Навчально-науковий інститут інформаційних технологій
Харківський національний економічний університет
імені Семена Кузнеця

Звіт
З Виконання лабораторної роботи №4
за дисципліною: “ Безпека банківських систем ”
на тему: “ДОСЛІДЖЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ У СПРОЩЕНИХ EDI-СИСТЕМАХ”

Виконав: студент кафедри
Кібербезпеки та інформаційних
технологій
4 курсу, спец. Кібербезпека,
групи 6.04.125.010.21.2
Бойко Вадим Віталійович
Перевірив:
Лимаренко Вячеслав Володимирович

ХНЕУ ім. С. Кузнеця
2024

Мета: ознайомитися з системою EDI (Electronic Data Interchange) та методами захисту інформації в даній системі. Отримати практичні навички з роботи із системою GNU Privacy Guard із використанням оболонки Kleopatra

Завдання:

1. Завантажити та встановити програмне забезпечення GNU Privacy Guard із використанням оболонки Kleopatra.
2. Повторити приклади з Розділу 2.
3. Протестувати програму на роботу з помилковими ключами.
4. Перевірити можливість прочитати файл без використання системи дешифрування.

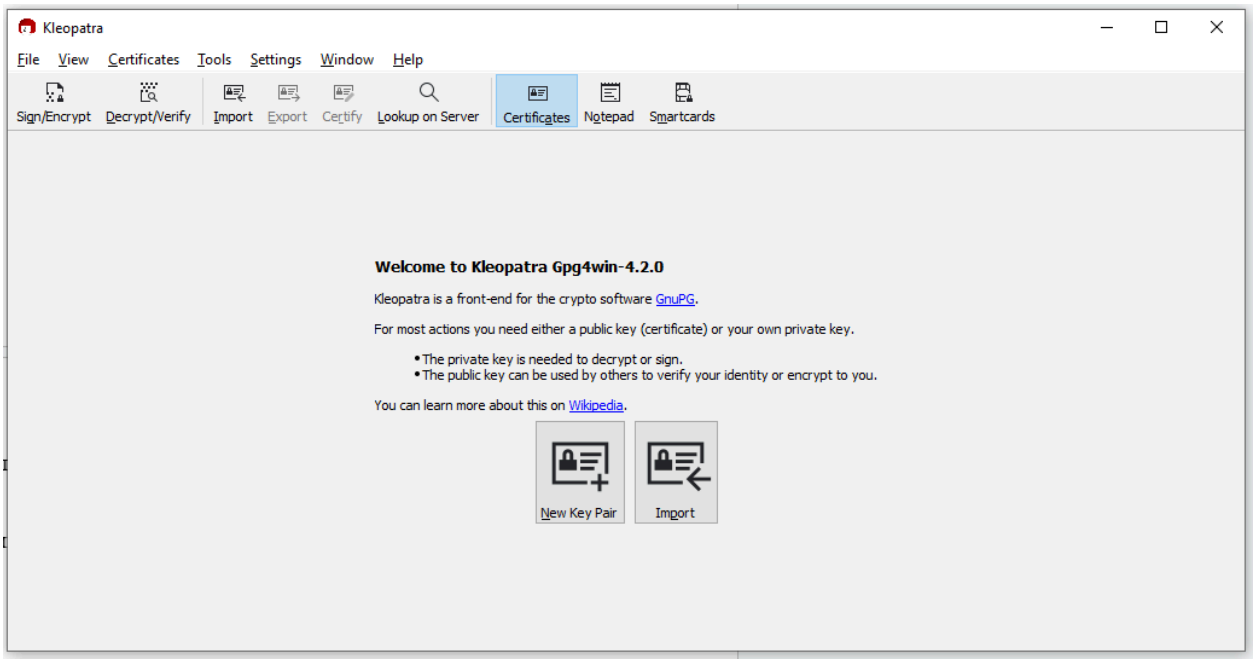
Контрольні питання:

1. Що являє собою система EDI?
2. Які типи стандартних EDI-документів ви знаєте?
3. Як використовується система EDI в банківській сфері?
4. Яке призначення програми GNU Privacy Guard?
5. Яким чином GNU Privacy Guard захищає документи?

