Товариство з обмеженою відповідальністю «С.І.Т»

Засіб криптографічного захисту інформації

3DA CA CLIENT

Настанова користувача

версія 2.0.16

Київ 2024

Терміни та скорочення

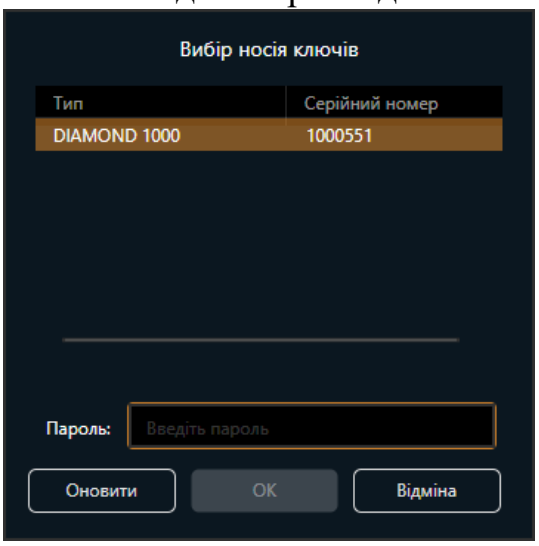
Ключ – особистий ключ;
Сертифікат – сертифікат відкритого ключа;
ЗНКІ – захищений носій ключової інформації
ПЗ – програмний засіб
СВС – список відкликаних сертифікатів
КНЕДП – кваліфікований надавач електронних довірчих послуг
КЕДП – кваліфіковані електронні довірчі послуги
API – Application Programming 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

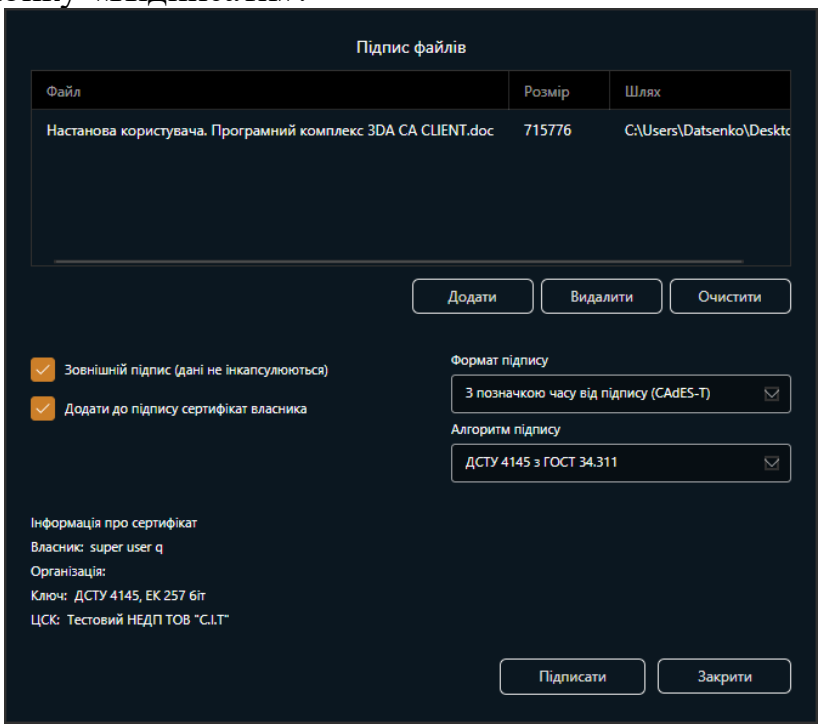
Для накладання електронного підпису на електронні документи у вигляді файлів натисніть кнопку «Підписати файли» у головному вікні програми. Після цього оберіть ЗНКІ та введіть пароль до нього.



Якщо на ЗНКІ знаходиться декілька ключів підпису, потрібно обрати необхідний та у наступному діалоговому вікні, за допомогою кнопки «Додати» або методом перетягуванням (drag-and-drop) додати файли, а також обрати параметри підпису, а саме:

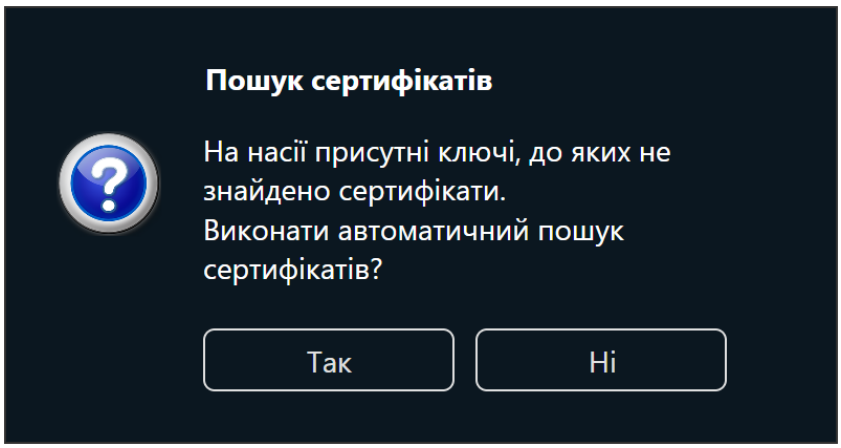
1. Формат підпису
2. Алгоритм підпису
3. Інші параметри

Після завантаження файлів та вибору всіх необхідних параметрів потрібно натиснути кнопку «Підписати».

