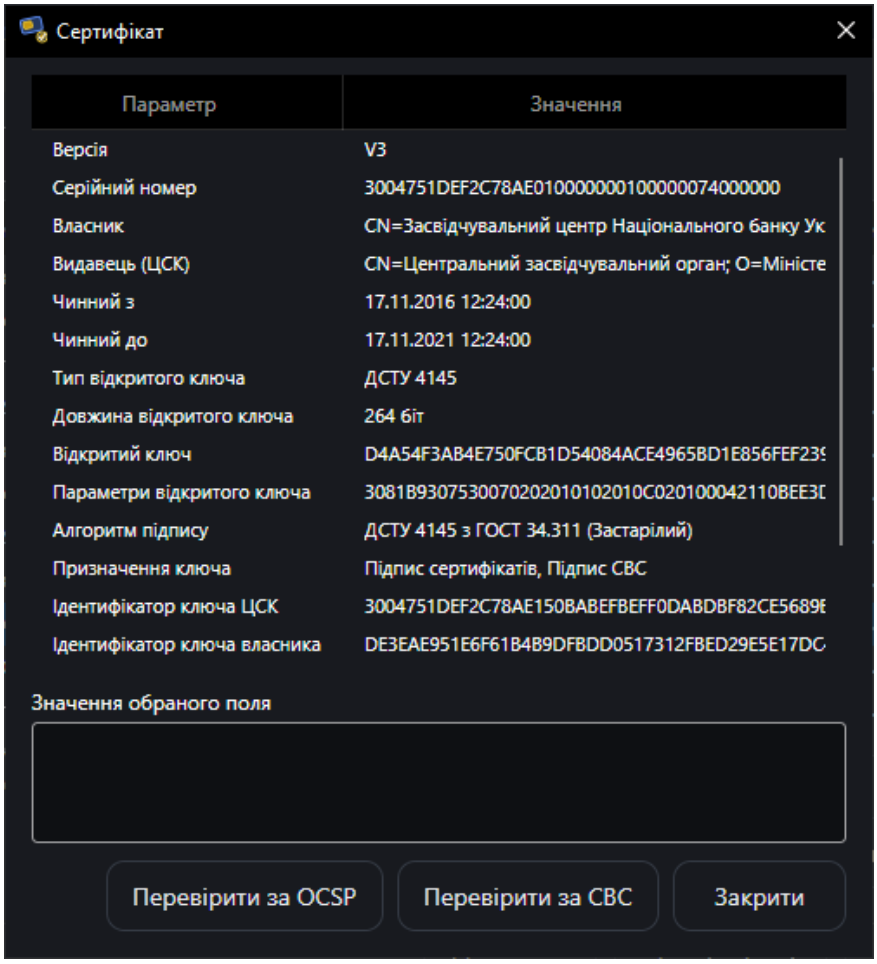
Для імпорту сертифікатів у локальне сховище, натисніть кнопку «Імпортувати», оберіть необхідні сертифікати у стандартному діалоговому вікні і натисніть кнопку «Відкрити».

Для видалення сертифікатів з локального сховища, оберіть необхідні сертифікати та натисніть кнопку «Видалити».

Для експорту сертифікатів з локального сховища, оберіть необхідний сертифікат та натисніть кнопку «Експортувати». У наступному діалоговому вікні задайте ім’я файлу та натисніть кнопку «Зберегти».

Для перегляду детальної інформації про сертифікат, оберіть необхідний сертифікат і натисніть кнопку «Переглянути».

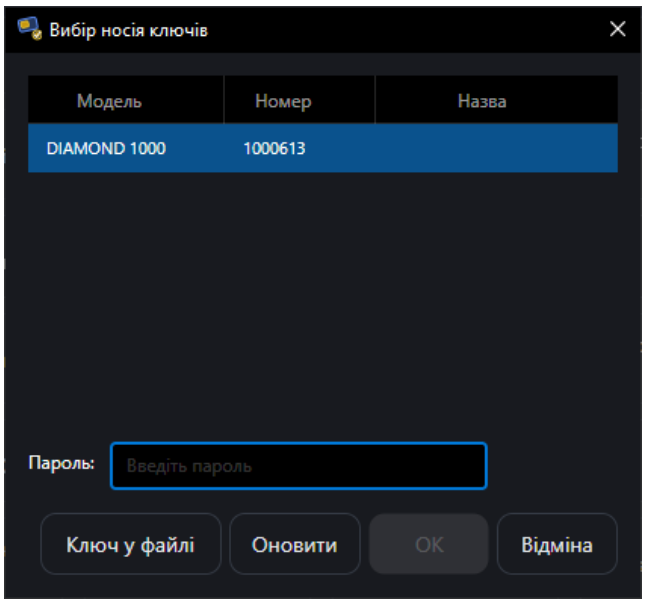
При перегляді інформації про сертифікат є можливість перевірити його статус за протоколами OCSP та CBC за допомогою відповідних кнопок «перевірити за OCSP» та «Перевірити за CBC».



