Приватне акціонерне товариство «Науково-дослідний інститут прикладних інформаційних технологій»

ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ ПрАТ „НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПРИКЛАДНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ”

Інструкція користувача послуг ЦСК

2015 р.

ЗМІСТ

1. Вступ
    1.1. Анотація
    1.2. Призначення програми
    1.3. Системні вимоги
    1.4. Інсталяція програми
2. Початок роботи з програмою
    2.1. Завантаження сертифікатів
        2.1.1. Завантаження сертифікатів підписувачів
        2.1.2. Завантаження сертифіката ЦСК
        2.1.3.Завантаження кореневого сертифіката ЦЗО
    2.2. Налагодження параметрів
        2.2.1. Загальні
        2.2.2. З’єднання
        2.2.3. Сховища
        2.2.4. Цілісність сертифіката ЦСК
3. Робота з програмою
    3.1. Підпис
        3.1.1. Підписання повідомлень
        3.1.2. Перевірка підписаного повідомлення
        3.1.3. Об'єднання підписів
        3.1.4. Додавання підпису
    3.2. Шифрування та розшифрування повідомлень
        3.2.1. Зашифрувати повідомлення
        3.2.2. Розшифрування повідомлення
    3.3. Зміна статусу сертифіката
    3.4. Запит на отримання сертифіката
    3.5. Перевірка цілісності
    3.6. Захищений носій
    3.7. Сховища сертифікатів
    3.8. Сховище списків відкликаних сертифікатів
    3.9. Пошук сертифікатів
4. Повторне отримання сертифіката
    4.1. Генерація ключів на картці
    4.2. Створення запиту на отримання сертифіката
    4.3. Завантаження сертифікатів до сховища

1. Вступ

1.1. Анотація

Цей посібник для користувачів програми Клієнт програмно технічного комплексу "НДІ ПІТ ЦСК" (далі – “Клієнт ЦСК”). У цьому документі наведені загальні відомості про встановлення, настроювання, функціонування та засоби обміну даними програми “Клієнт ЦСК”.

Користувачі програми повинні мати досвід роботи з операційною системою MS Windows, вміти працювати з клавіатурою та мишею, тому у керівництві не наведені пояснення, що таке форма (або вікно), меню, подвійний клік мишею тощо. Слід підкреслити, що базові знання та навички роботи з ОС MS Windows є необхідними для успішного використання програми

1.2. Призначення програми

Програма “Клієнт ЦСК” забезпечує наступні можливості:

- накладання, перевірка, об'єднання та додання електронних цифрових підписів (у тому числі разом з позначками часу. Накладання здійснюється з використанням особистого ключа користувача, що зберігається на смарт-карті. Можливе використання для накладення електронного цифрового підпису програмної криптографічної бібліотеки або вбудованих апаратних засобів захищеного носія ключів);
- можливість криптографічного захисту інформації (шифрування/розшифрування), що дозволяє передавати інформацію у відкритій мережі, завдяки направленому шифруванню;
- формування та перевірка запитів на зміну статусу власних сертифікатів відкритих ключів;
- формування та перевірка запитів на формування сертифікатів відкритих ключів;
- перевірка цілісності виконуваного файлу та бібліотек програми “Клієнт ЦСК”.
- можливість зміни та розблокування кодів доступу та кодів розблокування коду доступу до смарт-карток;
- перевірка чинності сертифікатів відкритих ключів;
- пошук на інформаційному ресурсі ЦСК, завантаження, імпорт та експорт сертифікатів відкритих ключів та списків відкликаних сертифікатів відкритих ключів у сховищах та у вигляді файлів;
- зміна налагоджень програми “Клієнт ЦСК” (зміна значень параметрів у файлі конфігурації);

1.3. Системні вимоги

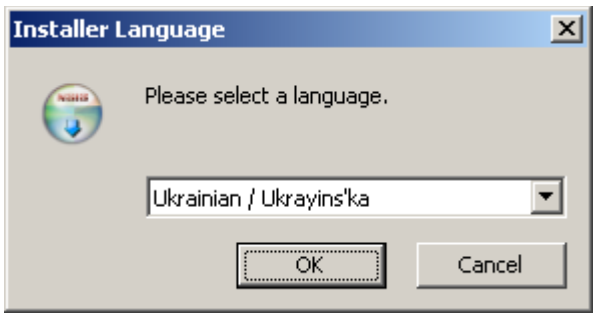
Програма “Клієнт ЦСК” працює під ОС Windows XP, Windows 7 та Windows 8. Для встановлення програми на диск необхідно до 35 МБайт вільного простору.

1.4. Інсталяція програми

Для того, щоб встановити програму “Клієнт ЦСК” на комп'ютер потрібно виконати інсталяцію програми.

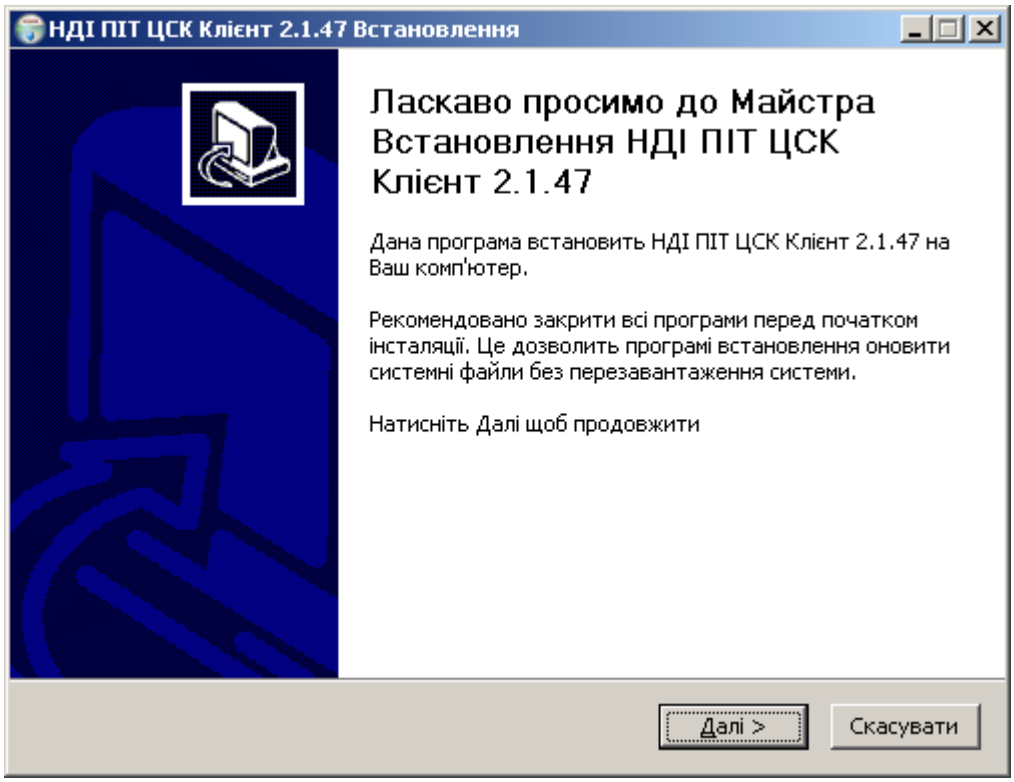
Для інсталяції програми потрібно виконати наступні дії:

1) запустіть програму установки, на екрані з'явиться вікно (мал. 1.1) встановлення із запрошенням обрати мову інтерфейсу. Для продовження інсталяції оберіть мову та натисніть “Ok”, для скасування встановлення натисніть “Cancel”.



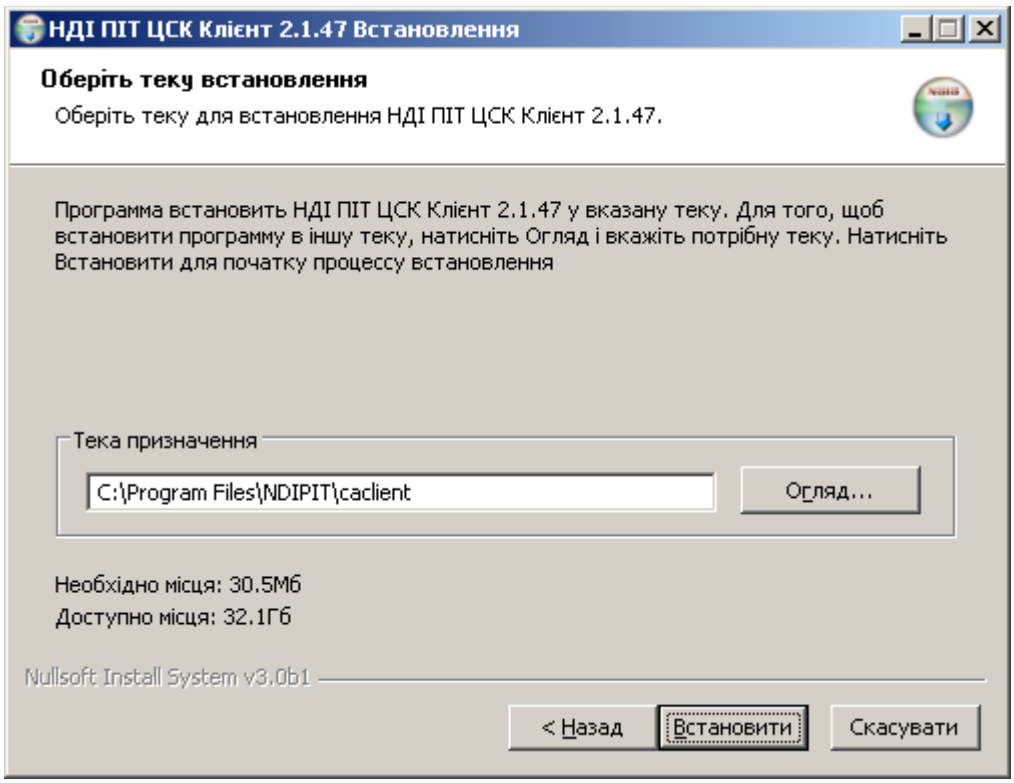
Мал. 1.1 Вікно вибору мови інсталятора.

2) На наступному кроці у вікні привітання (мал. 1.2), щоб розпочати встановлення програми, натисніть “Далі”, для відміни встановлення натисніть “Скасувати”.



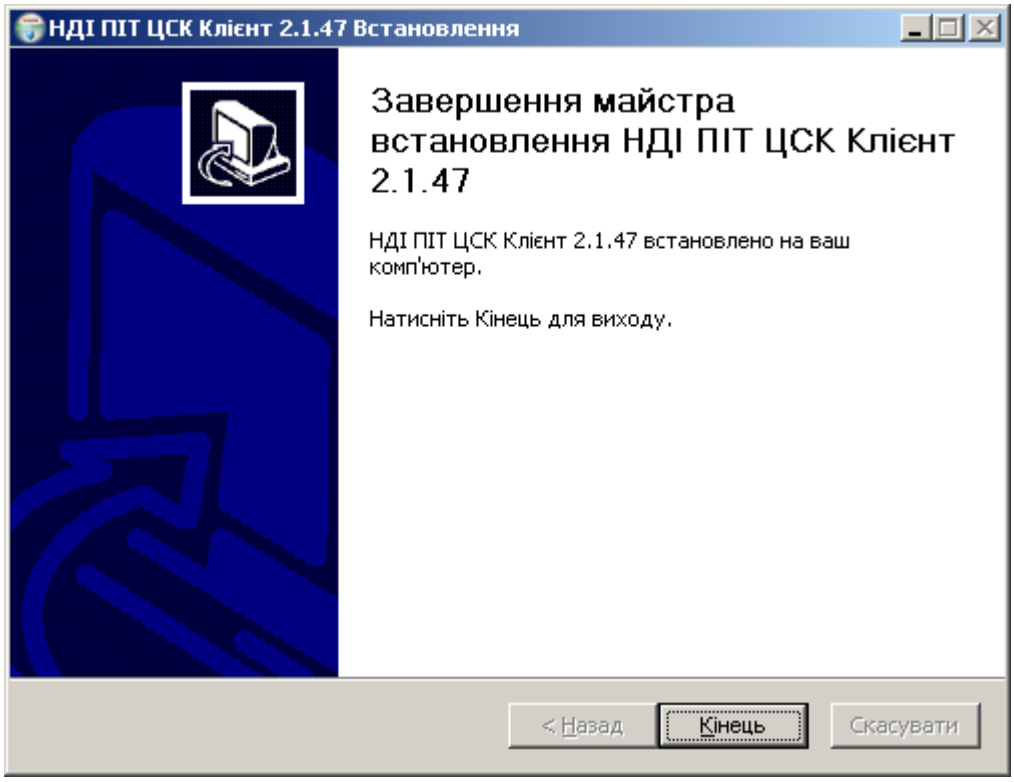
Мал. 1.2 Вікно привітання майстра встановлення.

3) На наступному кроці у вікні обрання теки призначення (мал. 1.3) є можливість змінити теку, у яку буде встановлено програму, в залежності від вільного місця на дисках. Для продовження натисніть кнопку “Встановити”.



Мал. 1.3 Обрання теки призначення.

4) Чекайте завершення роботи установки. Після вдалого завершення процесу встановлення Ви побачите відповідне вікно (мал. 1.4).



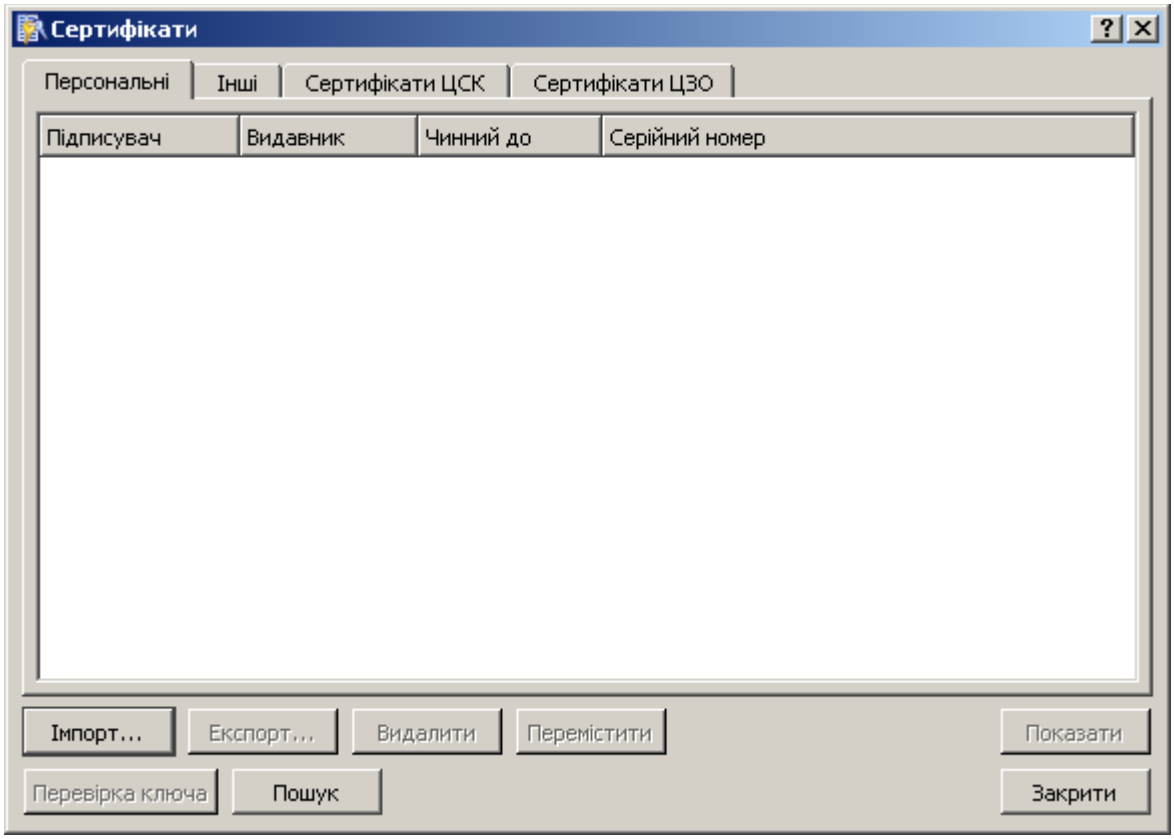
Мал. 1.4 Вікно завершення встановлення.

Після завершення встановлення на робочому столі з’явиться ярлик  , що дозволяє швидко викликати програму.

2. Початок роботи з програмою

2.1. Завантаження сертифікатів

Для роботи із сертифікатами в сховищі сертифікатів програми “Клієнт ЦСК”, необхідно в меню “Інструменти” вибрати пункт меню “Сертифікати” - відкриється вікно “Сертифікати” (мал. 2.1). Сховище сертифікатів розділено на чотири розділи: “Персональні”, “Інші”, “Сертифікати ЦСК”, “Сертифікати ЦЗО”. Відповідні кнопки вікна дозволяють сертифікати: імпортувати до сховища, експортувати та видаляти зі сховища, переміщати між розділами сховища, перевіряти ключа з носія, вставленого до карт-рідера, на відповідність ключу із вибраного сертифіката, шукати сертифікати на інформаційному ресурсі ЦСК. Кнопка “Показати” відкриває вікно з детальної інформації про вибраний сертифікат.