Хід роботи:

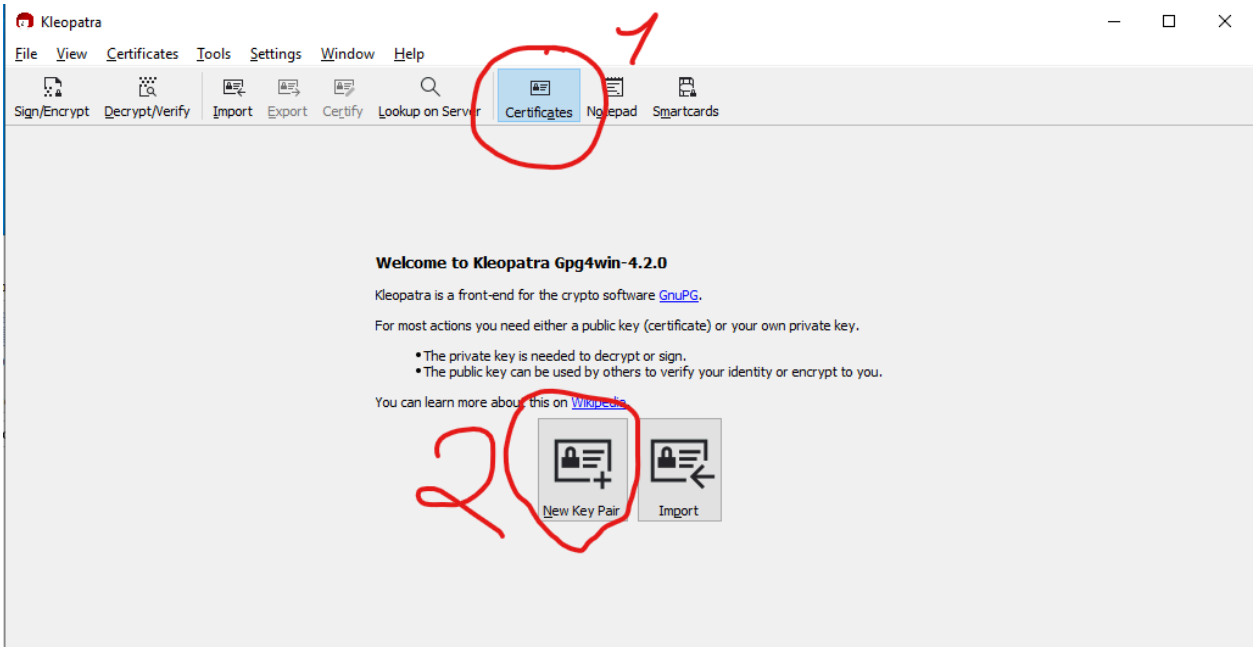
Завдання № 1

Встановив GNU Privacy Guard із використанням оболонки Kleopatra

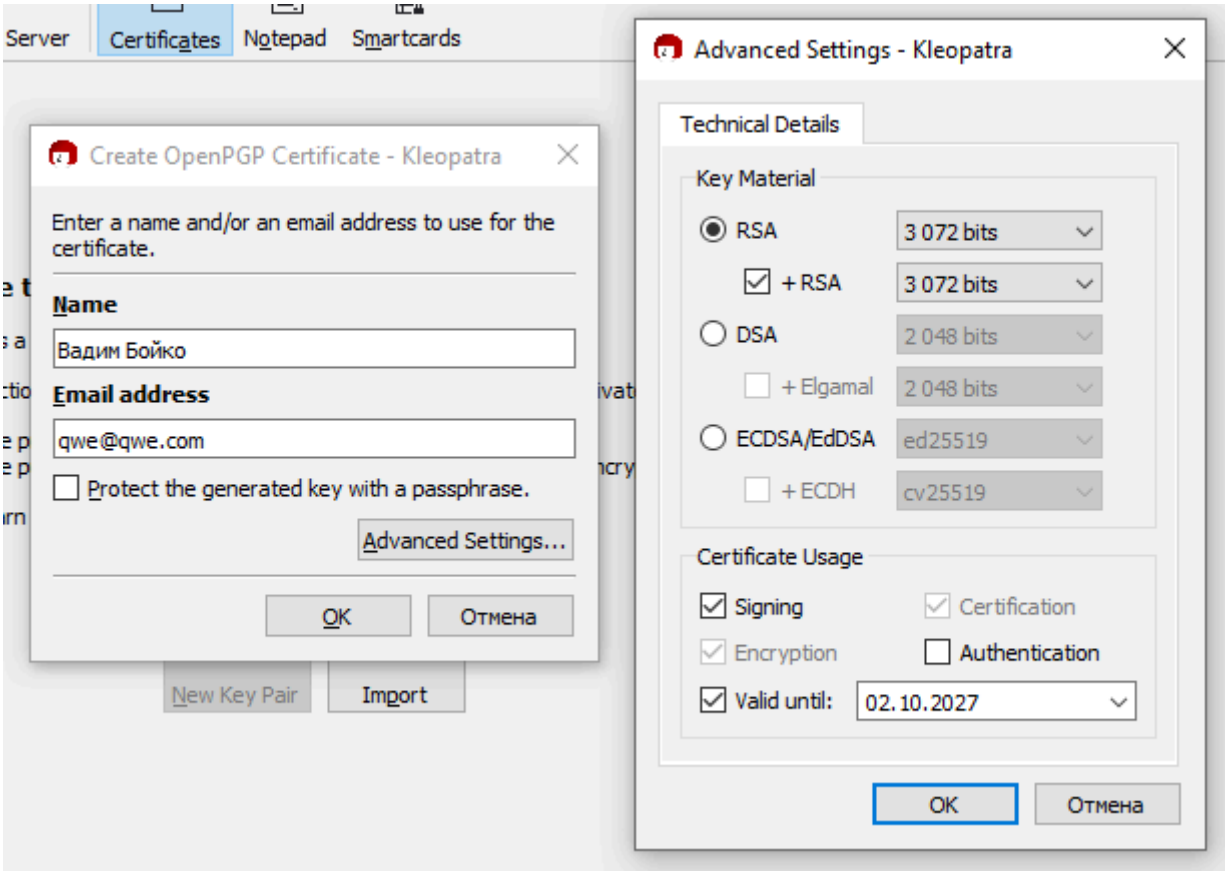