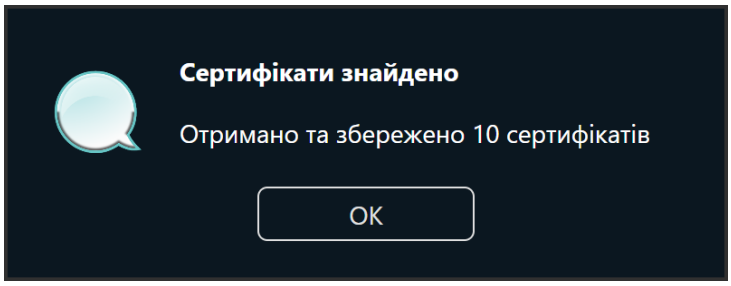


У разі успіху, буде сформовано підписані у файли з додатковим розширенням «.p7s» та збережені у тому ж каталозі, де знаходились файли для підпису.

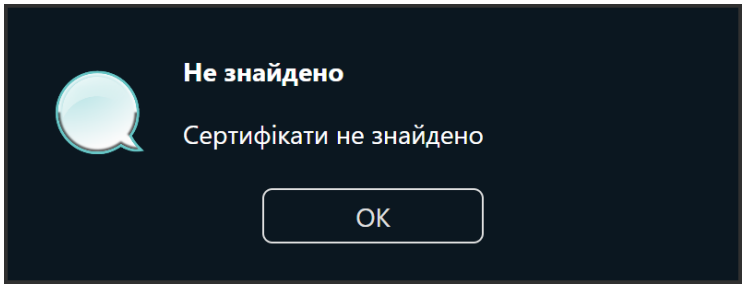
У разі відсутності сертифікатів до ключів на носії, користувачу буде запропоновано здійснити пошук таких сертифікатів на серверах КНЕДП.



У разі відповіді користувача «Так», буде здійснено пошук сертифікатів та повідомлено про результат пошуку і збереження сертифікатів:

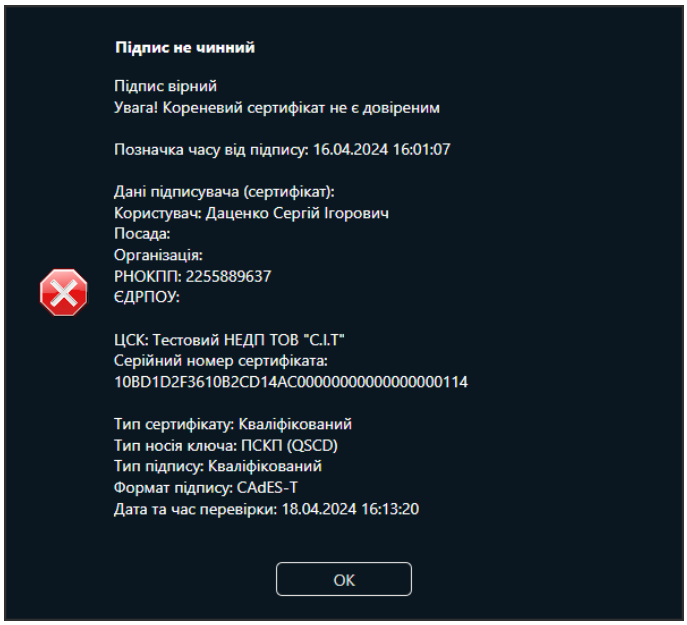


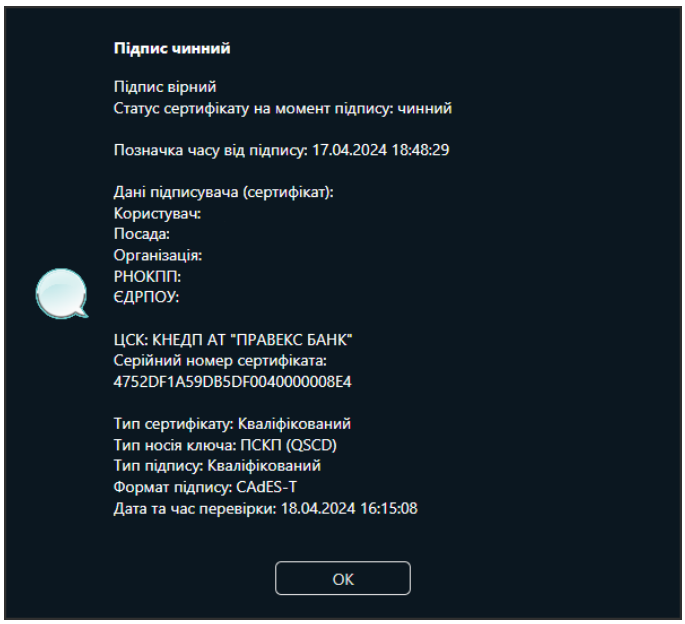
або



Перевірка підпису

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

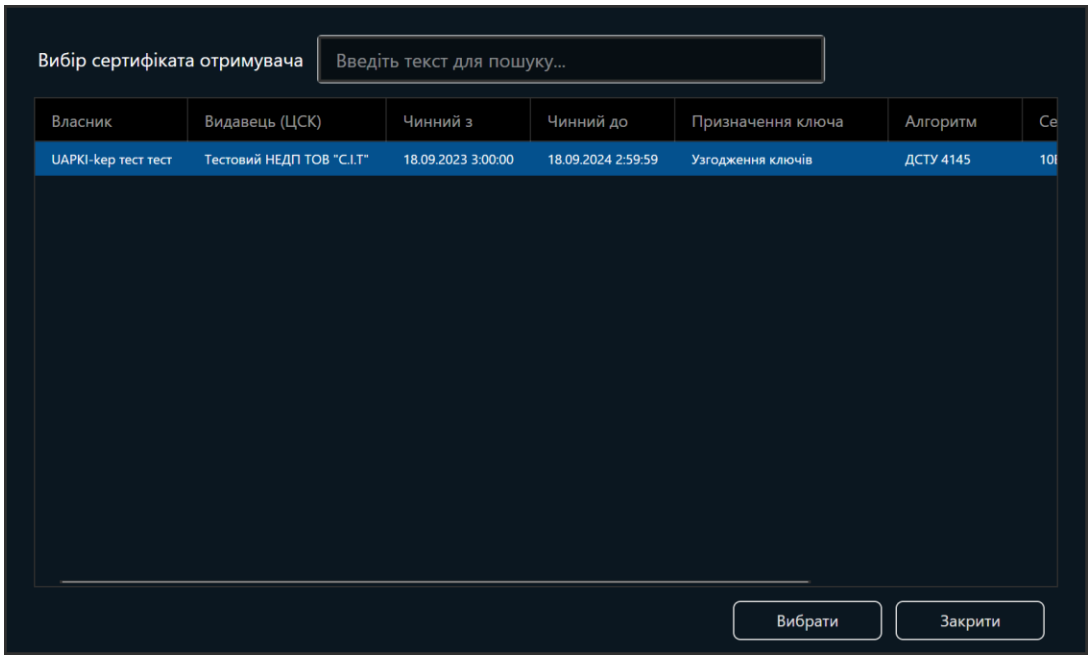




У разі використання підпису з інкапсульованими даними, в каталозі, в якому знаходиться відповідний файл підпису, буде створено файл, що містить інкапсульовані дані без розширення «.p7s».

Зашифрування файлів

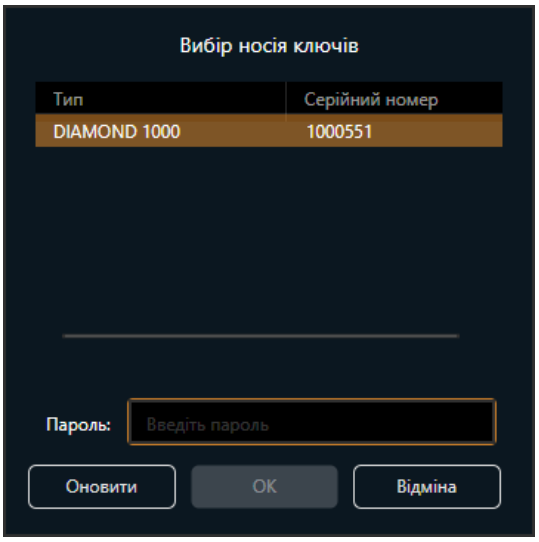
Для зашифрування файлів натисніть кнопку «Зашифрувати файли» та у стандартному діалоговому вікні вибору файлів, оберіть файли, які необхідно зашифрувати. Після цього, у відповідному вікні оберіть сертифікат отримувача.



У разі успішного виконання операції зашифрований файл буде збережено у тому ж каталозі, що і вхідний файл, з додатковим розширенням «.p7e».