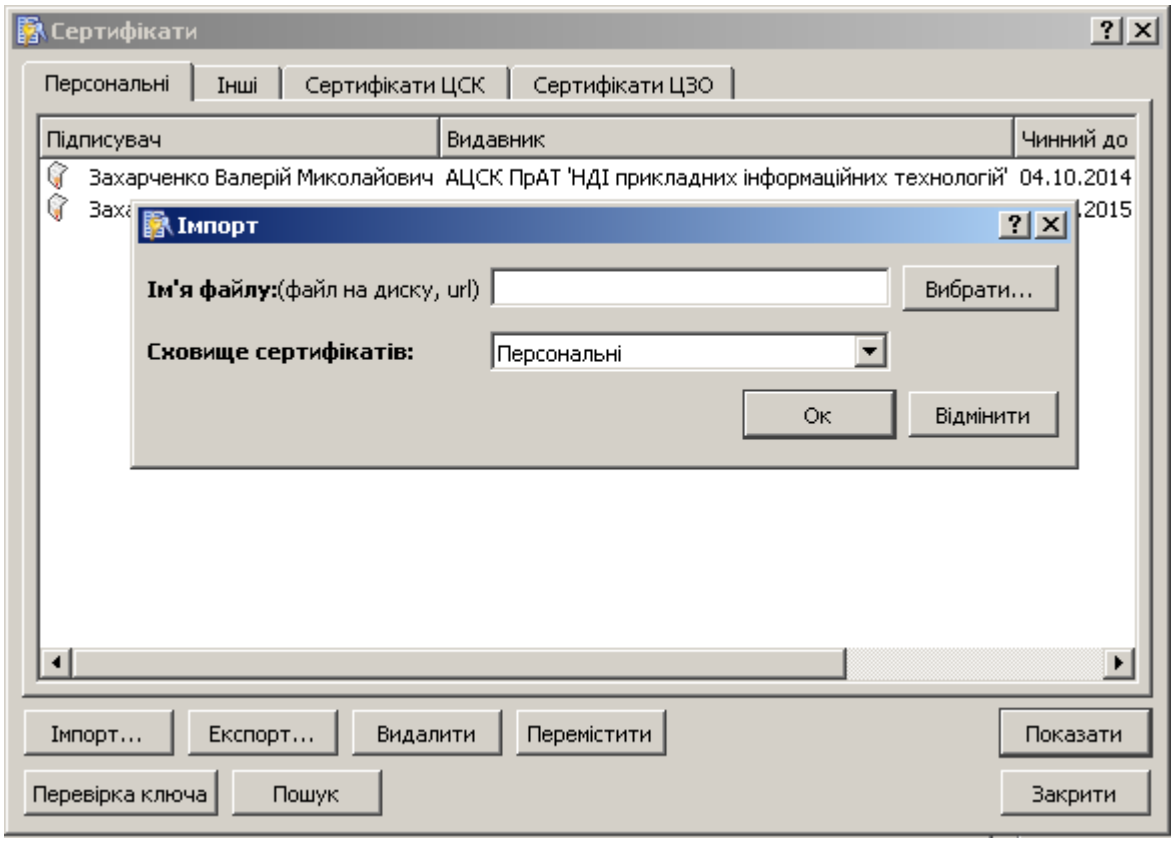
Мал. 2.1 Вікно “Сертифікати”.

Перед початком завантаження сертифікатів, для зручності, слід створити окрему теку, в якій будуть зберігатися завантажені із сайтів сертифікати ЦЗО, ЦСК та користувачів (далі – тека сертифікатів). Завантажити новий кореневий сертифікат ЦЗО до теки сертифікатів можна з офіційного сайту Центрального засвідчувального органу (http://www.czo.gov.ua), у розділі “СЕРТИФІКАТИ ЦЗО”. Завантажити новий сертифікат ЦСК до теки сертифікатів можна з офіційного сайту Центрального засвідчувального органу (http://www.czo.gov.ua) у розділі “ЕЛЕКТРОННИЙ РЕЄСТР СУБ'ЄКТІВ СФЕРИ ЕЦП”.

2.1.1. Завантаження сертифікатів підписувачів

Для завантаження сертифікатів підписувачів до сховища програми “Клієнт ЦСК” в меню “Інструменти” оберіть пункт меню “Сертифікати”, після чого з’явиться вікно “Сертифікати”. На вкладці “Персональні” зберігаються персональні сертифікати, на вкладці “Інші” – сертифікати інших підписувачів. Натиснути кнопку “Імпорт…”. У вікні “Імпорт” (мал. 2.2) в полі “Ім'я файлу:” вибрати сертифікат збережений до теки сертифікатів (або вказати url сертифіката у загальнодоступній мережі, якщо є доступ). Натисніть “ОК”.

Якщо є доступ до Інтернету (інформаційного ресурсу ЦСК) можна завантажити сертифікати до сховища за допомогою кнопки “Пошук” вікна “Сертифікати”. Пошук сертифікатів проводиться на інформаційному ресурсі ЦСК згідно дій описаних у розділі “Пошук сертифікатів” даної інструкції.



Мал. 2.2. Імпорт сертифіката.

2.1.2. Завантаження сертифіката ЦСК

Якщо необхідно імпортувати сертифікат ЦСК до сховища сертифікатів програми “Клієнт ЦСК”, необхідно в меню “Інструменти” вибрати пункт меню “Сертифікати”. У вікні “Сертифікати” вибрати вкладку “Сертифікати ЦСК” та натиснути кнопку “Імпорт…”. У вікні “Імпорт” в полі “Ім'я файлу:” вибрати сертифікат ЦСК, збережений до теки сертифікатів (або вказати url сертифіката ЦСК у загальнодоступній мережі, якщо є доступ). Натисніть “ОК”. Геш завантаженого у сховище сертифіката ЦСК додається, як геш довіреного сертифіката, згідно пункту “Цілісність сертифіката ЦСК” даної інструкції.

2.1.3. Завантаження кореневого сертифіката ЦЗО

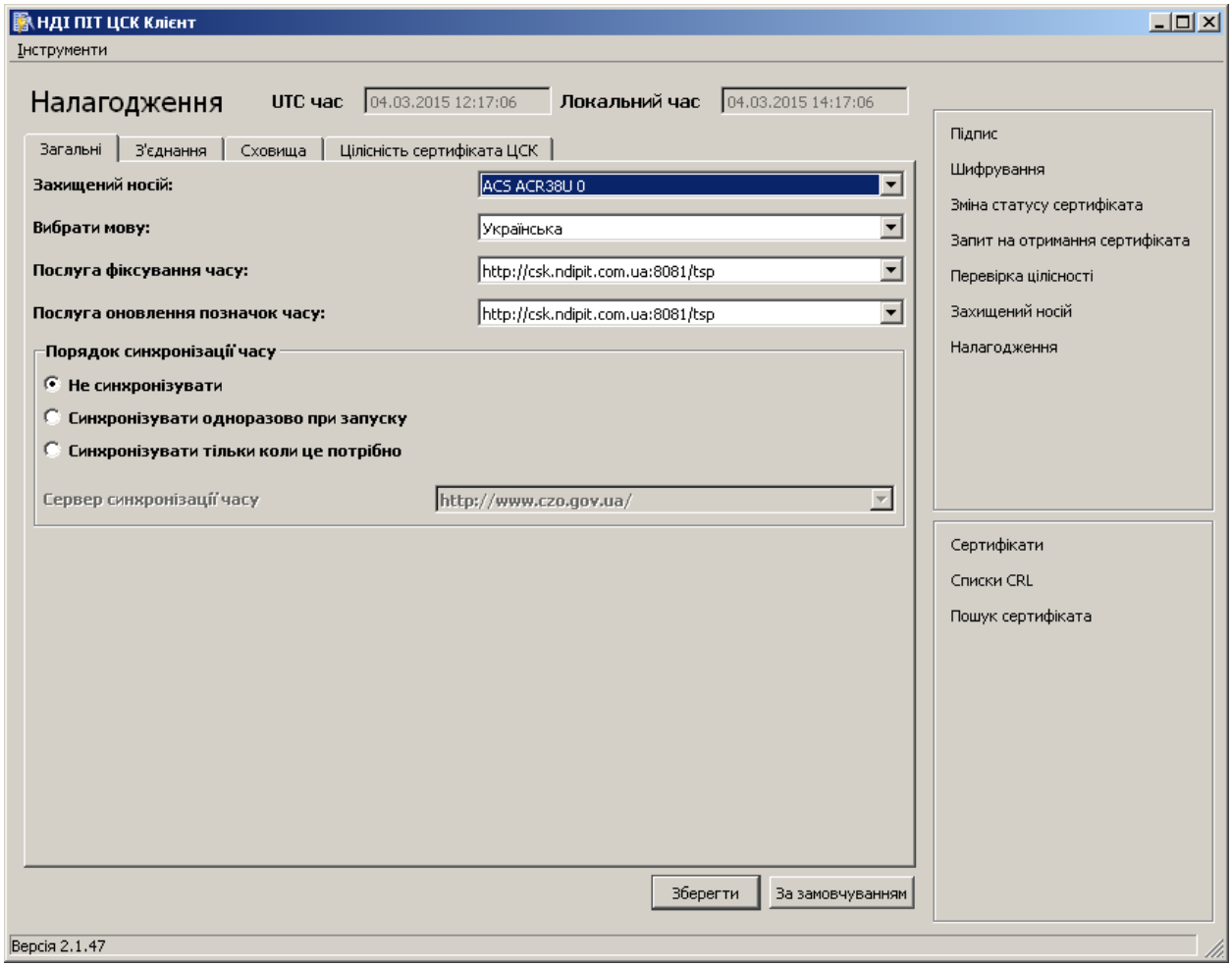
Якщо необхідно імпортувати новий сертифікат ЦЗО до сховища сертифікатів програми “Клієнт ЦСК”, необхідно в меню “Інструменти” вибрати пункт меню “Сертифікати”. У вікні “Сертифікати” вибрати вкладку “Сертифікати ЦЗО” та натиснути кнопку “Імпорт…”. У вікні “Імпорт” в полі “Ім'я файлу:” вибрати збережений до теки сертифікатів сертифікат ЦЗО (або вказати url сертифіката ЦЗО у загальнодоступній мережі, якщо є доступ). Натисніть “ОК”. Геш завантаженого у сховище сертифіката ЦЗО необхідно додати як геш довіреного сертифіката, як вказано в пункті “Цілісність сертифіката ЦСК” даної інструкції.

2.2. Налагодження параметрів

Перед роботою з програмою потрібно виконати налагодження параметрів програми. Програма інсталяції під час виконання встановлює основні параметри для роботи з програмою за замовчуванням. Для зміни цих параметрів в меню “Інструменти” потрібно вибрати пункт “Налагодження”. Змініть налагодження та натисніть “Зберегти”. Для того, щоб повернутися до первинних параметрів, натисніть кнопку “За замовчуванням”.

2.2.1 Загальні

У вікні “Налагодження” на вкладці “Загальні” (мал. 2.3) встановлюються загальні параметри роботи програми.



Мал. 2.3 Вкладка “Загальні”.

Захищений носій. У списку “Захищений носій” оберіть карт-рідер, в який буде вставляти носій особистого ключа.

Вибрати мову. У списку “Мова” вибирається мова для роботи з програмою. По замовчуванню встановлено “Українська”.

Послуга фіксування часу. У списку “Послуга фіксування часу” повинна зазначатися загальнодоступна точка доступу до послуги фіксування часу. По замовчуванню значення: url = http://csk.ndipit.com.ua:8081/tsp.

Послуга оновлення позначок часу. У списку “Послуга оновлення позначок часу” повинна зазначатися загальнодоступна точка доступу до послуги оновлення позначок часу. По замовчуванню значення url = http://csk.ndipit.com.ua:8081/tsp.

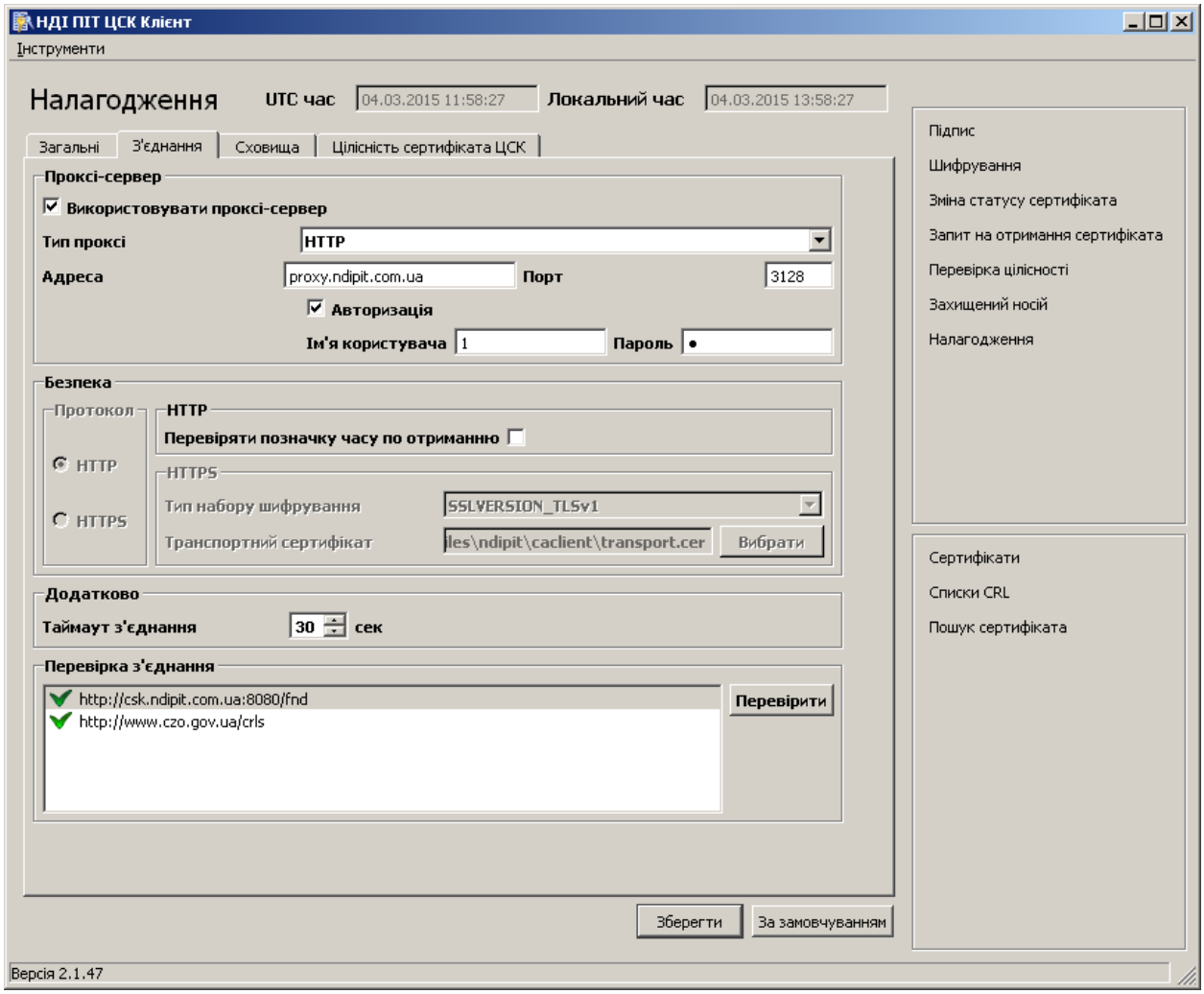
Порядок синхронізації часу. Група параметрів “Порядок синхронізації часу” дозволяє вказати порядок синхронізації часу у програмі (щоб здійснювалася синхронізація, потрібен доступ до Інтернет!). Можливі режими синхронізації:

- Не синхронізувати (при відсутності доступу до Інтернету необхідно вибрати цей пункт з метою запобіганню появи відповідних повідомлень при роботі Програми). Встановлено за замовчуванням;
- Синхронізувати одноразово при запуску (при наявності доступу до Інтернету). Програма синхронізується з сигналом точного часу (вказаному у списку “Сервер синхронізації часу”) тільки при запуску програми;
- Синхронізувати тільки коли це потрібно (при наявності доступу до Інтернету). Програма синхронізується з сигналом точного часу кожен раз, коли виникає необхідність отримати значення часу.

Сервер синхронізації часу. В даному списку обирається сервер, який надає сигнал точного часу мережею Інтернет. За замовчуванню встановлено параметр: http://www.czo.gov.ua/.

2.2.2. З’єднання

Параметри підключення та роботи з Інтернетом встановлюються у вікні “Налагодження” на вкладці “З'єднання” (мал. 2.4).



Мал. 2.4 Вкладка “З’єднання”.

Проксі-сервер. Дана група параметрів визначає можливість (за необхідності) підключатися до серверів взаємодії ЦСК у мережі Інтернет через проксі-сервер.

“Використовувати проксі-сервер”. У разі підключення Вашого комп’ютера до мережі Інтернет через проксі-сервер, необхідно активувати даний параметр. Тип сервера обрати у відповідному списку та прописати у відповідних полях ім’я сервера та номер порту.