Операції з сертифікатами на носії ключів

Для відображення списку сертифікатів, що знаходяться на ЗНКІ, їх імпорту, експорту, видалення та перегляду детальної інформації про сертифікат натисніть кнопку «Сертифікати на носії ключів».

Після входу у розділ, оберіть ЗНКІ, введіть пароль до нього та натисніть кнопку «ОК»



Для імпорту сертифікатів на ЗНКІ, натисніть кнопку «Імпортувати», оберіть необхідні сертифікати у стандартному діалоговому вікні і натисніть кнопку «Відкрити»

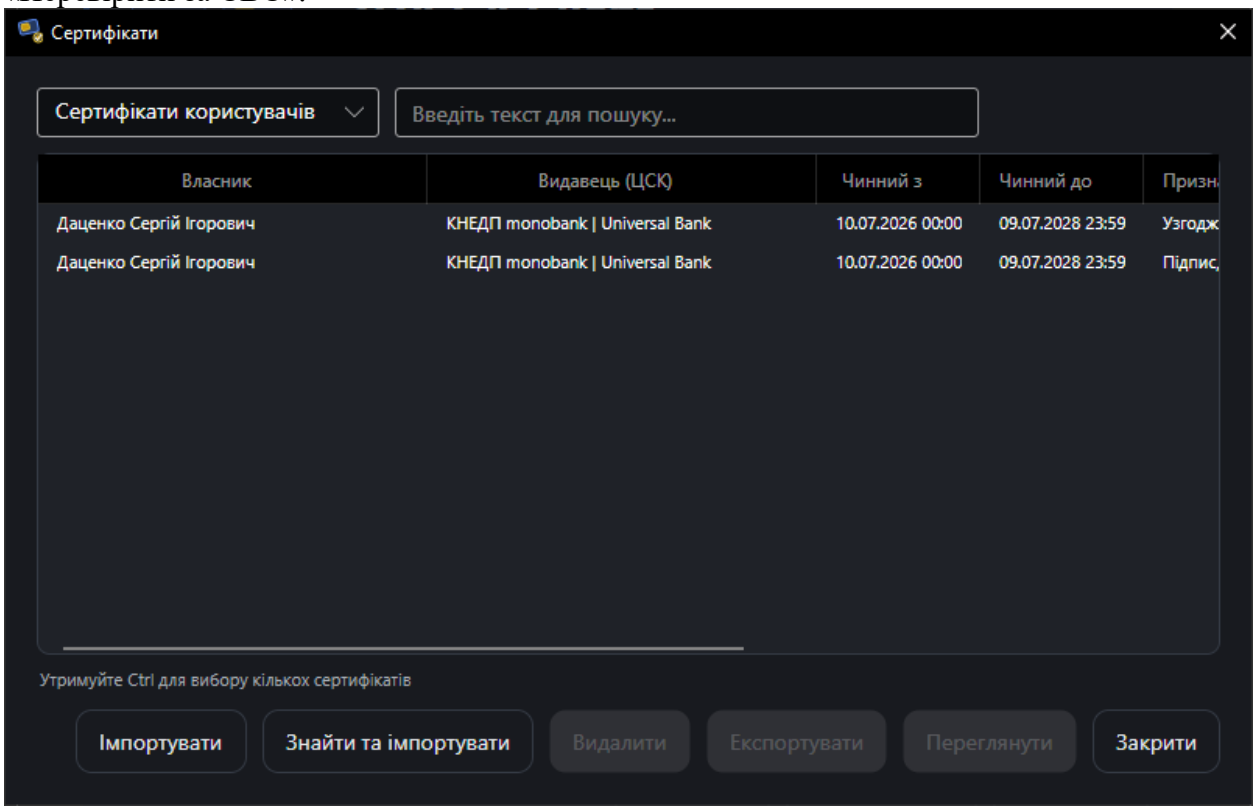
Для автоматичного пошуку сертифікатів, відповідних ключам на носії, натисніть кнопку «Знайти та імпортувати».