Розшифрування файлу

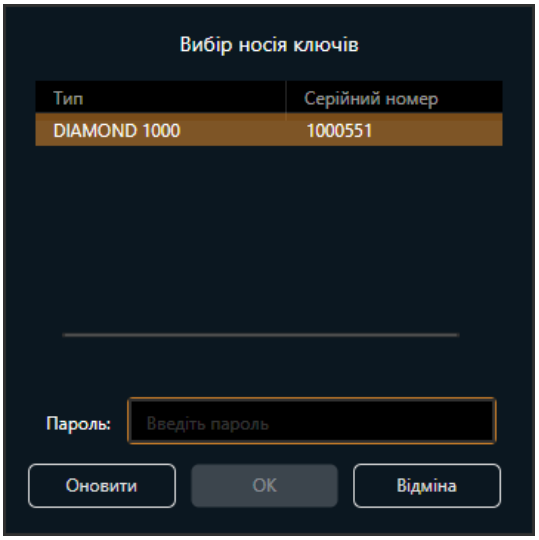
Для розшифрування файлу натисніть кнопку «Розшифрувати файл» та у стандартному діалоговому вікні вибору файлу, оберіть файл з розширенням «.p7e», який необхідно розшифрувати. Після цього оберіть ЗНКІ, на якому зберігається ключ розшифрування та введіть пароль до нього.



Якщо операцію виконано успішно, то розшифрований файл буде збережено у тому ж каталозі, що і вхідний файл. Якщо зашифрований файл містив розширення «.p7e», то після розшифрування воно буде прибрано, в іншому випадку – розшифрований файл буде містити розширення «.decrypted».

Генерація ключів

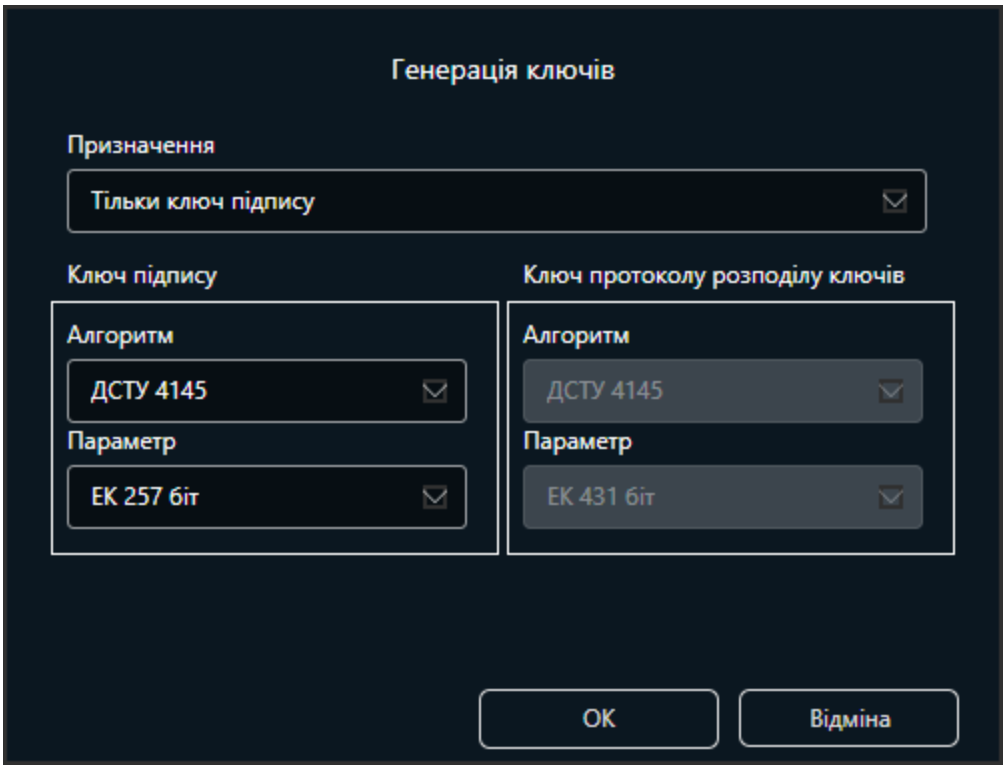
Для генерації нових ключів натисніть кнопку «Згенерувати ключі». Після цього необхідно обрати ЗНКІ та ввести пароль до нього.



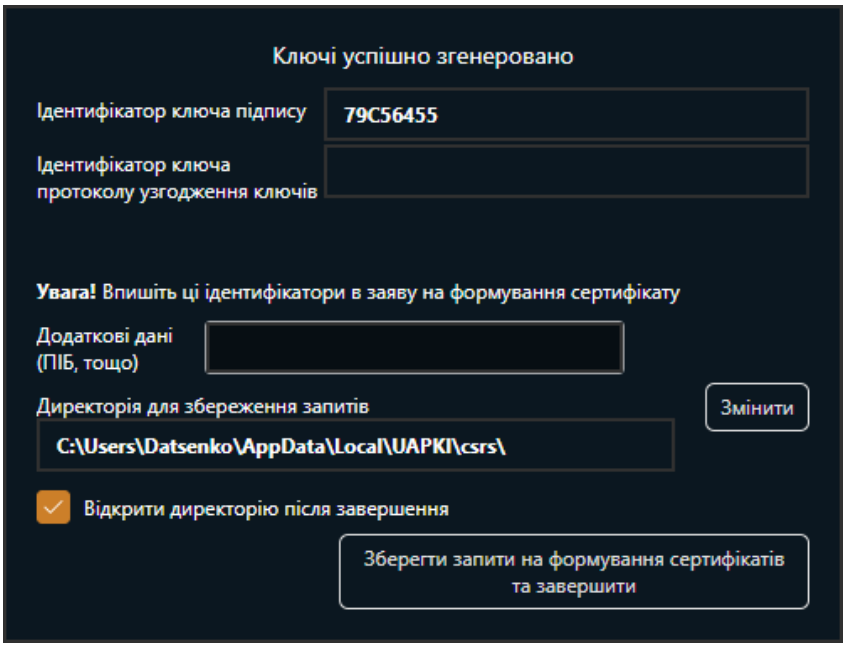
У наступному діалоговому вікні необхідно обрати призначення ключа:

- Тільки ключ підпису;
- Тільки ключ протоколу розподілу ключів;
- Ключ підпису та ключ протоколу розподілу ключів.

Додатково потрібно обрати алгоритм та параметр необхідних ключів і натиснути кнопку «ОК».

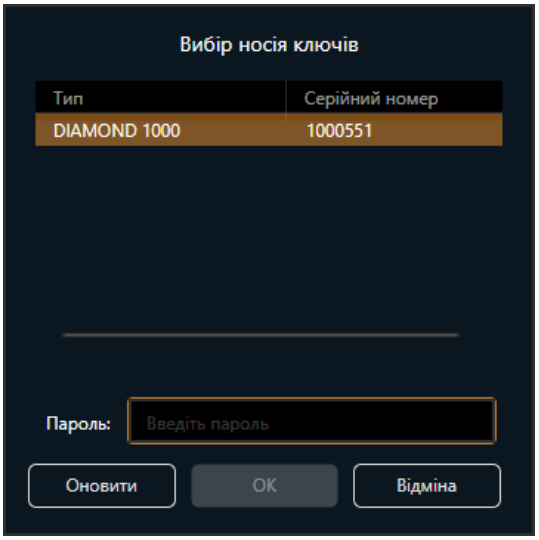


У наступному діалоговому вікні відображається інформація про згенеровані ключі, а також є можливість ввести додаткове ім’я запиту на формування сертифікату та вибору директорії для збереження запитів. Після натискання кнопки «Зберегти запити на формування сертифікатів та завершити» буде відкрито каталог з сформованими запитами.

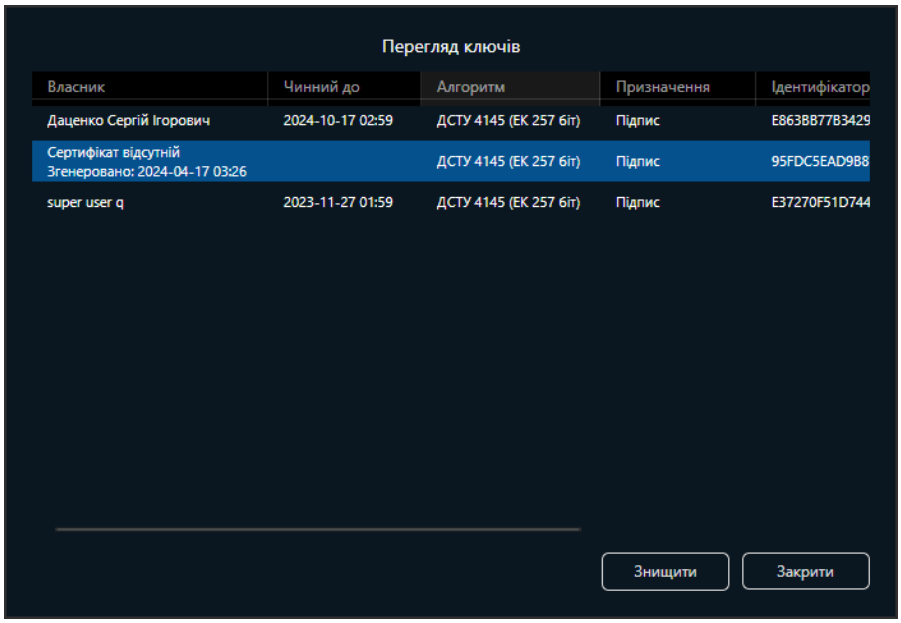


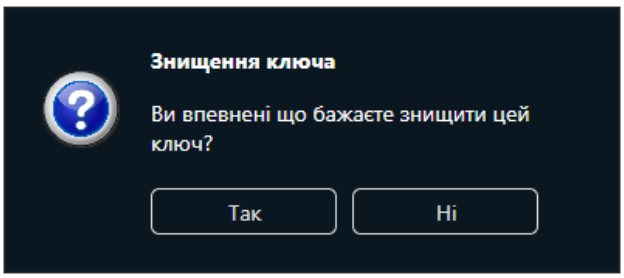
Перегляд ключів на ЗНКІ

Для перегляду ключів на ЗНКІ або їх видалення натисніть кнопку «Переглянути ключі». Після цього, необхідно обрати ЗНКІ та ввести пароль до нього.