“Авторизація”. Якщо для доступу до мережі необхідна авторизація, встановіть даний параметр та вкажіть у відповідних полях своє ім’я користувача та пароль.

За інформацією про параметри підключення Вашої локальної мережі (комп'ютера) звертайтесь до системного адміністратора Вашої мережі.

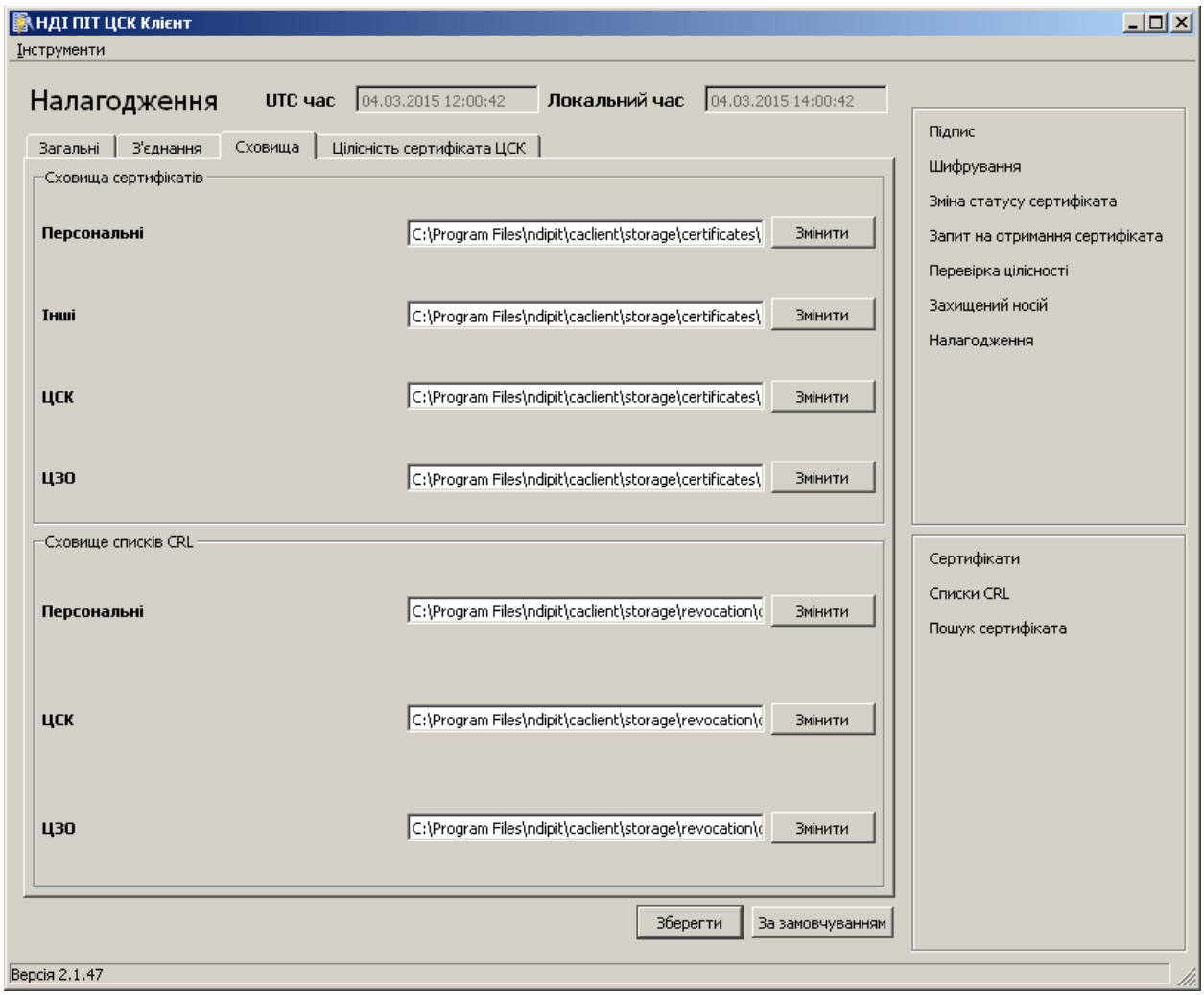
Безпека. Група параметрів для налаштування параметрів безпечного з’єднання. За замовчуванням встановлений протокол HTTP.

Додатково. Група параметрів, яка містить лише один параметр що встановлює Таймаут з’єднання.

Перевірка з’єднання. Для перевірки доступу до служб на серверах ЦСК та ЦЗО натисніть кнопку “Перевірка”. Результатом перевірки є значки ліворуч від відповідної адреси: вдалий - зелена галочка, невдалий – червоний хрестик.

2.2.3. Сховища

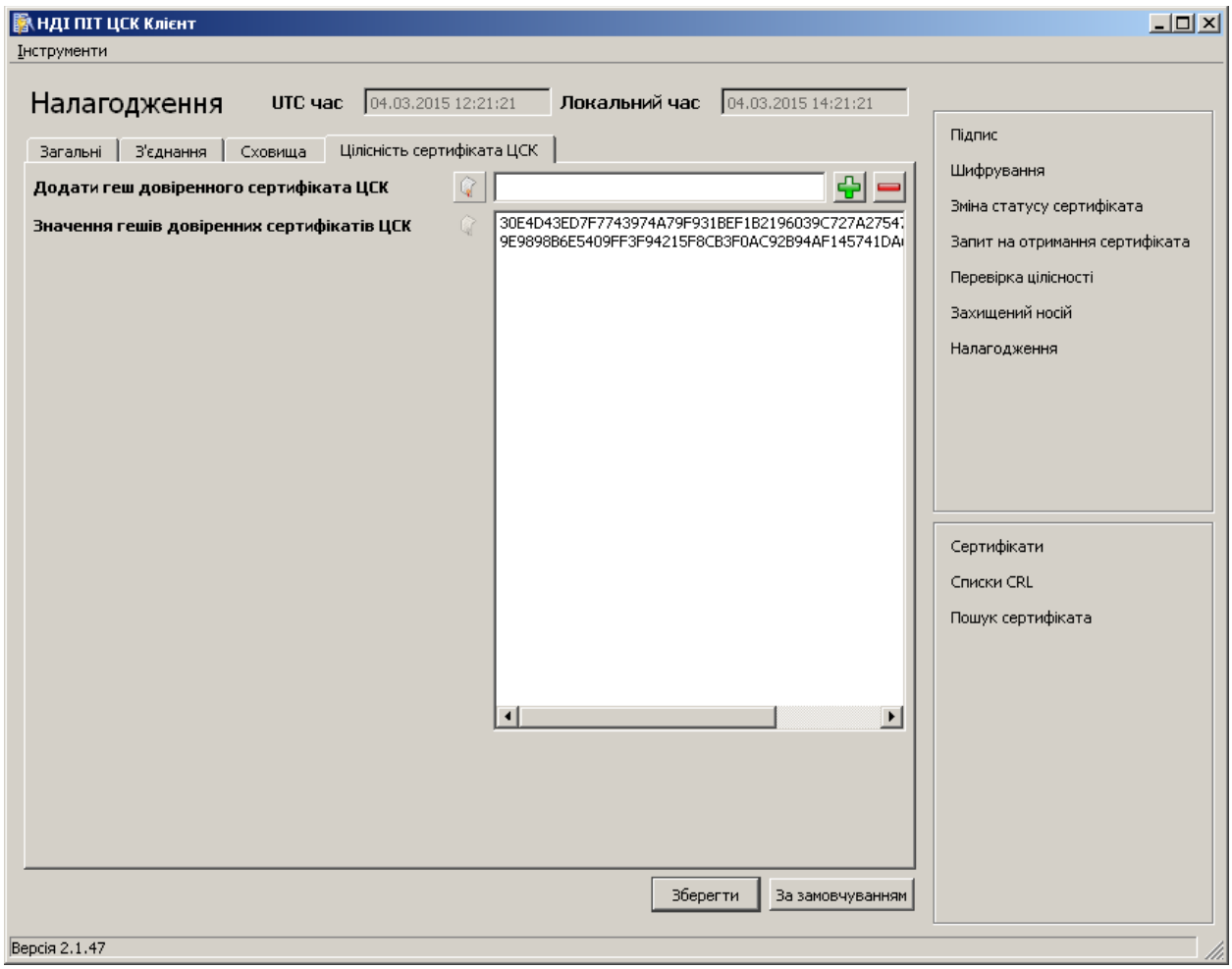
У вікні “Налагодження” на вкладці “Сховища” вказано місце зберігання завантажених сертифікатів та списків відкликаних сертифікатів (мал. 2.5). По замовчуванню сховища (тека “storage”) знаходяться у теці, в яку встановлено програму “Клієнт ЦСК”.



Мал. 2.5. Вкладка “Сховища”.

2.2.4. Цілісність сертифіката ЦСК

У вікні “Налагодження” на вкладці “Цілісність сертифіката ЦСК" (мал. 2.6) зберігаються геші довірених сертифікатів. Цей параметр може бути не встановлений за замовчуванням, але він є обов'язковим при роботі з програмою та призначений для зберігання еталонного значення гешу сертифікатів ЦСК.



Мал. 2.6. Вкладка “Цілісність сертифіката ЦСК”.

На вкладці “Цілісність сертифіката ЦСК” натисніть на кнопку-іконку “Додати геш довіреного сертифіката ЦСК” (), у вікні, що з'явилося, перейдіть на вкладку “Сертифікати ЦСК” (або “Сертифікати ЦЗО”), виділіть курсором необхідний сертифікат та натисніть кнопку "Вибрати". Щоб додати це значення в “Значення гешів довірених сертифікатів ЦСК” потрібно натиснути кнопку “плюс” ().

Щоб переглянути сертифікат до обраного гешу в полі “Значення гешів довірених сертифікатів ЦСК”, необхідно натиснути кнопку перегляду вибраного сертифіката () Щоб видалити значення, необхідно його вибрати та натиснути кнопку “мінус” ().

Перевірка цілісності сертифіката ЦСК полягає в порівнянні еталонного значення геш-функції сертифіката відкритого ключа ЦСК з підрахованим значенням геш-функції, розповсюджуваного сертифіката відкритого ключа ЦСК.

3. Робота з програмою

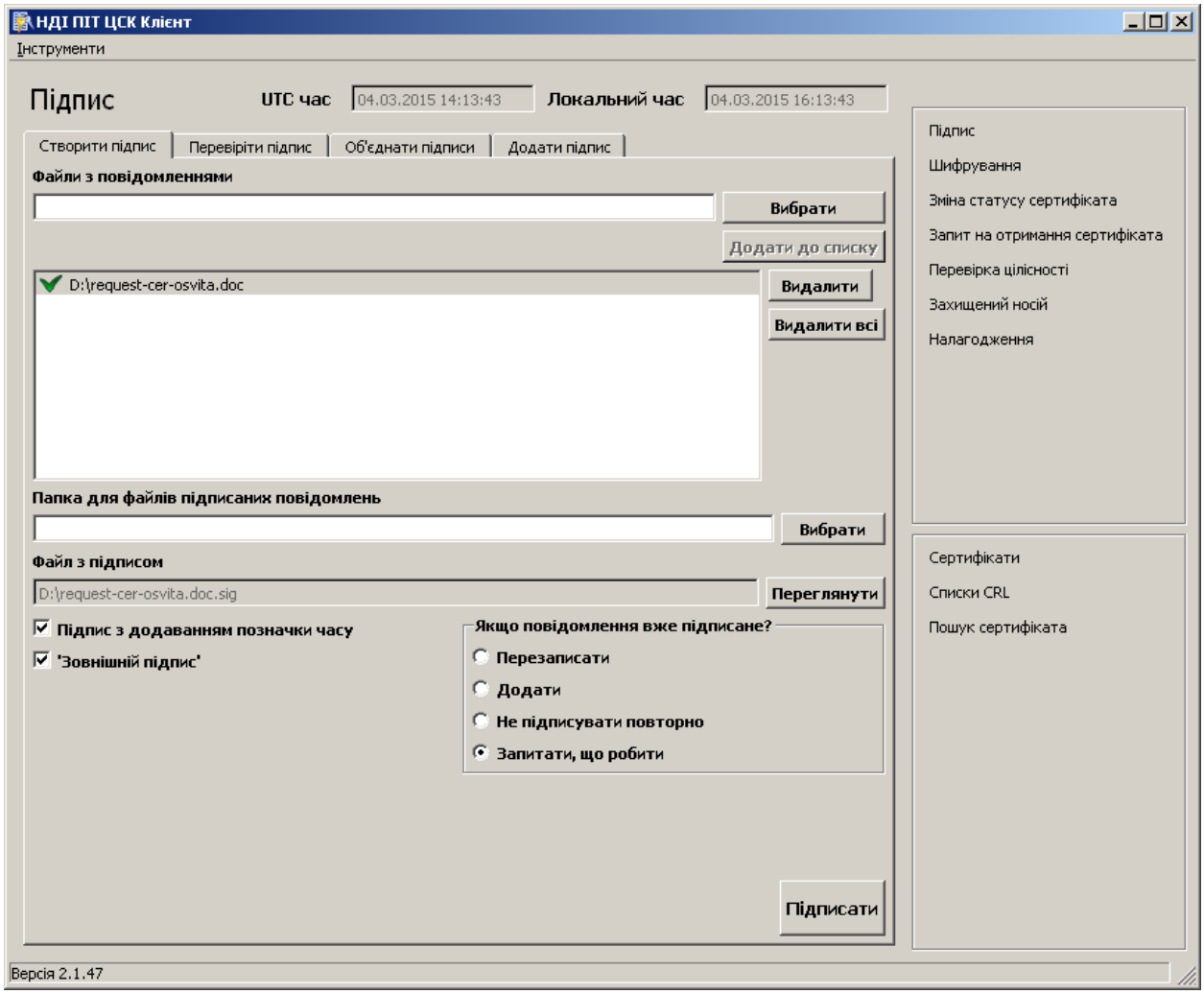
3.1. Підпис

3.1.1. Підписання повідомлень

Порядок накладання електронно-цифрового підпису:

1. Потрібно в меню “Інструменти” вибрати пункт “Підпис”.

2. На вкладці “Створити підпис” (мал. 3.1) натиснути кнопку “Вибрати” для того, щоб знайти файл, який необхідно підписати (або ввести адресу місцезнаходження цього файлу у поле “Файли з повідомленнями” та натиснути кнопку “Додати до списку”). Видалити файли з переліку, які буде підписано, можна за допомогою кнопки “Видалити” та “Видалити всі”.



Мал. 3.1 Вкладка “Створити підпис”.

Підпис з додаванням позначки часу. За необхідності можна включити у підпис позначку часу, встановивши прапорець “Підпис з додаванням позначки часу”.

Послуга “Позначка часу” дозволяє встановити чинність сертифіката на момент підпису документу та ідентифікувати момент накладання підпису.

Можливість зміни значення позначки часу підписаного документа в майбутньому навіть автором підпису – неможлива. Можливо, лише повторний підпис з фіксацією нового часу.

Зовнішній підпис. Даний параметр вказує, чи повинен файл підпису містити дані, що підписуються. Встановлений прапорець “Зовнішній підпис” означає, що підпис буде

зберігатися в окремому файлі. Доцільно використовувати у разі, якщо файл, який необхідно підписати, має великий розмір (що ускладнить його передачу через мережу Інтернет) або його можливо отримати з загальнодоступних ресурсів. Якщо файл підписується декількома користувачами даний параметр необхідно встановити кожному з них.

При накладанні зовнішнього підпису (зі встановленою позначкою “Зовнішній підпис”) - створюється новий файл, який містить усі підписи але не містить самих даних , що підписувались. Тому при перевірці зовнішнього підпису необхідно, щоб із файлом підписів знаходився файл, який було підписано. Якщо не встановлена позначка “Зовнішній підпис” – створюється файл з підписами, який містить дані, що підписуються.

В полі “Папка для файлів підписаних повідомлень” можна вказати папку, до якої буде записано створений файл з підписом. Це поле заповнювати не обов`язково. За замовчуванням файл з підписом записується в той же каталог, де знаходиться вхідний файл, що підписується.

Програма дозволяє сформувати для одного документу декілька підписів.

При наявності у файлу, що підписується, раніше накладеного підпису, потрібно обрати: чи повинна програма замінити існуючий підпис, чи додати підпис до вже існуючого, чи запитати, що робити для кожного такого файлу індивідуально. Це робиться за допомогою групи параметрів: “Якщо повідомлення вже підписане”.