Для видалення сертифікатів з ЗНКІ, оберіть необхідні сертифікати та натисніть кнопку «Видалити».

Для експорту сертифікатів з ЗНКІ, оберіть необхідний сертифікат та натисніть кнопку «Експортувати». У наступному діалоговому вікні задайте ім’я файлу та натисніть кнопку «Зберегти».

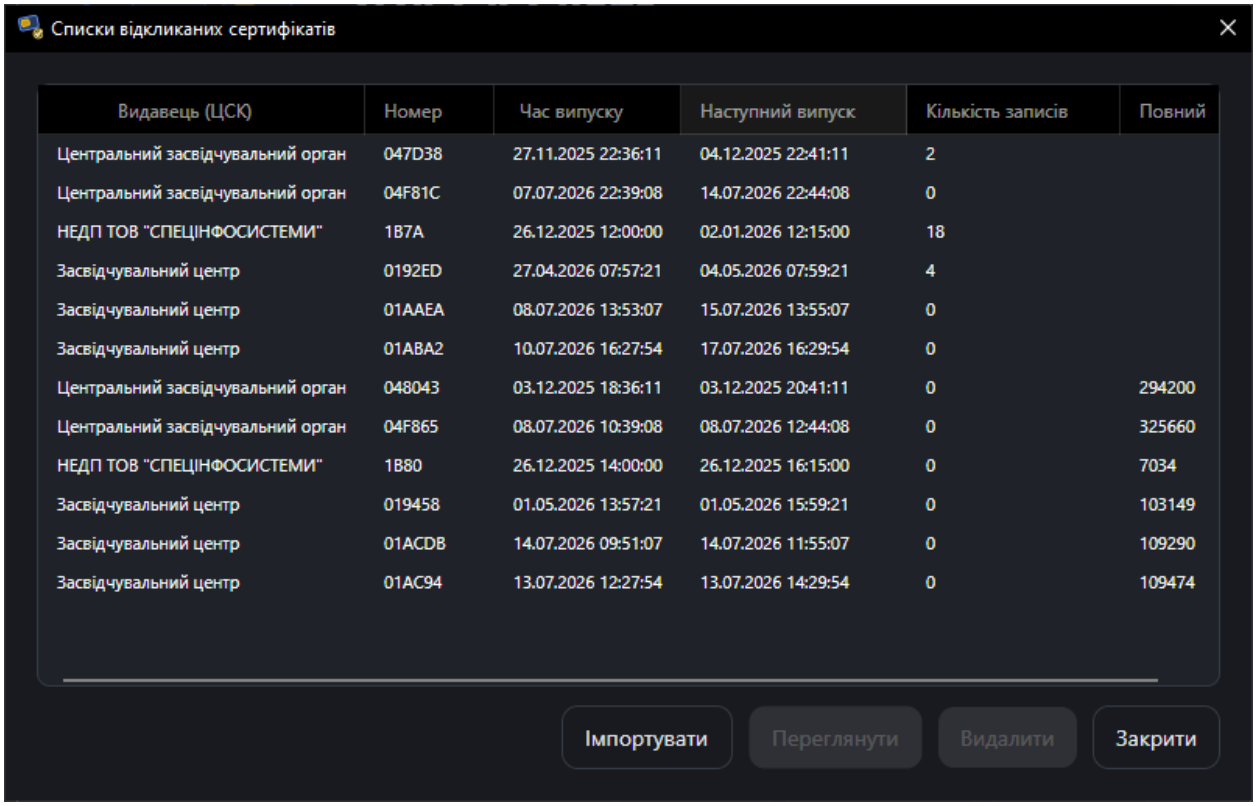
Для перегляду детальної інформації про сертифікат, оберіть необхідний сертифікат і натисніть кнопку «Переглянути».

При перегляді інформації про сертифікат є можливість перевірити його статус за протоколами OCSP та CBC за допомогою відповідних кнопок «перевірити за OCSP» та «Перевірити за CBC».