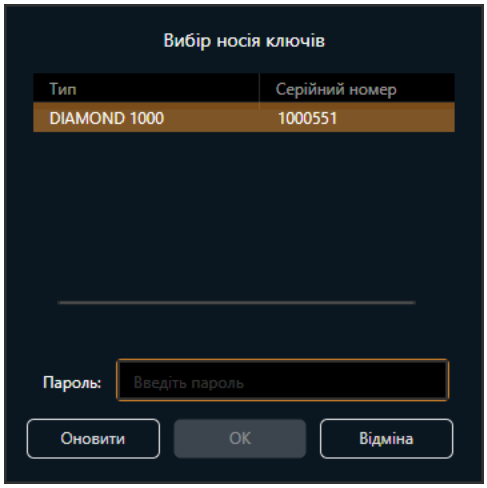
У наступному діалоговому вікні будуть відображені всі ключі, наявні на ЗНКІ та інформація про них.
Для видалення ключа з ЗНКІ необхідно обрати ключ, натиснути кнопку «Знищити» та підтвердити операцію.



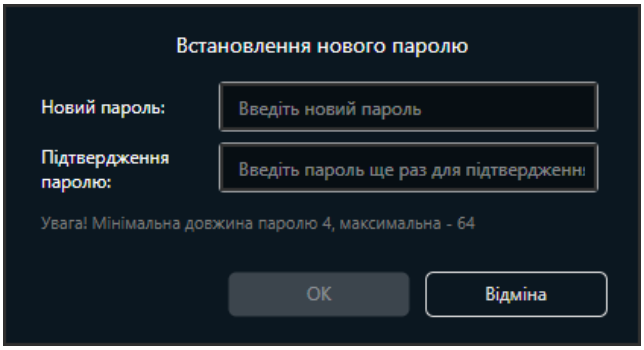


Зміна пароля ЗНКІ

Для зміни паролю доступу до ЗНКІ натисніть кнопку «Змінити пароль носія ключів». Після цього, необхідно обрати ЗНКІ та ввести пароль до нього.

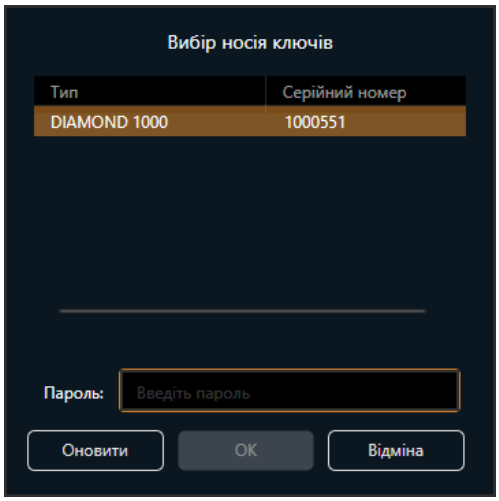


У наступному діалоговому вікні потрібно ввести новий пароль та його підтвердження і натиснути кнопку «ОК» для збереження.