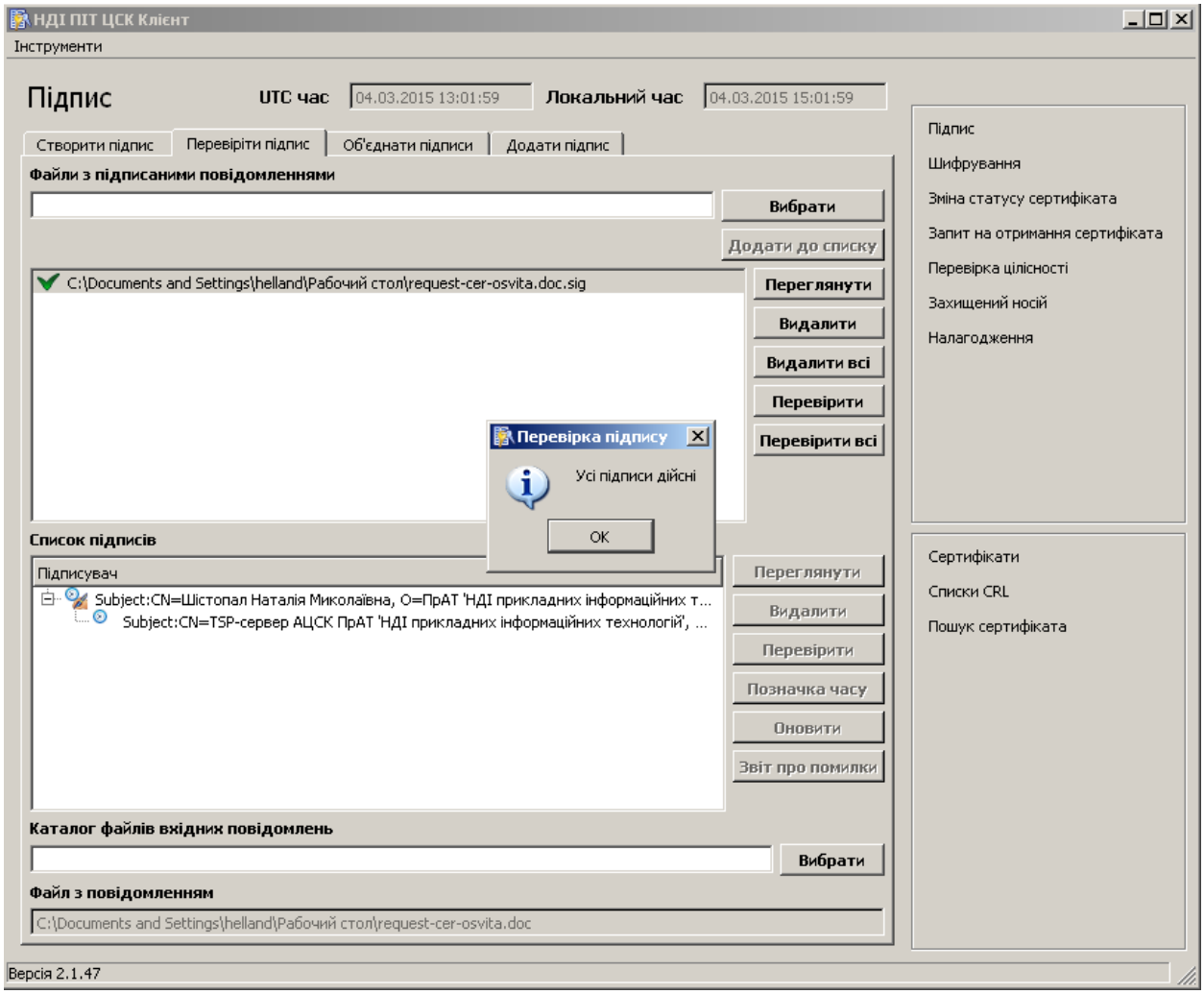
3. Після вибору необхідних параметрів, вставте захищений носій у карт-рідер. Даний рідер має бути обраний в пункті меню “Налагодження” вкладка “Загальні” в полі “Захищений носій”

4. Натиснути кнопку “Підписати”.

5. У вікні “Перевірити ПІН”, що з'явиться, потрібно вписати ПІН для доступу до особистого ключа та натиснути ОК.

3.1.2. Перевірка підписаного повідомлення

Для перевірки підпису потрібно в меню “Інструменти” вибрати пункт меню “Підпис”, у вікні “Підпис” перейти на вкладку “Перевірити підпис” (мал. 3.2), вибрати підписані файли за допомогою кнопки “Вибрати” (“Додати до списку”) та натиснути кнопку “Перевірити” або “Перевірити всі”. У разі успішної перевірки з'явиться вікно з повідомленням “Усі підписи дійсні” або “Підписи на усіх повідомленнях дійсні”.

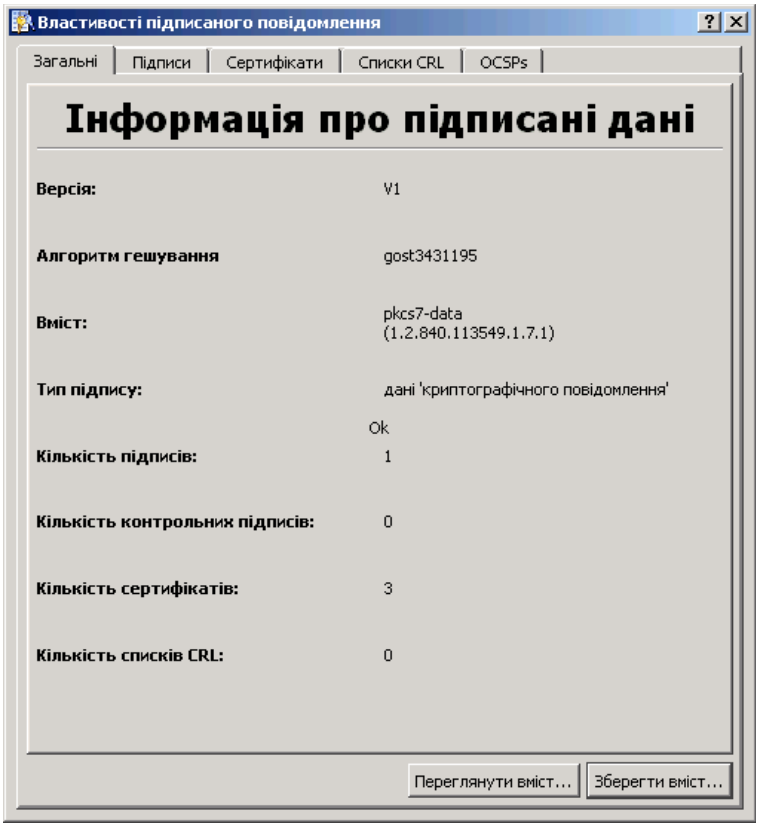


Мал. 3.2 Вкладка “Перевірити підпис”.

Властивості підписаного повідомлення можна переглянути у відповідному вікні (мал. 3.3), виділивши файл з підписами та натиснути з правої сторони кнопку “Переглянути”.

У разі необхідності отримання вихідного повідомлення, на який було накладено підписи, у вікні “Властивості підписаного повідомлення” на вкладці “Загальні”, для збереження натискаєте кнопку “Зберегти вміст…”, а для перегляду повідомлення, натиснути кнопку “Переглянути вміст…”.

На вкладках “Підписи” “Сертифікати”, “Списки CRL”, “OCSPs” можна отримати інформацію про підписи, відповідні сертифікати та дані, що підтверджують чинність підписів.



Мал. 3.3 Вікно “Властивості підписаного повідомлення”.

У полі “Список підписів” відображається усі підписи. Для отримання інформації про підписувача необхідно виділити курсором необхідний підпис та натиснути кнопку “Переглянути”. У вікні “Властивості підпису”, що з’явиться, можна переглянути інформація про сертифікати підписувача та отримати їх. За необхідності видалити підпис із файлу підписів – виділяєте курсором підпис та натискаєте кнопку “Видалити”. Перевірити вибраний підпис зі списку можна натиснувши кнопку “Перевірити”. За необхідності додати позначку часу до одного з підписів – виділяєте курсором підпис у списку та натискаєте кнопку “Позначка часу”. Для оновлення позначки часу на вибраному підписі - натискаєте кнопку “Оновити”.

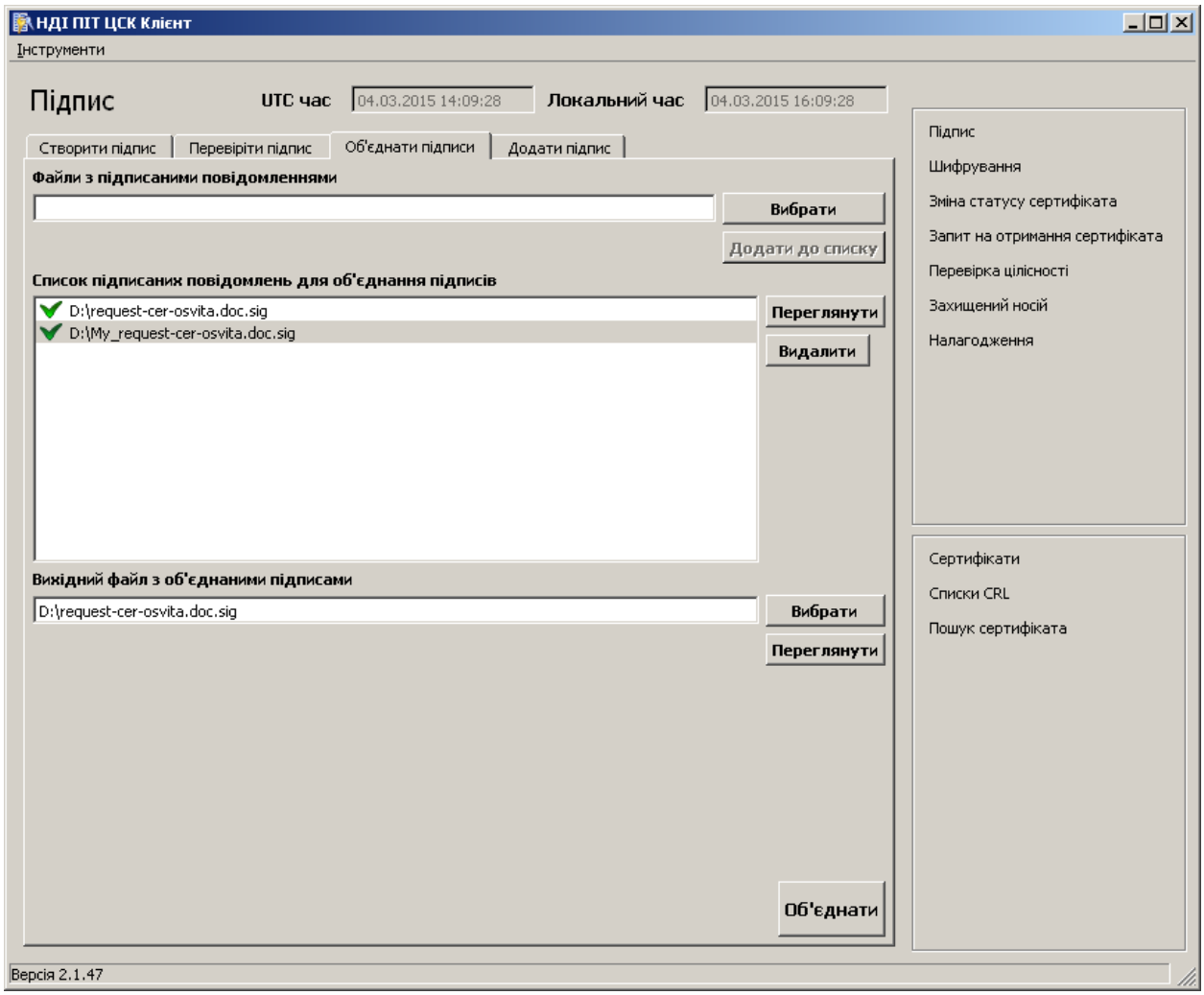
Для отримання інформації при невдалій перевірці підпису необхідно натиснути кнопку “Звіт про помилку”.

При перевірці зовнішнього підпису, якщо файл підпису і підписане повідомлення лежать в різних каталогах – необхідно в полі “Каталог файлів вхідних повідомлень” вказати шлях до підписаного файлу, підпис якого перевіряється.

3.1.3. Об'єднання підписів

Для об'єднання декількох підписів, що знаходяться у декількох файлах в один файл з цими підписами, потрібно вибрати пункт “Підпис” меню “Інструменти”, перейти на вкладку “Об'єднати підписи” (мал.. 3.4). У полі “Вихідний файл з об'єднаними підписами” вибрати вихідний файл, що буде містити об'єднані підписи. Вибрати решту файлів підписаних повідомлень, підписи яких необхідно долучити до вихідного файлу, за допомогою кнопки “Вибрати”, що розташована поряд з вікном “Файли з підписаними повідомленнями” і натиснути кнопку “Об'єднати”. Отримаємо повідомлення “Всі підписи підписаних повідомлень успішно об'єднано”. Дана функція використовується у разі необхідності об'єднати підписи одного і того ж файлу декількох підписувачів, які розглядали файл одночасно, за умови, що файл був підписаний без редагувань. В

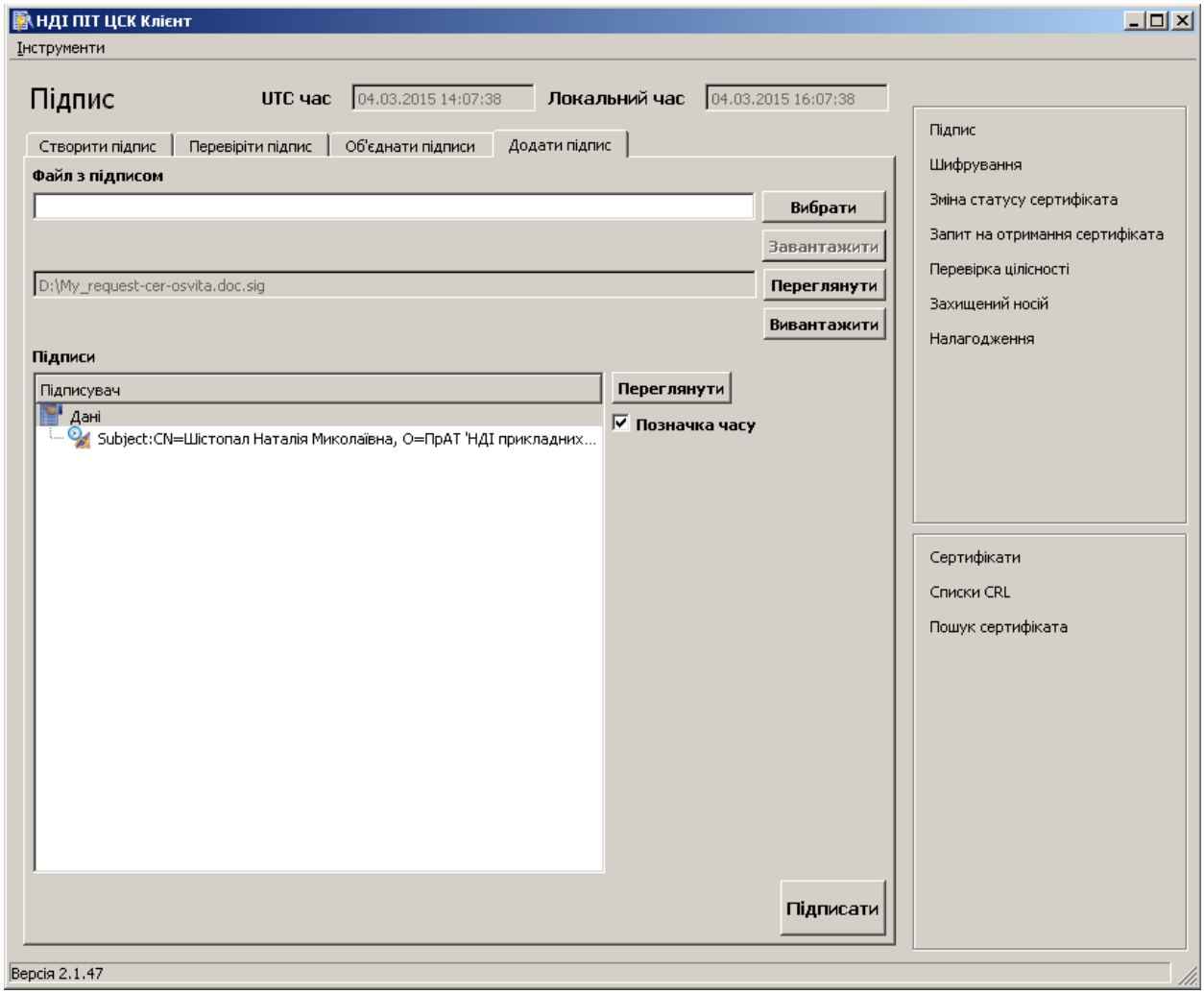
результаті утворюється один файл, що буде містити усі підписи. Кнопки “Переглянути” дозволяє ознайомитись із властивостями підписаного повідомлення.



Мал. 3.4 Вкладка “Об'єднати підписи”.

3.1.4. Додавання підпису

Щоб додати свій підпис до вже підписаного файлу, потрібно у вікні “Підпис” перейти на вкладку “Додати підпис” (мал. 3.5). Вказати файл з підписом за допомогою кнопки “Вибрати” або прописати повний шлях до файлу з підписом у відповідному полі і натиснути кнопку “Завантажити”.



Мал. 3.5 Вкладка “Додати підпис”.

Кнопки “Переглянути” дозволяють переглянути підписане повідомлення, а також властивості підписаного повідомлення та підписів.

Встановлений параметр “Позначка часу” дозволяє накласти підпис із позначкою часу. Для підписання даних файлу повідомлення необхідно, щоб у вікні “Підписи” було обрано “Дані”. Після вибору необхідних параметрів потрібно натиснути кнопку "Підписати". Вставте захищений носій у пристрій для роботи з захищеними носіями (карт-рідер).