Завдання № 2

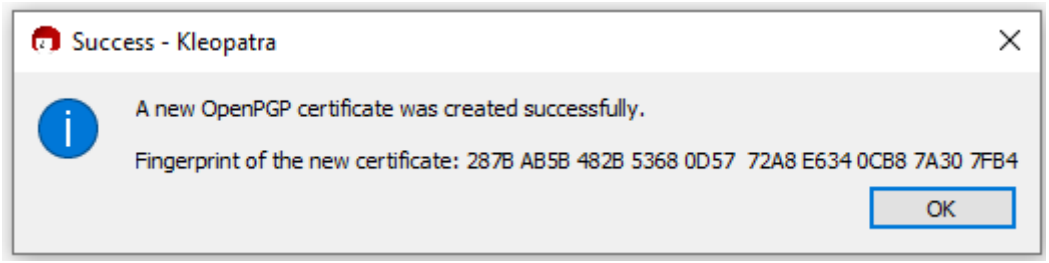
Створю пару ключів



Заповню поля для пари ключів

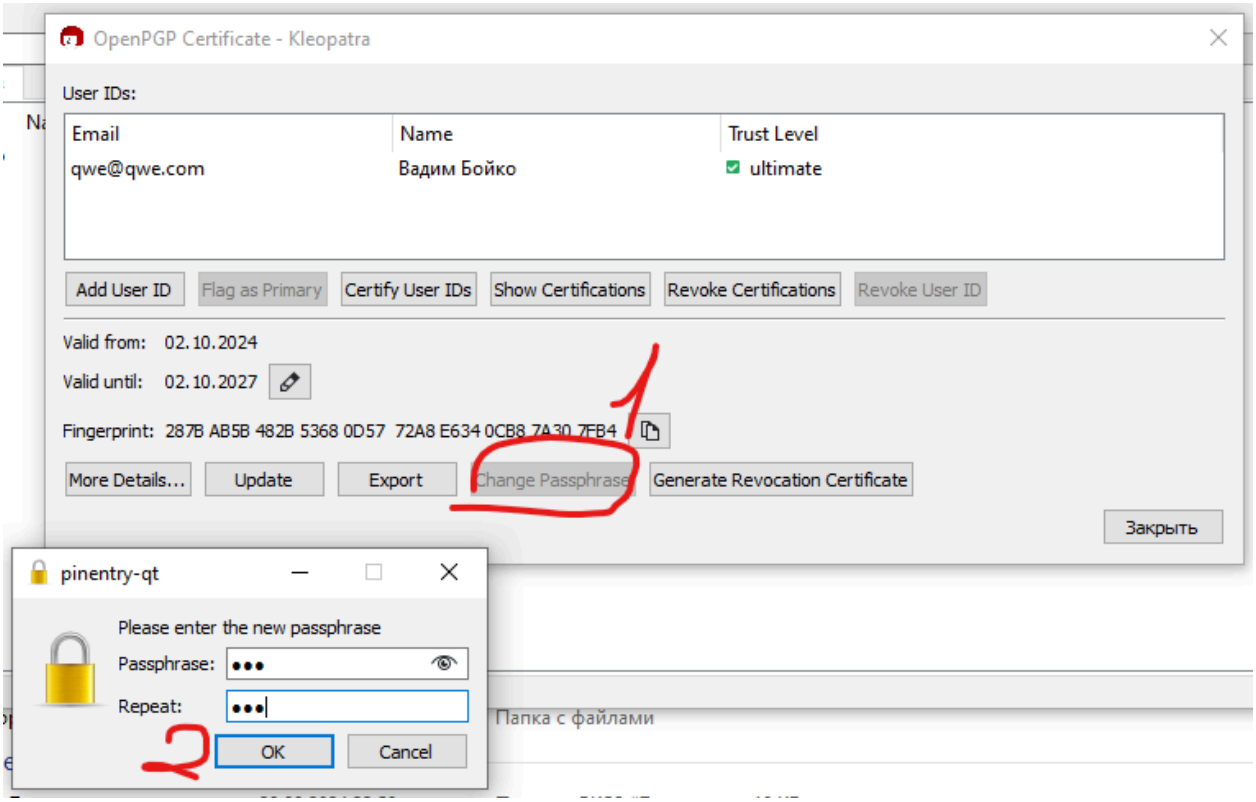


Й натискаю “Ок”