Створення запитів на формування сертифіката

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

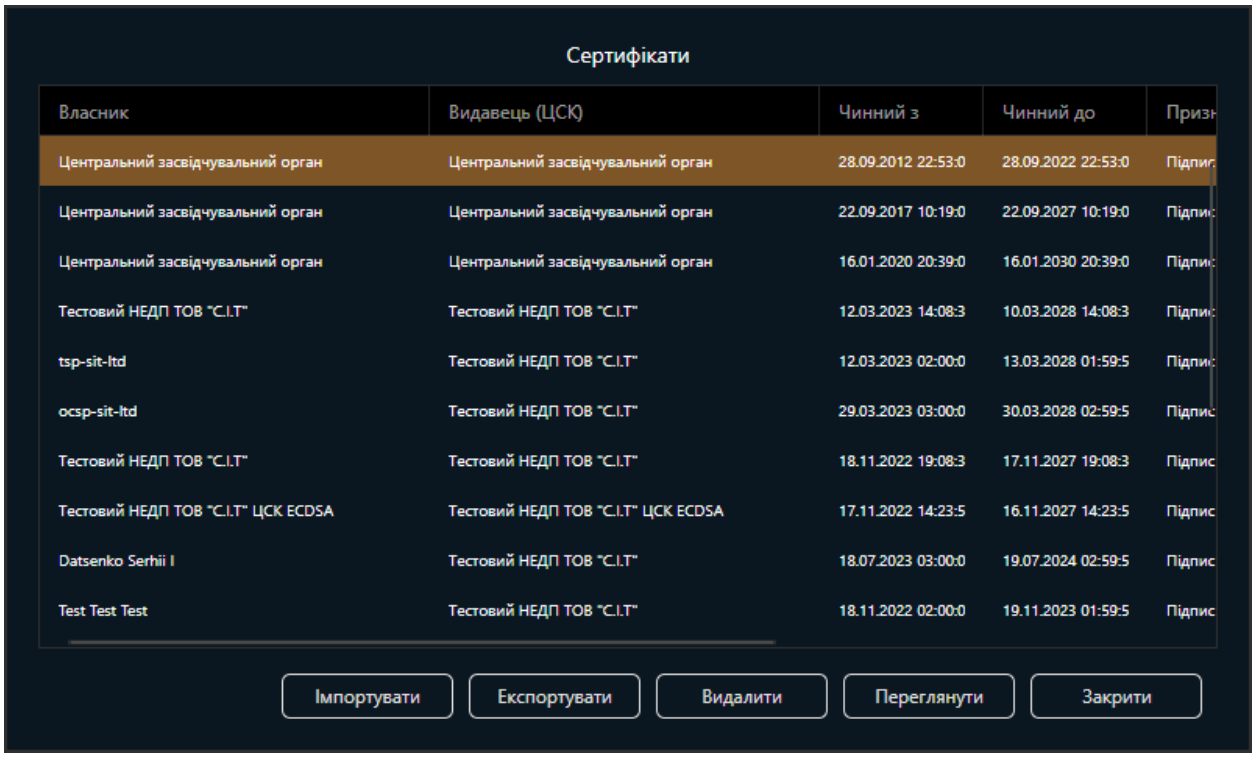


Для обраного ключа буде сформовано запит на формування сертифіката та відкрито діалог збереження запитів на сертифікат аналогічний до діалогового вікна при виконанні генерації ключів.

Операції з сертифікатами на комп’ютері

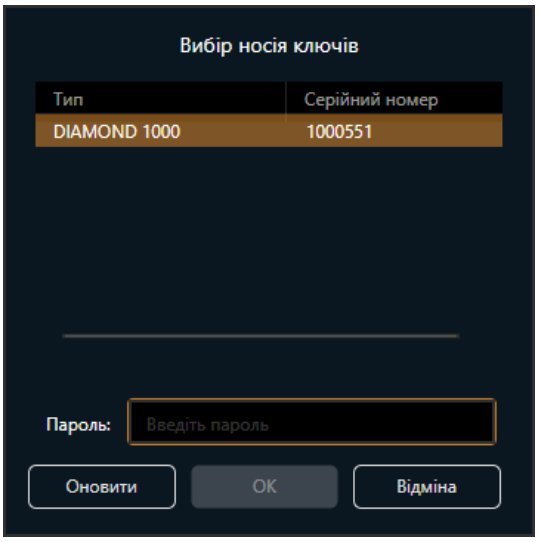
Для відображення списку сертифікатів, що знаходяться у локальному сховищі, на комп’ютері, їх імпорту, експорту, видалення та перегляду детальної інформації про сертифікат натисніть кнопку «Сертифікати на комп’ютері».

Для імпорту сертифікатів в локальне сховище, натисніть кнопку «Імпортувати» та у стандартному діалоговому вікні оберіть необхідні сертифікати і натисніть кнопку «Відкрити».
Для експорту сертифіката з локального сховища, оберіть необхідний сертифікат і натисніть кнопку «Експортувати». Після цього у стандартному діалоговому вікні оберіть теку для експорту, задайте ім’я файлу та у стандартному діалоговому вікні оберіть необхідні сертифікати і натисніть кнопку «Зберегти».
Для видалення сертифіката з локального сховища, оберіть необхідний сертифікат і натисніть кнопку «Видалити».
Для перегляду детальної інформації про сертифікат, оберіть необхідний сертифікат та натисніть кнопку «Переглянути».



Операції з сертифікатами на ЗНКІ

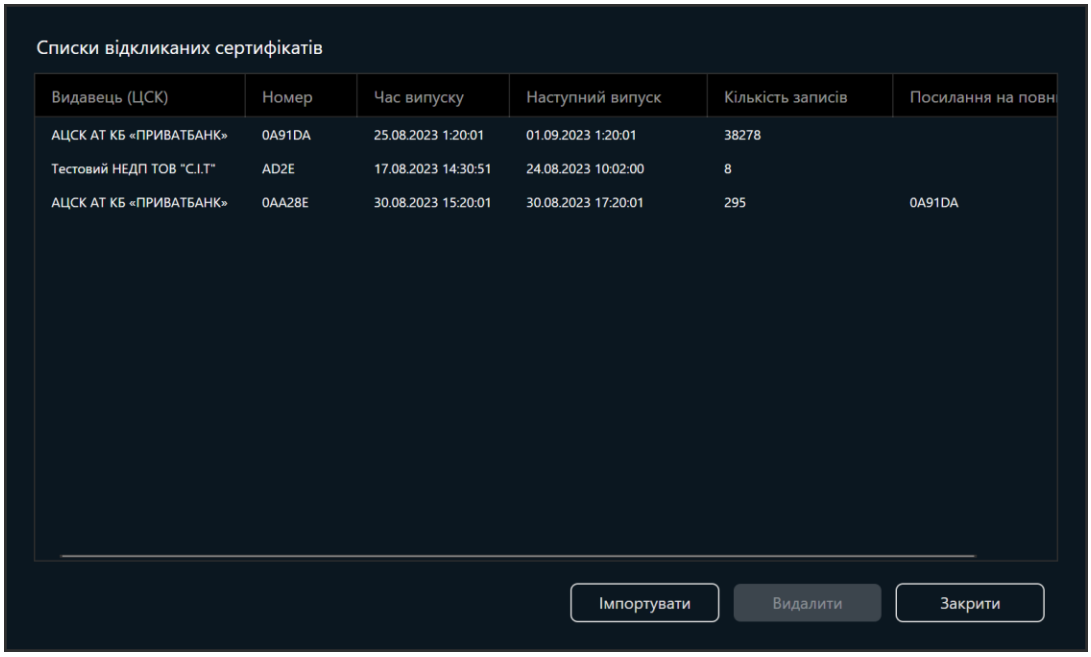
Для відображення списку сертифікатів, що знаходяться на ЗНКІ, їх імпорту, експорту, видалення та перегляду детальної інформації про сертифікат натисніть кнопку «Сертифікати на носії ключів». Після цього, необхідно обрати ЗНКІ та ввести пароль до нього.