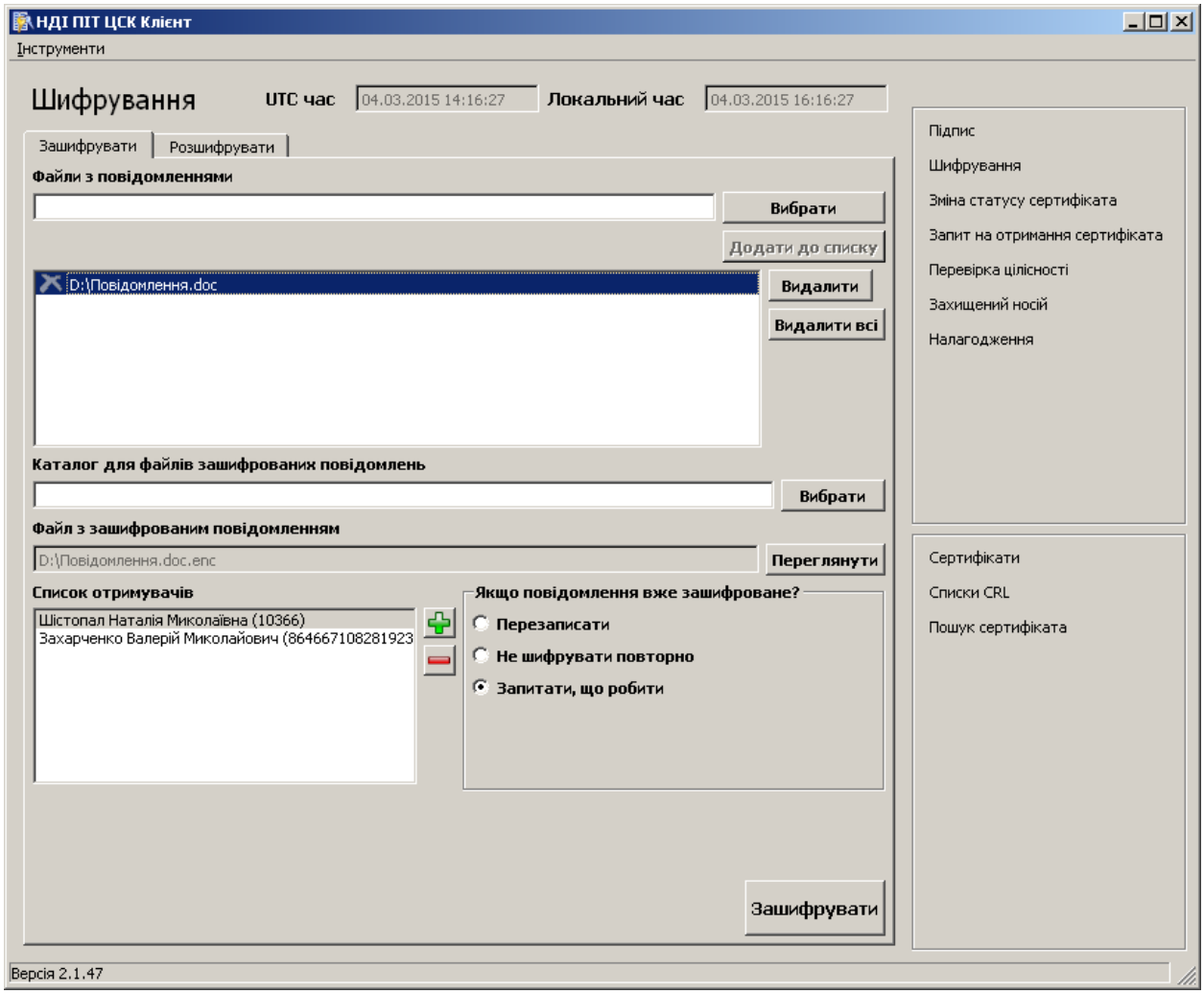
У вікні “Перевірити ПІН”, що з'явиться, потрібно вписати ПІН для доступу до особистого ключа, та натиснути ОК.

Примітка. У разі необхідності отримання вихідного повідомлення, на який було накладено підписи, потрібно виділити файл з підписами та натиснути з правої сторони кнопку “Переглянути”, а у вікні, що відкриється – кнопку “Зберегти вміст”, після чого вибрати місце, куди необхідно зберегти повідомлення.

У разі необхідності переглянути вихідне повідомлення, на яке було накладено підписи, без його зберігання, потрібно виділити файл з підписами та натиснути з правої сторони кнопку “Переглянути”, а у вікні, що відкриється – кнопку “Переглянути вміст”, після чого відкриється текст вихідного повідомлення.

3.2. Шифрування та розшифрування повідомлень
3.2.1. Зашифрувати повідомлення

Для зашифровування файлу з повідомленням потрібно в меню “Інструменти” вибрати пункт “Шифрування”. На вкладці “Зашифрувати” (мал. 3.6) в полі “Файл з повідомленнями” вказати необхідний файл для зашифровування, натиснувши кнопку “Вибрати”.



Мал. 3.6 Вкладка “Зашифрувати”.

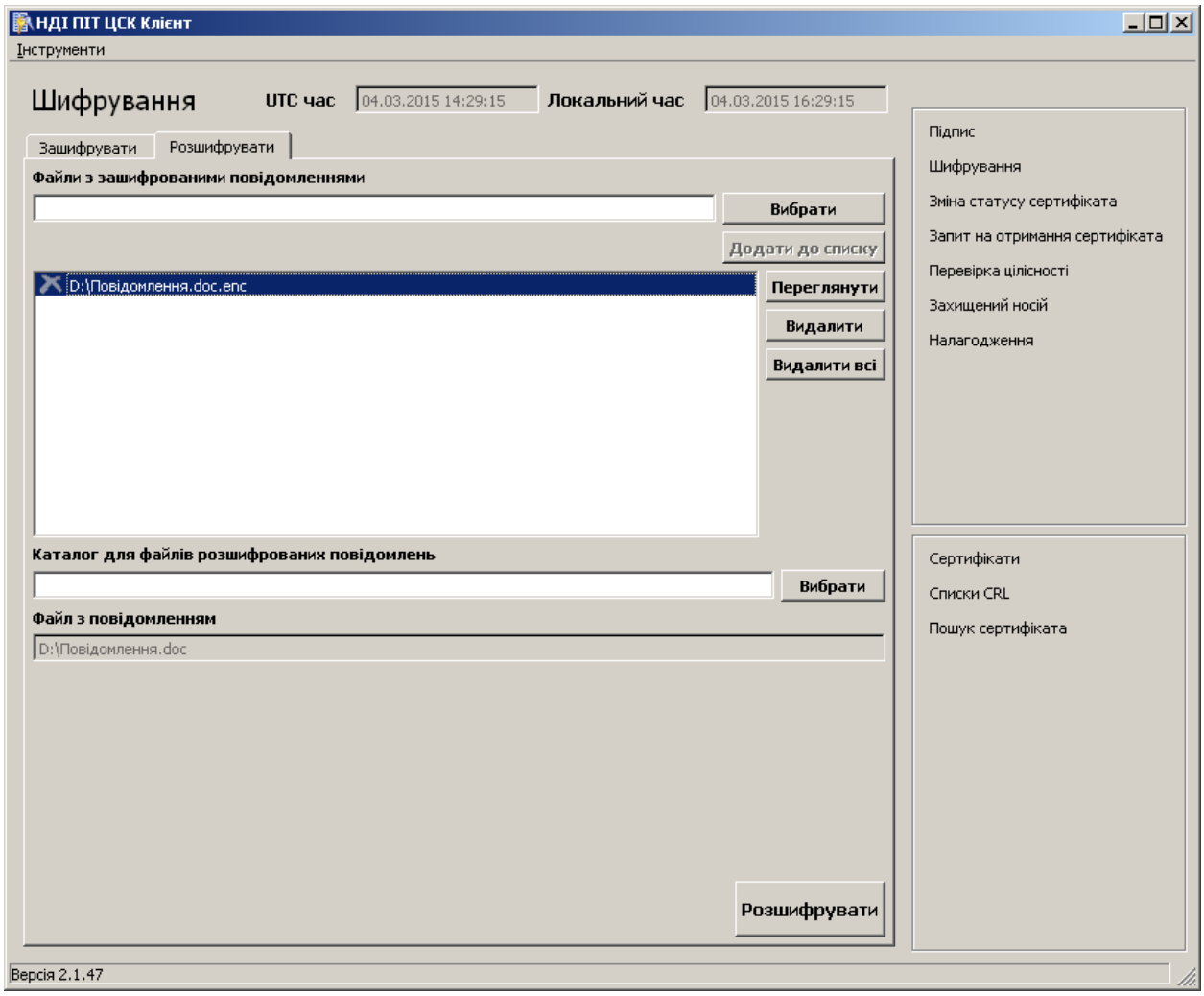
Кнопки “Видалити” та “Видалити всі” дозволяють редагувати список повідомлень для зашифровування. В полі “Каталог для файлів зашифровуваних повідомлень” можна вказати каталог, до якого буде записано зашифровуваний файл. Це поле заповнювати не обов`язково. По замовчуванню зашифрований файл записується в ту ж теку, де знаходиться вхідний файл, що шифрується. У разі, якщо вибраний файл вже зашифровано, потрібно обрати один з наступних варіантів: потрібно перезаписати існуючий шифрований файл (застосовується у разі, якщо необхідно змінити список отримувачів, при цьому потрібно, щоб був наявний вихідний файл), відмовитися зашифрувати повторно (у разі, якщо було вибрано помилково вже зашифрований файл), чи запитати, що робити для кожного такого файлу індивідуально. Це робиться за допомогою групи параметрів: “Якщо повідомлення вже зашифроване”.

Обов'язково необхідно додати в поле “Список отримувачів” сертифікати отримувачів, які зможуть розшифрувати це повідомлення, натиснувши кнопку  “Плюс” та натисніть “Зашифрувати”.

Після зашифрування можна переглянути інформацію про файл з зашифрованим повідомленням, натиснувши на кнопку “Переглянути”.

3.2.2. Розшифрування повідомлення

Для розшифрування отриманого повідомлення зашифрованого для Вас, необхідно у вікні “Шифрування” перейти на вкладку “Розшифрувати” (мал. 3.7). За допомогою кнопки ”Вибрати” оберіть файли з зашифрованими повідомленнями.



Мал. 3.7 Вкладка "Розшифрувати".

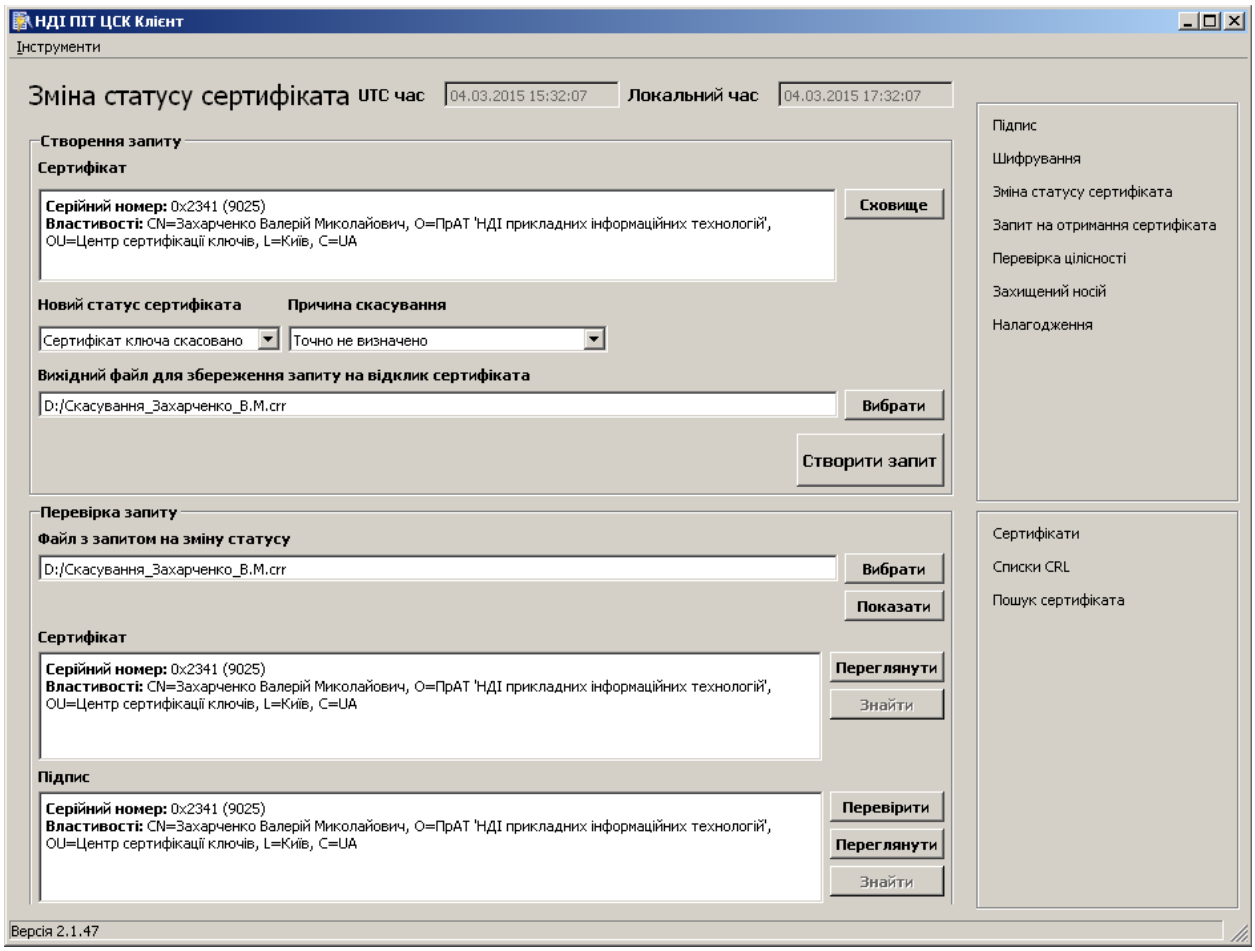
За допомогою кнопки “Переглянути” можна переглянути інформацію про зашифроване повідомлення. Кнопки “Видалити” та “Видалити всі” дозволяють редагувати список зашифрованих повідомлень для розшифрування. В полі “Каталог для файлів розшифрованих повідомлень” можна вказати каталог, до якого буде записано розшифровані файли. Це поле заповнювати не обов`язково. По замовчуванню розшифрований файл записується в той каталог, де знаходиться вхідний файл, що розшифровується.

Вставте захищений носій з особистим ключем до карт-рідера та натисніть кнопку “Розшифрувати”. У вікні “Перевірити ПІН”, що з'явиться, потрібно вписати ПІН для доступу до особистого ключа, та натиснути ОК.

3.3. Зміна статусу сертифіката

Щоб змінити статус сертифіката відкритого ключа необхідно в меню “Інструменти” вибрати пункт меню “Зміна статусу сертифіката”. У вікні “Зміна статусу сертифіката” (мал. 3.8) в групі параметрів “Створення запиту”, натиснувши кнопку “Сховище”, вибираєте зі сховища сертифікат, статус якого необхідно змінити.

Інформація про сертифікат, статус якого змінюється, відображається в полі “Сертифікат”. У списку “Новий статус сертифіката” вибираєте статус на який потрібно змінити діючий (при скасуванні вказується причина скасування у відповідному списку). У відповідному полі вказуєте назву вихідного файлу для збереження запиту на відклик сертифіката. По замовчуванню файл створюється у теці, в якій встановлено програму. Повний шлях файлу вказується або за допомогою кнопки “Вибрати”, або прописом в полі імені файлу. Натискаєте кнопку “Створити запит”, підписуєте запит. Після вдалого підписання формується файл запиту на зміну статусу сертифіката.



Мал. 3.8 Вікно “Зміна статусу сертифіката”.