Операції з СВС

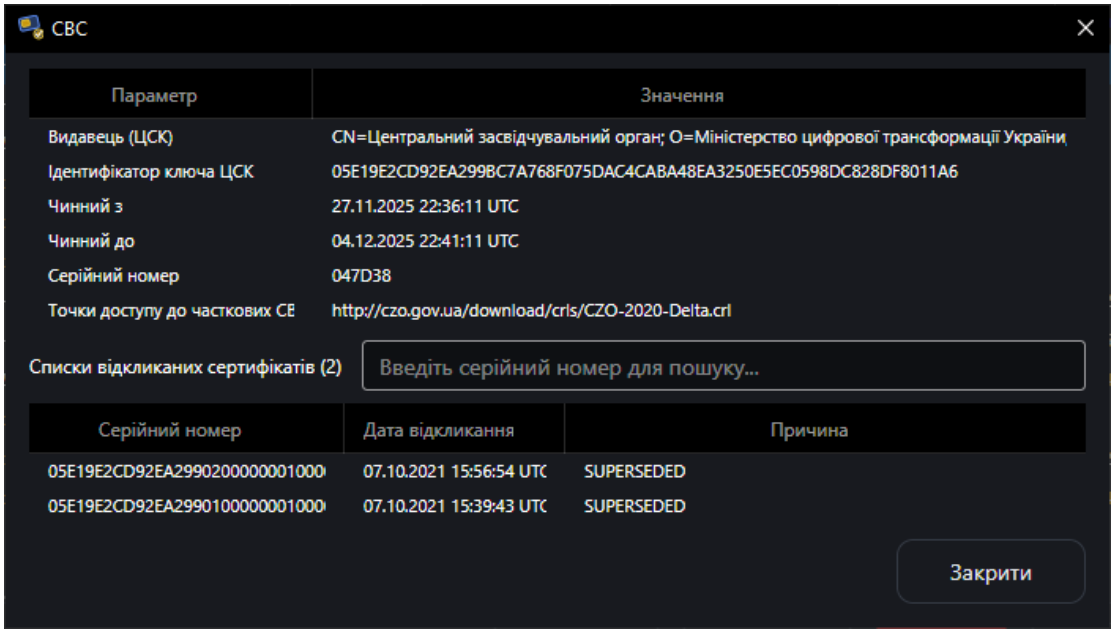
Для відображення списку, імпорту та видалення списків відкликаних сертифікатів списків відкликаних сертифікатів натисніть кнопку «СВС». Зазвичай всі операції з СВС виконується програмою в автоматичному режимі і не потребують втручання користувача.



Для імпорту СВС у локальне сховище, натисніть кнопку «Імпортувати», оберіть необхідні файли у стандартному діалоговому вікні і натисніть кнопку «Відкрити».

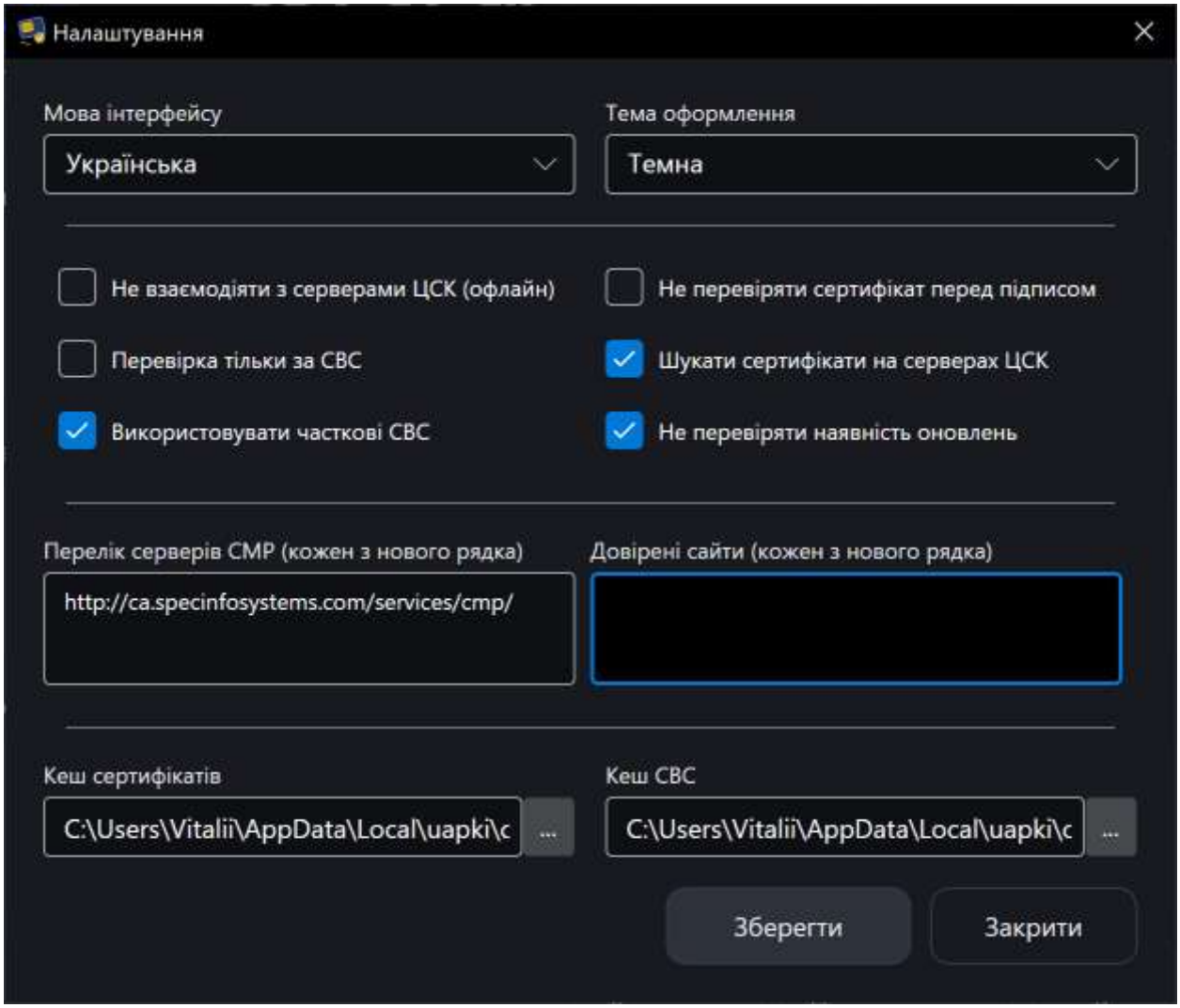
Для перегляду детальної інформації про СВС, оберіть необхідний сертифікат і натисніть кнопку «Переглянути».