Для імпорту сертифікатів до ЗНКІ, натисніть кнопку «Імпортувати» та у стандартному діалоговому вікні оберіть необхідні сертифікати і натисніть кнопку «Відкрити».
Для експорту сертифіката з ЗНКІ, оберіть необхідний сертифікат і натисніть кнопку «Експортувати». Після цього у стандартному діалоговому вікні оберіть теку для експорту, задайте ім’я файлу та у стандартному діалоговому вікні оберіть необхідні сертифікати і натисніть кнопку «Зберегти».
Для видалення сертифіката з ЗНКІ, оберіть необхідний сертифікат і натисніть кнопку «Видалити».
Для перегляду детальної інформації про сертифікат, оберіть необхідний сертифікат та натисніть кнопку «Переглянути».

Операції з СВС

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

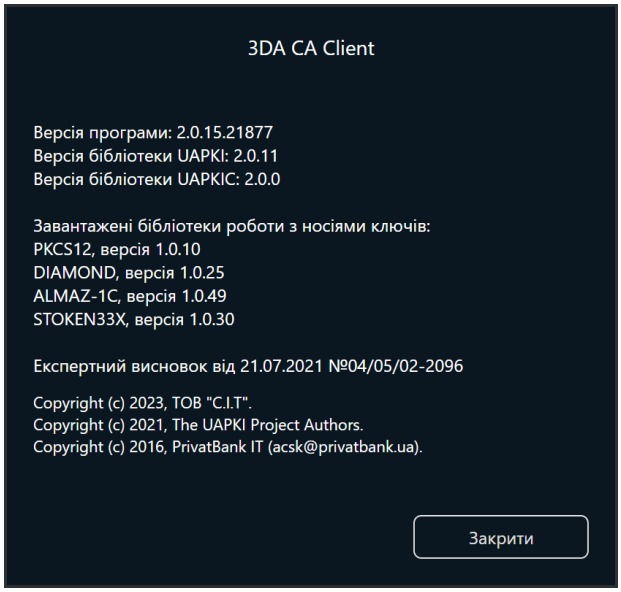


Допомога

Призначено для відображення інформації про ПЗ.

Про програму

Для відображення інформації про версії ПЗ, криптобібліотек, а також інформації про авторські права на ПЗ, натисніть кнопку «Про програму».



Вихід

Вихід з ПЗ.

Налаштування ПЗ

Налаштування ПЗ відбувається шляхом внесення змін у файл конфігурації «3daclient.json». Файл знаходиться в каталозі з інстальованим ПЗ.

Параметри налаштувань:

1. certCache – налаштування сховища сертифікатів і провайдерів НКІ;
   path – налаштування шляху до сховища сертифікатів;
   allowedProviders – налаштування переліку провайдерів НКІ, шляхом підключення їх бібліотек.
2. trustedCerts – налаштування переліку довірених кореневих сертифікатів, шляхом додавання до списку сертифіката у форматі base64.
3. crlCache – налаштування шляху до сховища списків відкликаних сертифікатів.
4. tsp – налаштування точки доступу для отримання позначки часу.
5. certSearch – налаштування пошуку сертифікатів на зовнішніх ресурсах;
   certSearchEnabled – включити/виключити пошук сертифікатів за ідентифікатором відкритого ключа;
   updateCaCertsUrl – точка доступу для завантаження актуального переліку сертифікатів КНЕДП України. У разі наявності цього параметру при старті програми здійснюється перевірка чи є оновлення в сертифікатах і, якщо є, вони автоматично оновлюються;
   byKeyId / servers – налаштування переліку серверів надавачів довірчих послуг на яких здійснюється пошук за протоколом CMP.