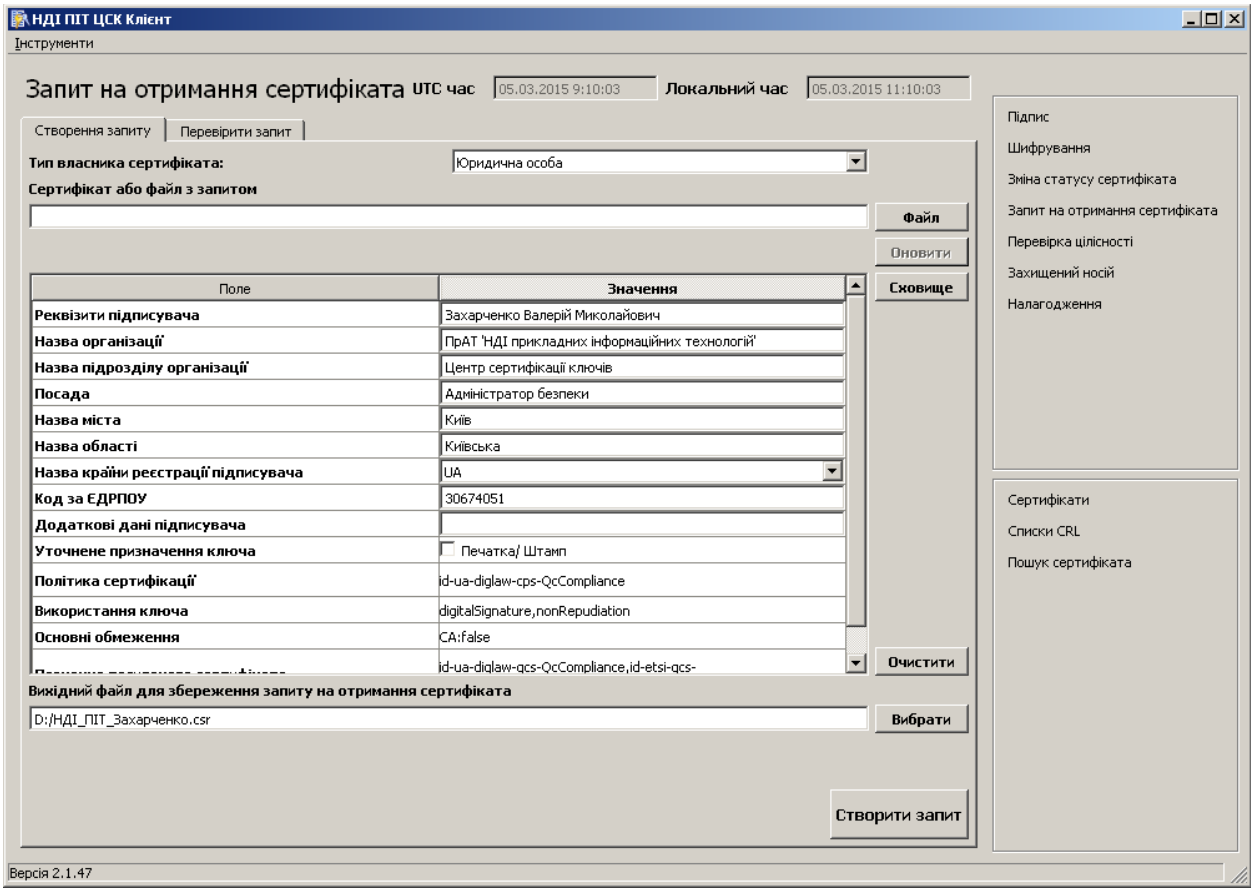
Група параметрів “Перевірка запиту” надає можливість перевірити запит на зміну статусу сертифіката. За допомогою кнопки “Вибрати” обираєте файл з запитом на зміну статусу у відповідному полі. Кнопка “Показати” дозволяє відобразити інформацію про формування запиту.

У полі “Сертифікат” відображається інформація про сертифікат, статус якого змінюється. Кнопка “Переглянути” відкриває вікно “Властивості сертифіката” з детальною інформацією про сертифікат, статус якого змінюється.

У полі “Підпис” відображається інформація того, хто підписав запит на зміну статусу сертифіката. Кнопка “Перевірити” – дозволяє перевірити підпис на запиті. Кнопка “Переглянути” відкриває вікно властивостей сертифіката, яким підписано запит.

3.4. Запит на отримання сертифіката

Щоб сформувати запит на отримання сертифіката ключа потрібно в меню “Інструменти” вибрати пункт меню “Запит на отримання сертифіката”. У вікні “Запит на отримання сертифіката”, що з’явиться, містяться дві вкладки: “Створення запиту” (мал. 3.9) та “Перевірити запит” (мал. 3.10).



Мал. 3.9 Вкладка “Створення запиту”.

“Створення запиту”. Для формування файлу запиту необхідно в списку “Тип власника сертифіката” вибрати, кому формується сертифікат: представникам юридичної особи - “Юридична особа”; фізичним особам - “Фізична особа”; для ключа шифрування - “Узгодження ключів”; фізичній особі-підприємцю - “Фізична особа-підприємець” і заповнити форму, що міститься нижче.

Заповнюєте значення полів даними, які буде внесено до сертифікатів. Щоб заповнити форму запиту даними з існуючого файлу запиту або сертифіката, в полі “Сертифікат або файл з запитом” вкажіть необхідний файл. Кнопка “Оновити” дозволяє оновити дані в формі запиту після редагування з обраного файлу. Кнопка “Сховище” дозволяє вибрати сертифікат, даними з якого буде заповнена форма запиту. Кнопка “Очистити” дозволяє очистити та встановити по замовчуванню поля запиту на формування сертифіката.

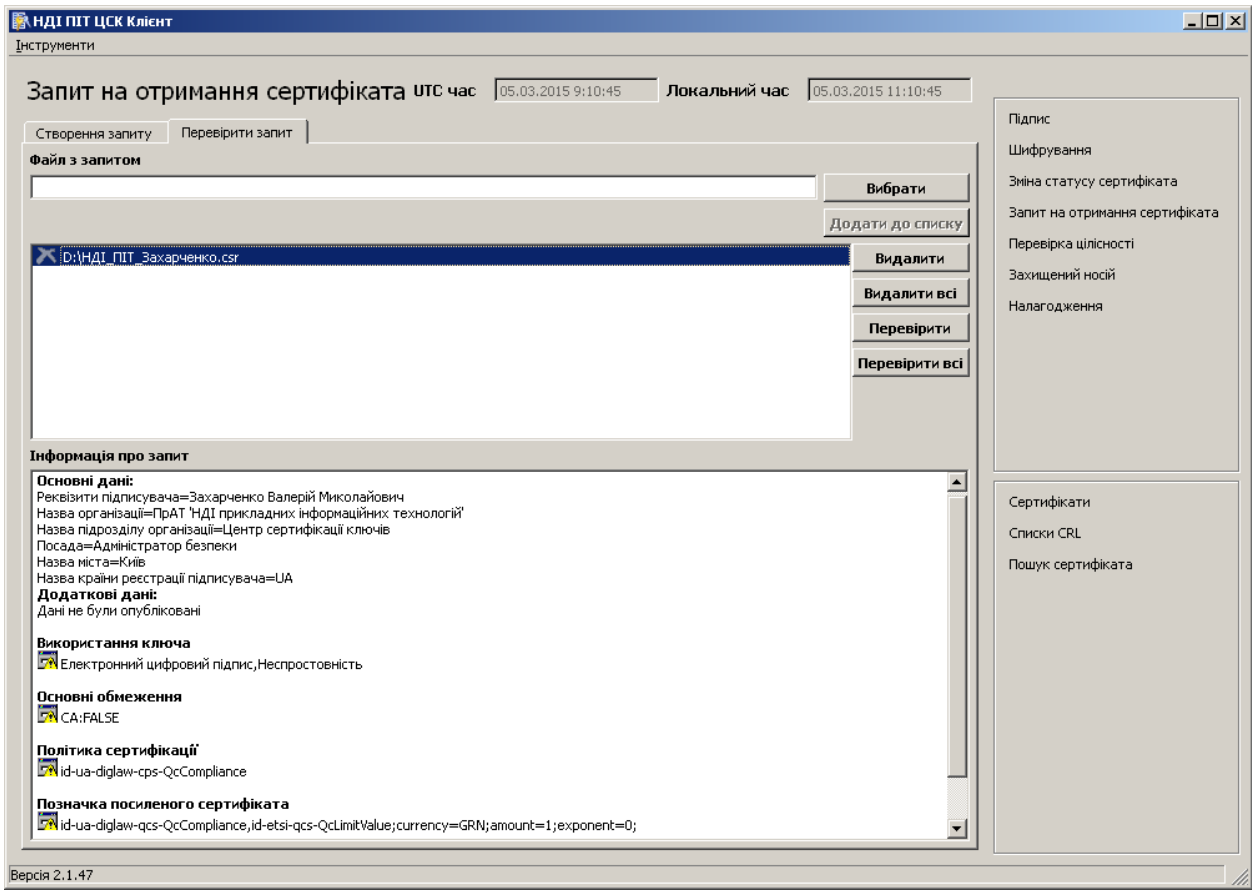
Назву вихідного файлу для збереження запиту на отримання сертифіката вказується у відповідному полі. По замовчуванню файл створюється у теці, в яку встановлена програма. Кнопка “Вибрати” дозволяє вказати іншу теку для збереження файлу запиту.

Для створення файлу запиту на отримання сертифіката, на основі вказаних даних, необхідно встановити захищений носій ключової інформації, зі згенерованим ключем, в карт-рідер та натиснути кнопку “Створити запит”.

“Перевірити запит”. Для перевірки запиту необхідно на вкладці “Перевірити запит” (мал. 3.10) в полі “Файл з запитом” вибрати файл із запитом на отримання сертифіката: кнопка “Вибрати” дозволяє вибрати файл у вікні пошуку; прописати в полі “Файл з запитом” повну адресу файлу та натиснути кнопку “Додати до списку”. При виділенні запиту курсором, у полі “Інформація про запит” відображаються дані, з якими буде сформований сертифікат.

Кнопки “Видалити” та “Видалити всі” дозволяють редагувати список запитів.

Кнопки “Перевірити” та “Перевірити всі” дозволяють перевірити деякі або всі запити на отримання сертифіката зі списку.

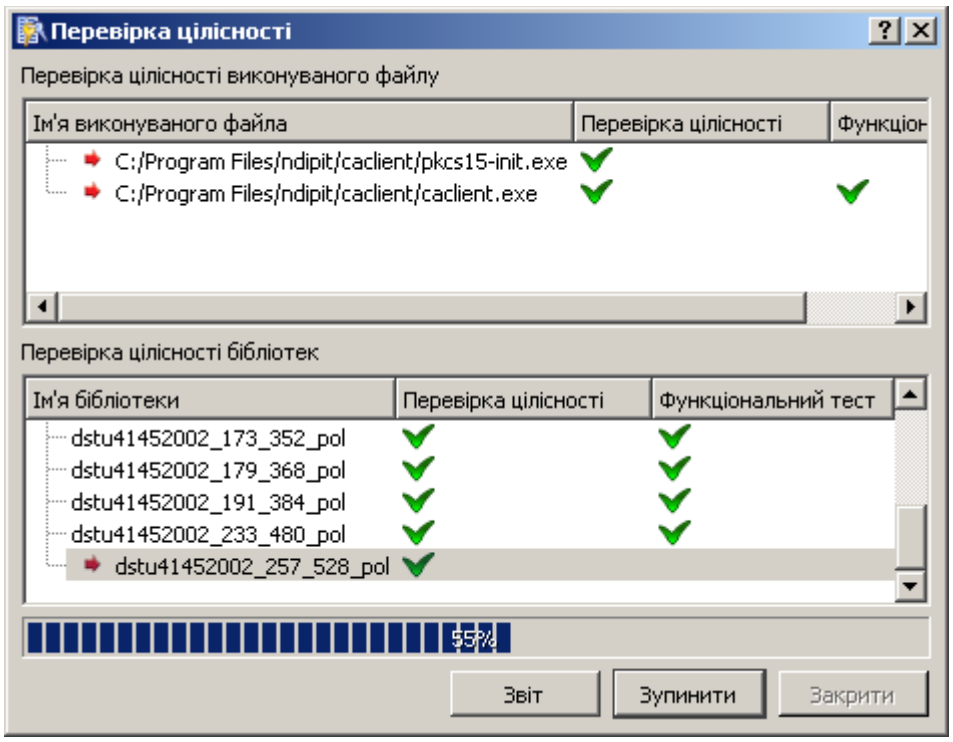


Мал. 3.10 Вкладка “Перевірити запит”.

3.5. Перевірка цілісності

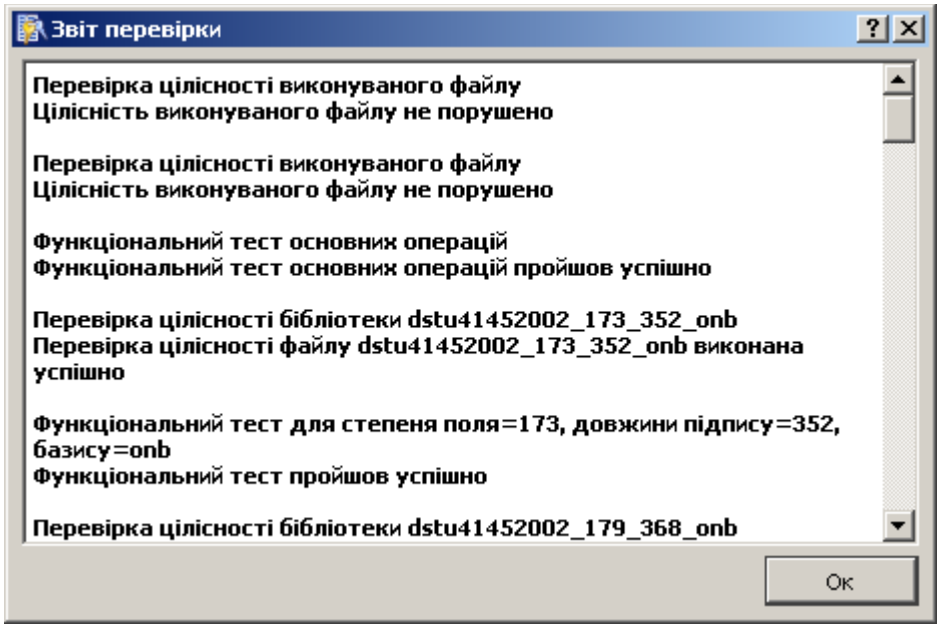
У разі виникнення збоїв при роботі з програмою необхідно робити перевірку цілісності програми. Перевірка цілісності – виконання набору тестів для оцінки правильності роботи програми та здійснення перевірки цілісності власних виконуваних файлів та програмних бібліотек.

Перевірка виконується за запитом користувача: в меню “Інструменти” вибрати пункт “Перевірка цілісності”, у вікні “Перевірка цілісності” (мал. 3.11), що з'явиться, натисніть кнопку “Старт”.



Мал. 3.11 Вікно “Перевірка цілісності”.

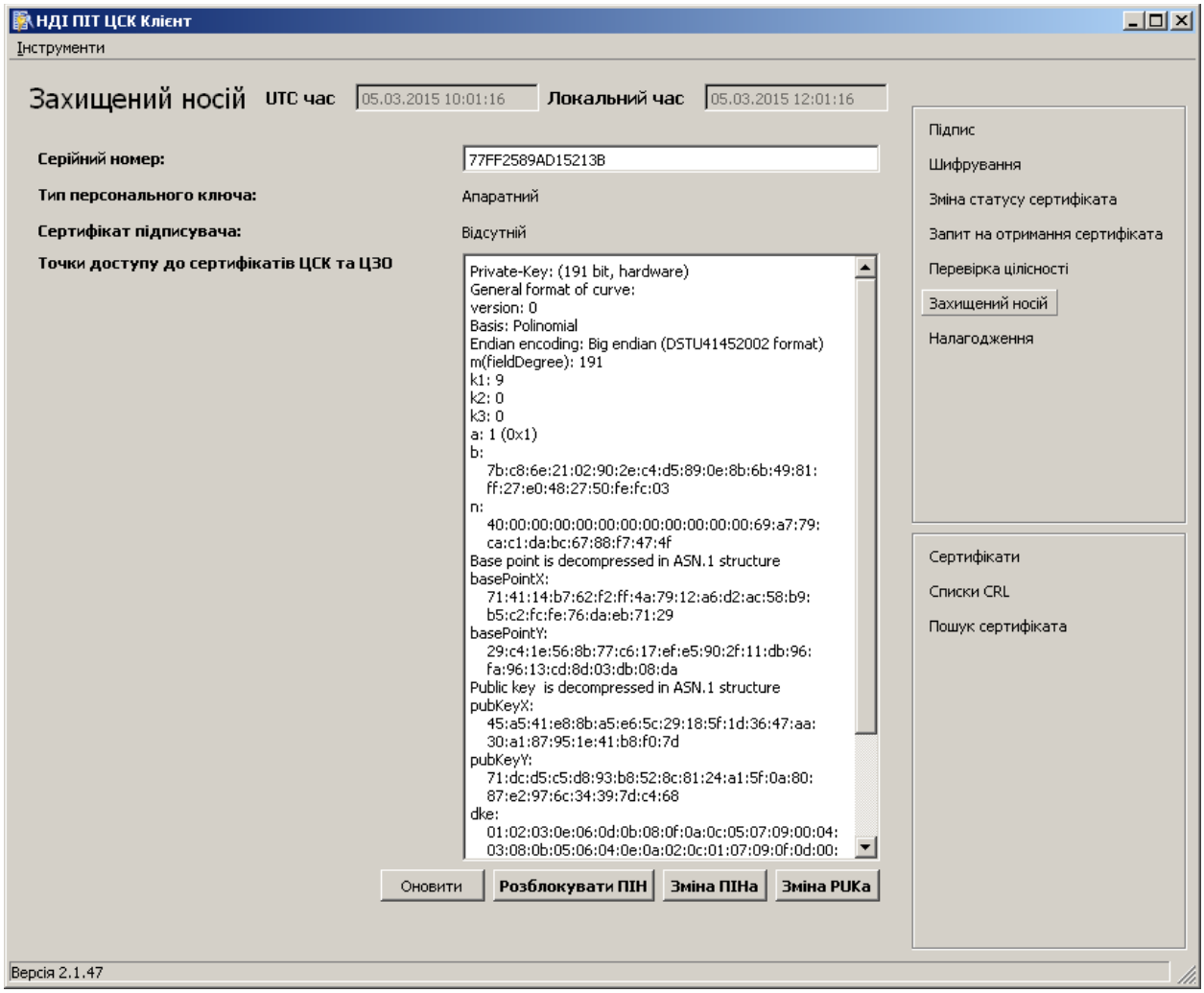
Червоний хрест у полі “Перевірка цілісності” вказує на те, що дана компонента не пройшла успішно перевірку і могла бути пошкоджена. Після закінчення даної операції можна переглянути звіт перевірки (мал. 3.12).