Для видалення СВС з локального сховища, оберіть необхідні файли та натисніть кнопку «Видалити».



Налаштування

Для переходу в налаштування ПЗ натисніть кнопку «Налаштування».



Встановлення прапорця на параметрі «Взаємодіяти з НЕДП» керує дозволяє взаємодіяти з серверами НЕДП для завантаження сертифікатів та СВС, перевірки статусів сертифікатів та отримання позначки часу.

Встановлення прапорця на параметрі «Перевіряти тільки за СВС» дозволяє налаштувати ПЗ на перевірку статусу сертифікату лише за СВС, без доступу до серверу OCSP.

Встановлення прапорця на параметрі «Використовувати часткові СВС» дозволяє налаштувати ПЗ на перевірку статусу сертифікату за частковими СВС.

Встановлення прапорця на параметрі «Не перевіряти сертифікат перед підписом» дозволяє налаштувати ПЗ на підпис файлів без додаткової перевірки статусу сертифікату безпосередньо під час підписання файлу.

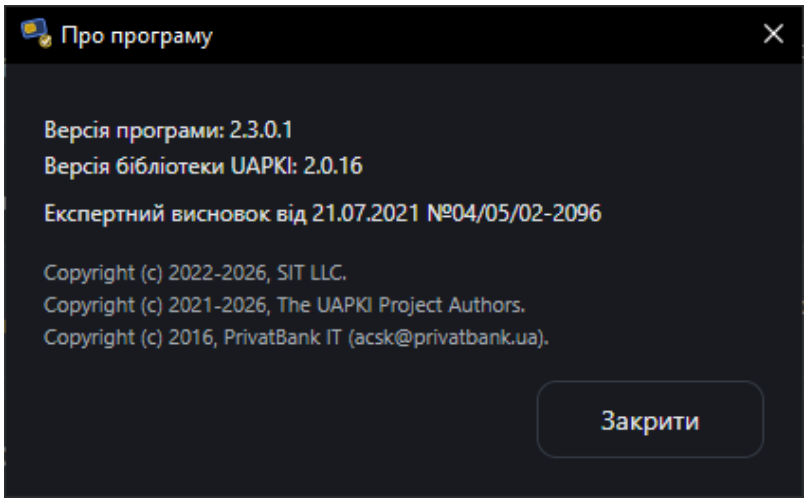
Встановлення прапорця на параметрі «Не перевіряти наявність оновлень» дозволяє налаштувати ПЗ на роботу без перевіряння наявності оновлень під час запуску ПЗ.

Допомога

Призначено для відображення інформації про ПЗ.

Про програму

Відображає інформації про версії ПЗ, бібліотек, а також інформації про авторські права на ПЗ.



Вихід

Вихід з ПЗ.