Мал. 3.12 Вікно “Звіт перевірки”.

3.6. Захищений носій

В меню “Інструменти” при виборі пункту меню “Захищений носій” відбувається зчитування та відображення даних з захищеного носія, який вставлено в карт-рідер (мал. 3.13). Для повторного зчитування інформації з носія вставленого в карт-рідер необхідно натиснути кнопку “Оновити”.



Мал. 3.13 Вкладка “Захищений носій”.

У вікні також надається можливість змінити ПІН та PUK до захищеного носія, який вставлений в карт-рідер.

Розблокувати ПІН. Щоб розблокувати заблокований ПІН до захищеного носія ключової інформації необхідно натиснути кнопку “Розблокувати ПІН”, у вікні, що з’явиться, у відповідні поля вводите код розблокування ПІНа та новий ПІН та натиснути кнопку “Ок”.

Зміна ПІНа. Щоб змінити код доступу до захищеного носія потрібно натиснути кнопку “Зміна ПІНа” та у вікні “Зміна ПІНа”, що з'явиться, ввести старий (поточний) та новий ПІН у відповідних полях. Натисніть кнопку “Ок” для зміни ПІНа або кнопку “Відмінити” для скасування.

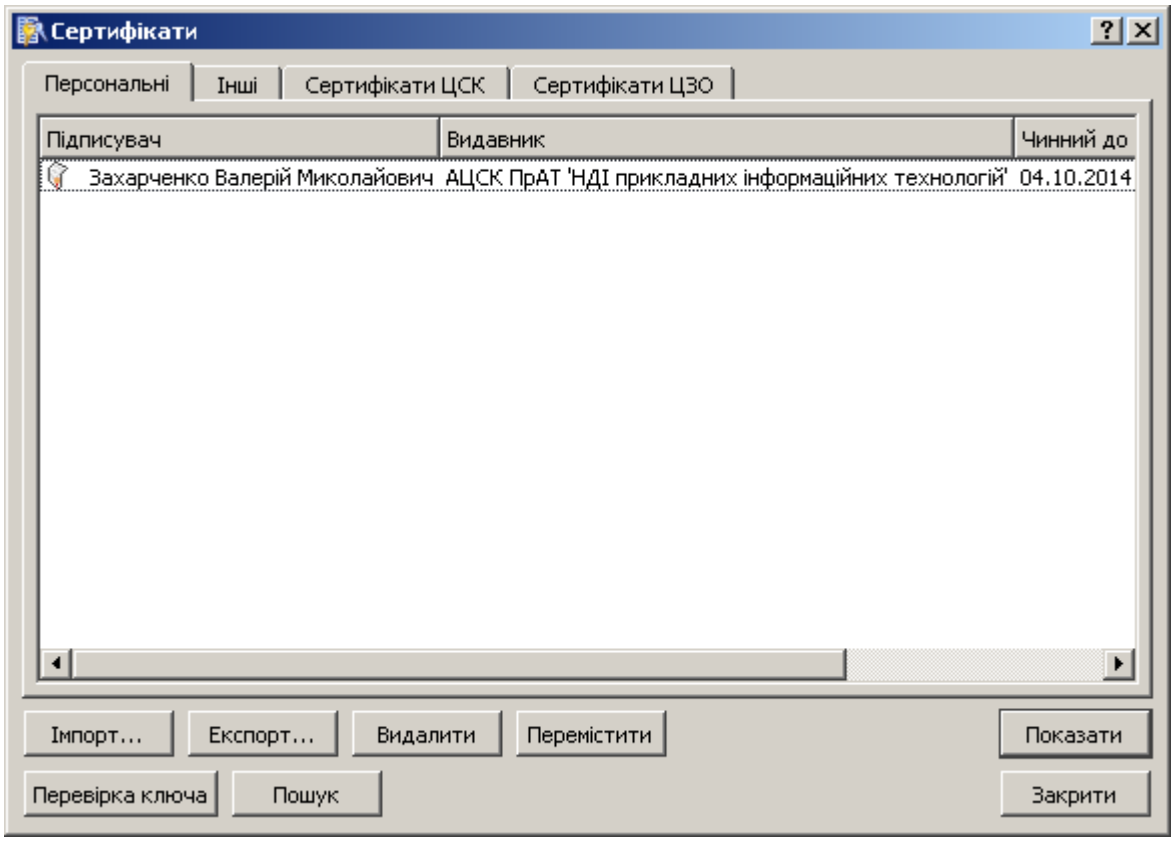
Зміна PUKa. Щоб змінити код розблокування ПІНа (PUK) до захищеного носія потрібно натиснути кнопку “Зміна PUKa” та у вікні “Зміна PUKa”, що з'явиться, ввести старий та новий PUK у відповідних полях. Натисніть кнопку “Ок” для зміни PUKa або кнопку “Відмінити” для скасування.

Примітка. Рекомендуємо відразу знищити старі значення ПІН та PUK, з метою усунення помилок при введенні кодів, оскільки після п’яти невдалих спроб введення кодів захищений носій блокується.

У разі блокування захищеного носія (при перевищенні кількості введення невірного кодів) або втрати паролів доступу звертайтесь за консультацією до співробітників ЦСК.

3.7. Сховища сертифікатів

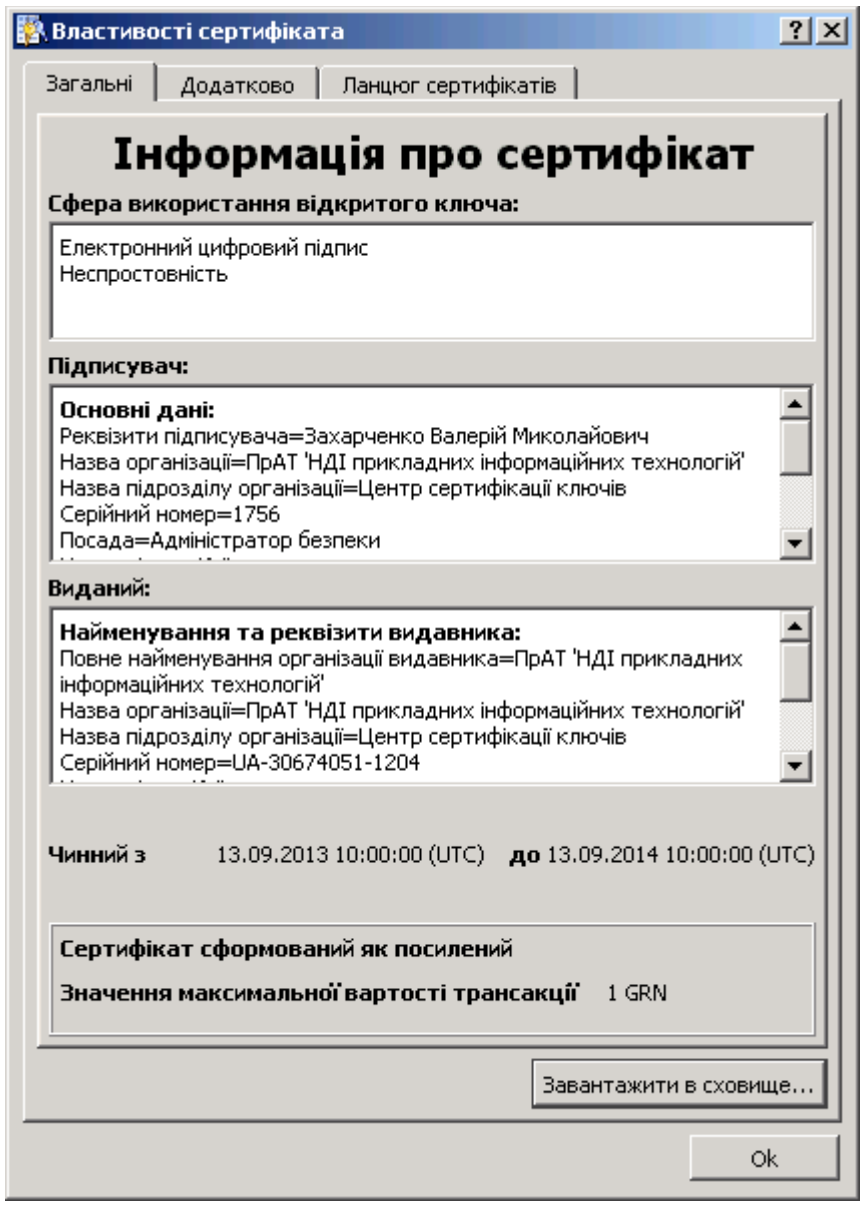
В меню “Інструменти” вибираємо пункт меню “Сертифікати”, відкривається вікно “Сертифікати” (мал. 3.14), де розміщені вкладки “Персональні”, “Інші”, “Сертифікати ЦСК” та “Сертифікати ЦЗО”. Для того щоб працювати в програмі “Клієнт ЦСК” потрібно завантажити сертифікати в сховища. Переходимо по черзі на кожну вкладку і імпортуємо відповідні сертифікати: персональні, сертифікат ЦСК та ЦЗО.



Мал. 3.14 Вікно “Сертифікати”.

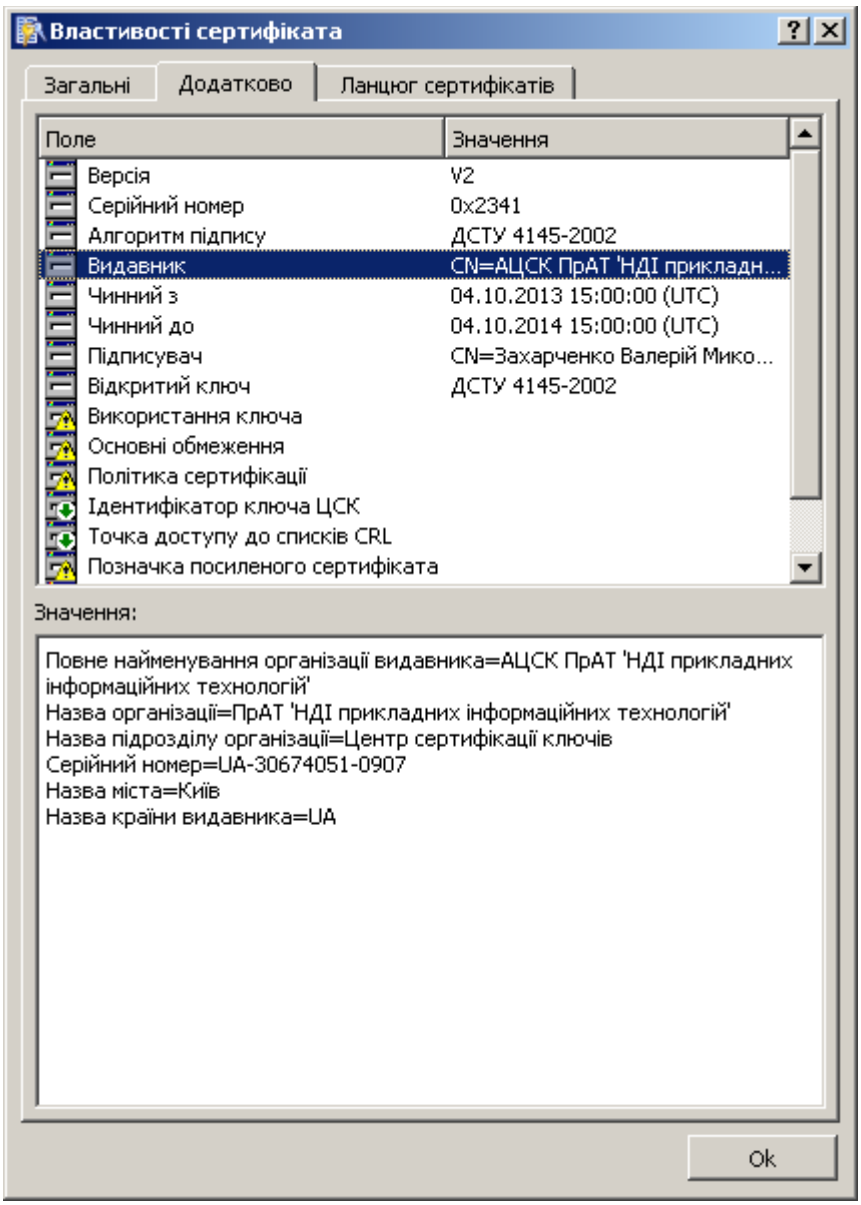
Виділивши курсором сертифікат, який був раніше імпортований, за допомогою відповідних кнопок можливо експортувати зі сховища, видалити або перемістити в інший розділ сховища.

Щоб переглянути дані, які містить сертифікат, натисніть кнопку “Показати”, відкривається вікно “Властивості сертифіката” (мал. 3.15). У вікні міститься вкладка “Загальні”, де знаходяться дані про підписувача, сферу використання відкритого ключа, про організацію, яка видала сертифікат та терміни чинності сертифіката.



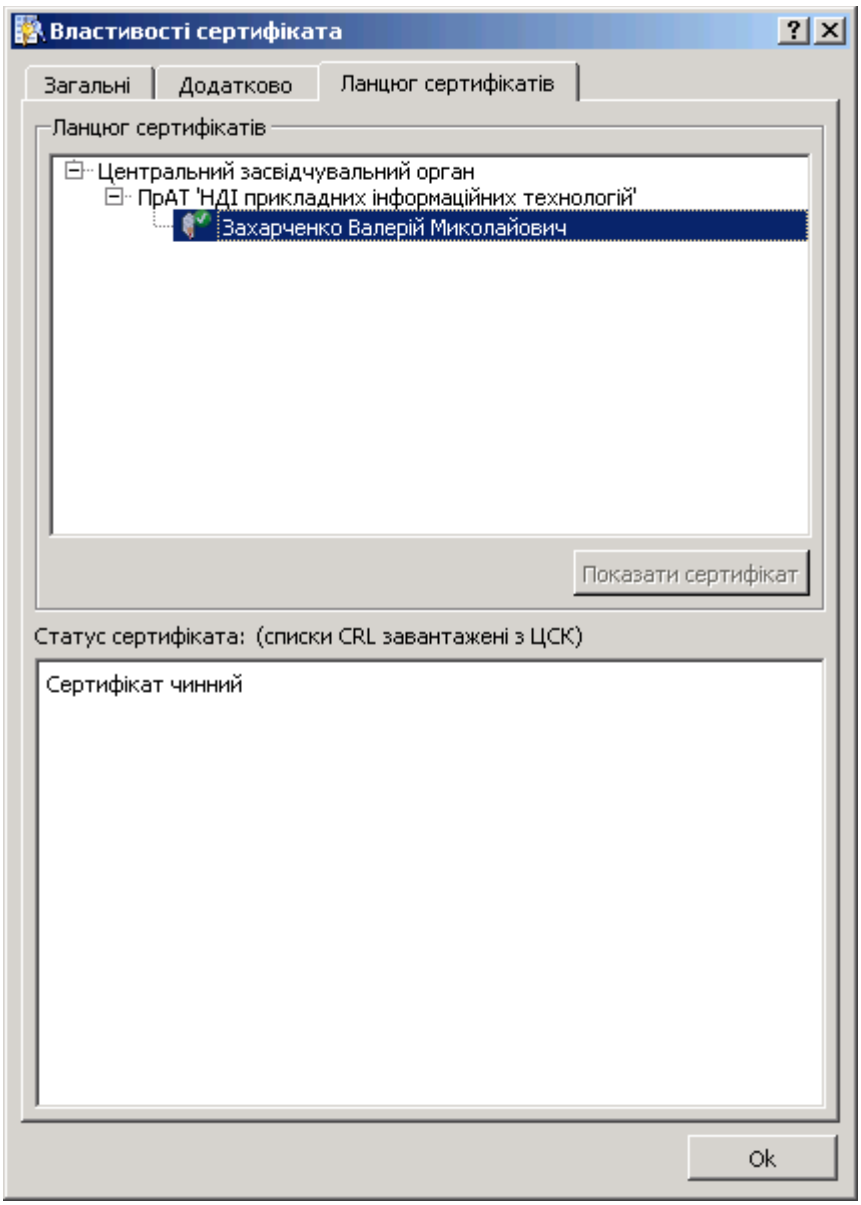
Мал. 3.15 Вікно "Властивості сертифіката".

У вкладці “Додатково” (мал. 3.16) містяться додаткові технічні дані такі як: серійний номер, алгоритм підпису, відкритий ключ, сферу використання ключа, основні обмеження, ідентифікатор ключа ЦСК, точка доступу до списків CRL та інші.



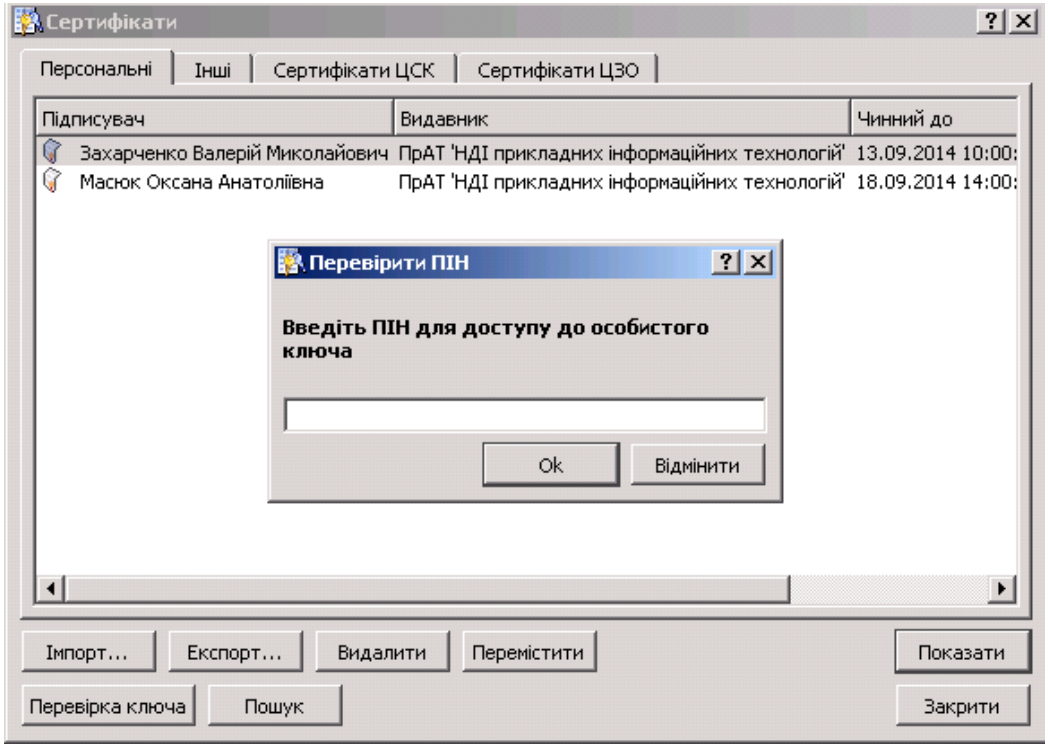
Мал. 3.16 Вкладка “Додатково” вікна “Властивості сертифіката”.

У вкладці “Ланцюг сертифікатів” (мал.. 3.17) можна подивитися сертифікат підписувача, сертифікат організації видавника та центрального засвідчувального органу, а також перевірити статус цих сертифікатів.



Мал.. 3.17 Вкладка “Ланцюг сертифікатів” вікна “Властивості сертифіката”.

У вікні “Сертифікати” можливо здійснити перевірку відповідності відкритого ключа у обраному сертифікаті особистому ключу з картки, натиснувши кнопку “Перевірка ключа” та ввівши ПІН код у вікні, яке відкриється (мал.. 3.18).

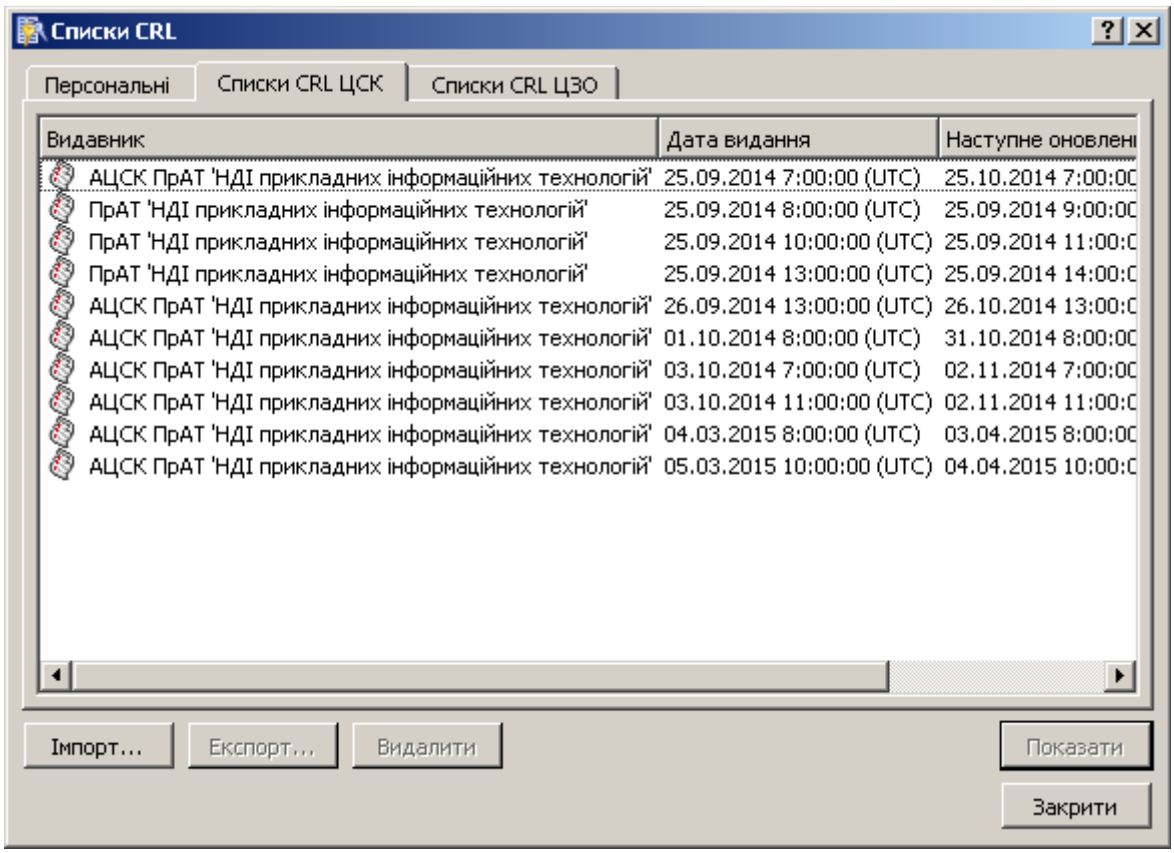


Мал. 3.18 Перевірка відповідності ключів.

У вікні “Сертифікати” є можливість знайти сертифікати, які розміщені у сховищі на інформаційному ресурсі ЦСК, натиснувши кнопку “Пошук”. Детальніше дивіться розділ “Пошук сертифікатів” даної інструкції.

3.8. Сховище списків відкликаних сертифікатів

В меню “Інструменти” обираєте пункт меню “Списки CRL”, після чого відкриється вікно “Списки CRL” (мал. 3.19) в якому можна переглянути списки відкликаних сертифікатів ЦСК, ЦЗО та персональні. Також можна експортувати, видаляти та імпортувати нові CRL, використовуючи відповідні кнопки.



Мал. 3.19 Вікно “Списки CRL”.

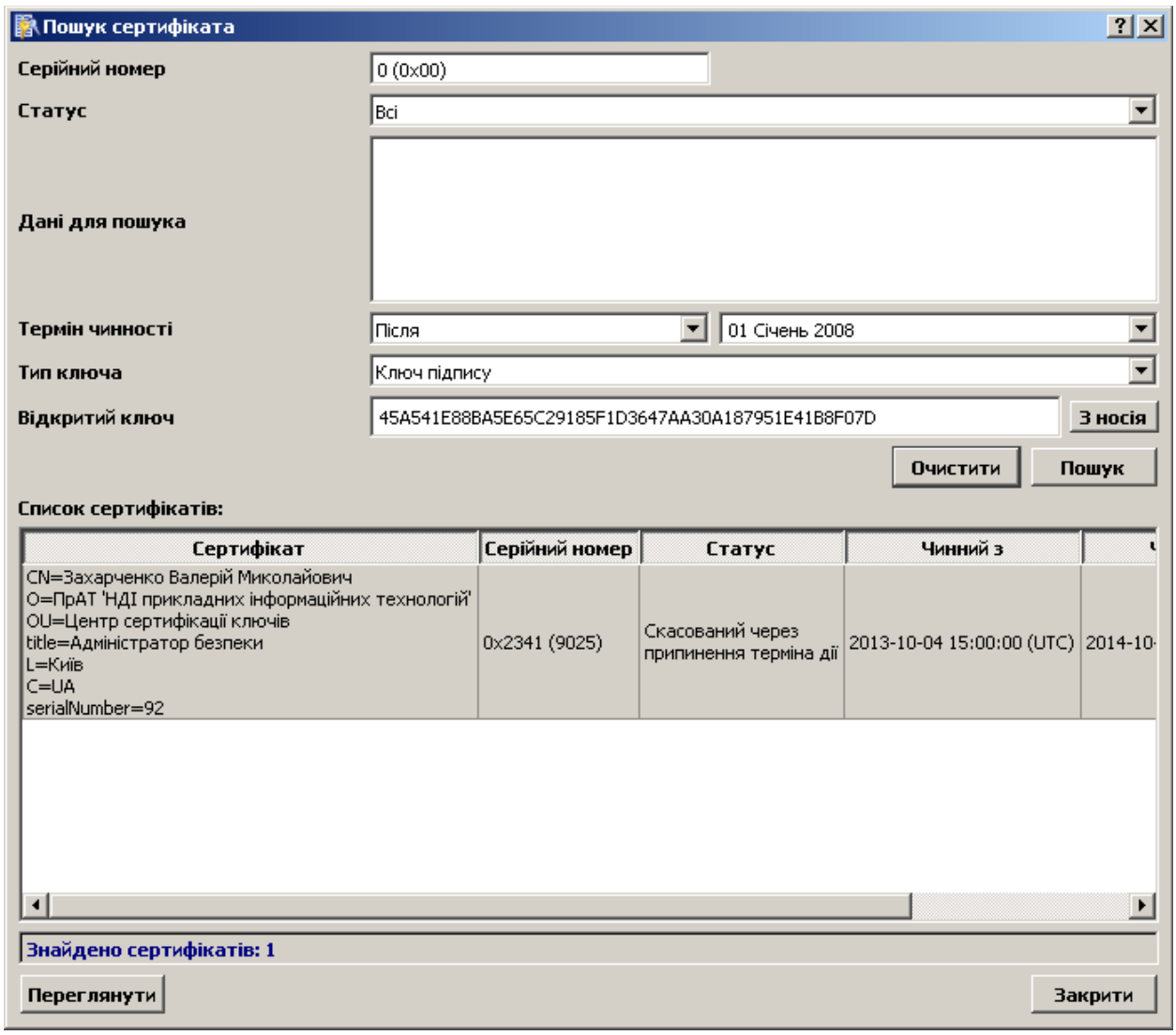
3.9. Пошук сертифікатів

Знайти сертифікати на інформаційному ресурсі ЦСК можна скориставшись меню “Інструменти”, перейшовши на розділ “Пошук сертифіката”. У вікні “Пошук сертифікатів” (мал. 3.20), що з’явиться, пошук сертифікатів можна здійснити за одним або кількома параметрами:

- за номером сертифіката (поле “Серійний номер”);
- за статусом, вибравши необхідний в списку “Статус”;
- прізвищем власника сертифіката або назвою організації введіть у полі “Дані для пошуку”;
- за терміном чинності, вказавши часовий діапазон терміну чинності у відповідних полях;
- за особистим ключем записаному на картку. Необхідно вставити картку і натиснути кнопку “З носія” (ліворуч від поля “Відкритий ключ”).

Для очистки параметрів пошуку необхідно натиснути кнопку “Очистити”. Якщо не встановити параметрів пошуку сертифікатів, то буде відображено повний перелік сертифікатів.

Для початку пошук потрібно натиснути кнопку “Пошук”.



Мал. 3.20 Вікно “Пошук сертифіката”.

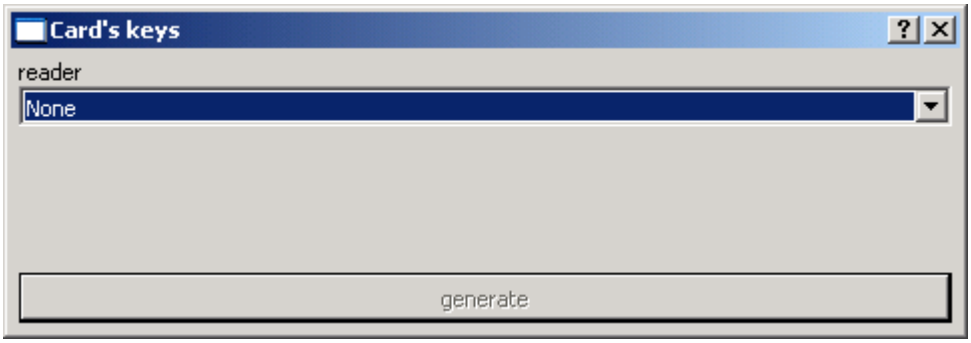
Результат пошуку відображається у формі “Список сертифікатів”. Виділивши курсором сертифікат та натиснувши на кнопку “Переглянути”, можна подивитися дані сертифіката і потім завантажити сертифікат в сховище за допомогою кнопки “Завантажити в сховище…” у вікні “Властивості сертифіката”.

4. Повторне отримання сертифіката

4.1. Генерація ключів на картці

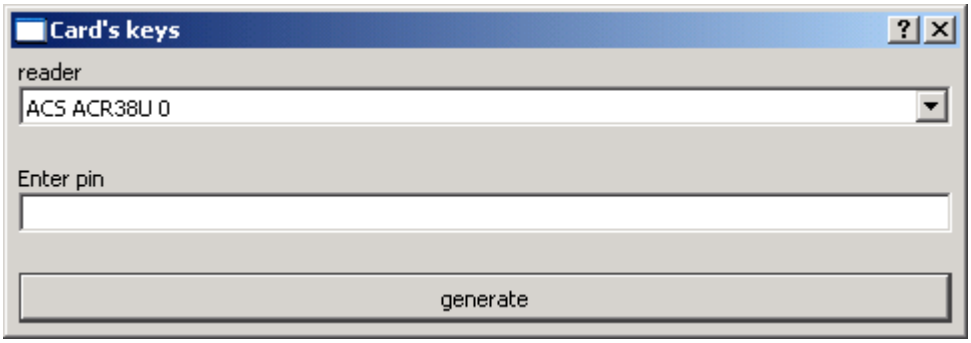
Увага! При генерації нових ключів попередні буде знищено! Виконуйте генерацію нових ключів виключно у випадках, якщо точно знаєте, що робите!

Для генерації ключа електронного цифрового підпису на картці (захищеному носії ключової інформації) необхідно в каталозі, в якому встановлена програма “Клієнт ЦСК”, запустити файл “CardsInitKey.exe”. Відкриється головне вікно програми для генерації ключів (мал. 4.1).



Мал. 4.1 Головне вікно програми генерації ключів

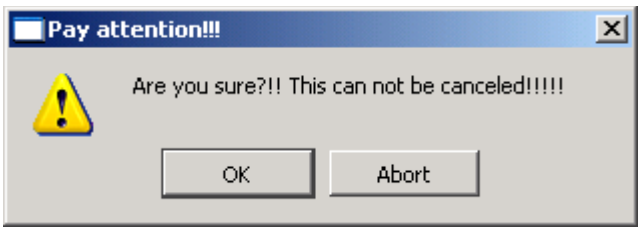
Вставте картку, на якій будете генерувати ключ, до рідера і оберіть його в полі «reader» програми. З’явиться поле для вводу коду доступу до носія (PIN) (мал. 4.2.). Вводите PIN, який встановлено до носія, та натискаєте кнопку «generate».



Мал. 4.2 Вікно із полем для вводу коду доступу до носія.

Далі зявиться діалогове вікна, в якому необхідно підтвердити, що бажаєте згенерувати нові ключі та Ви погоджуєтесь, що після знищення старих ключів із картки, не зможете зашифрувати/розшифрувати/підписати усі старі повідомлення (мал. 4.3). Якщо не бажаєте продовжувати дії натискаєте «Abort». Якщо бажаєте продовжити - натискаєте «Ок». Після чого зявляється вікно, що повідомляє, що подальші дії є безповоротними (мал. 4.4). Якщо не бажаєте перегенеровувати ключі – натискаєте «Abort». Якщо бажаєте згенерувати ключі – натискаєте «Ок».

Мал. 4.3 Вікно підтвердження генерації нових та затиранням старих ключів.



Мал. 4.4 Вікно підтвердження дій.

Після вдалої генерації ключів з'являється інформаційне вікно з відповідним повідомленням (мал. 4.5). Натисніть кнопку «Ок» для закриття вікна.

Мал. 4.5 Вікно вдалого завершення генерації ключів.

4.2. Створення запиту на отримання сертифіката

Після генерації ключів необхідно сформувати та перевірити запит на отримання сертифікати, для чого слідуйте вказівкам пункту 3.4. "Запит на отримання сертифіката" даної інструкції. Готовий запит передаєте в ЦСК з відповідними документами для формування на їх основі сертифіката.

4.3. Завантаження сертифікатів до сховища

Нові сертифікати потрібно імпортувати до сховища сертифікатів програми "Клієнт ЦСК", для чого слідуйте інструкціям розділу 2.1. "Завантаження сертифікатів".