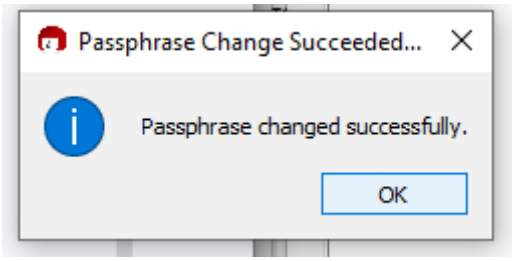
В результаті сертифікат був створений

Натискаю на “Change Passphrase” та задаю ключ

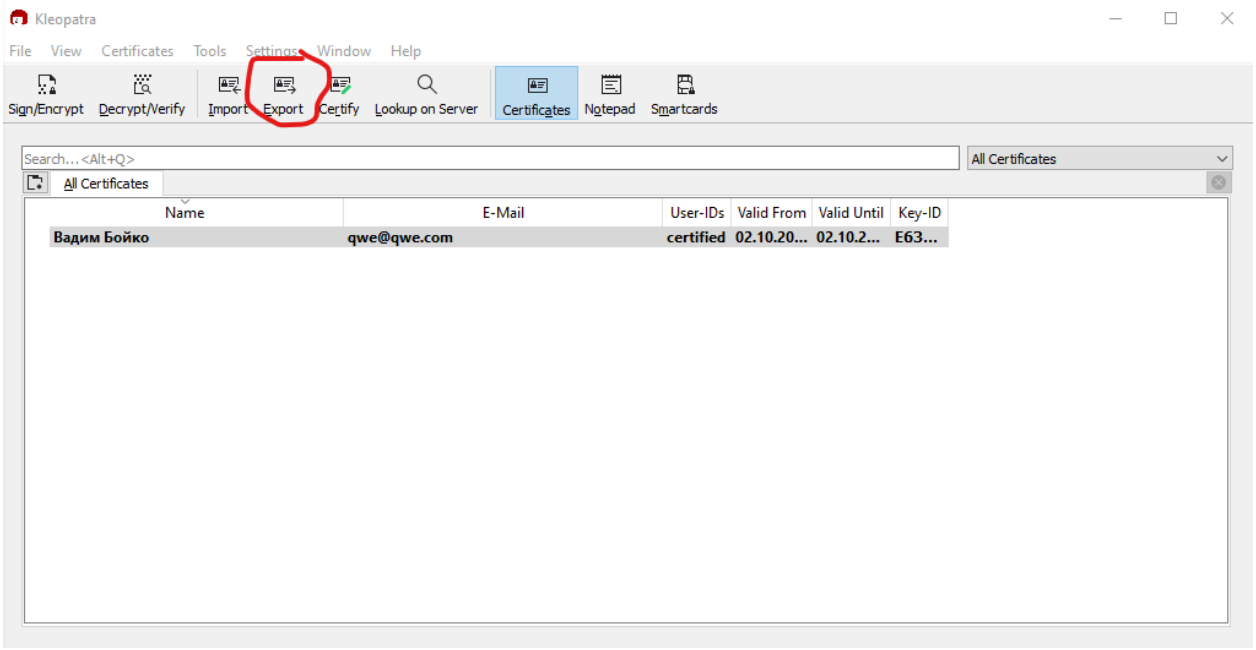


Та натискаю “Ок”

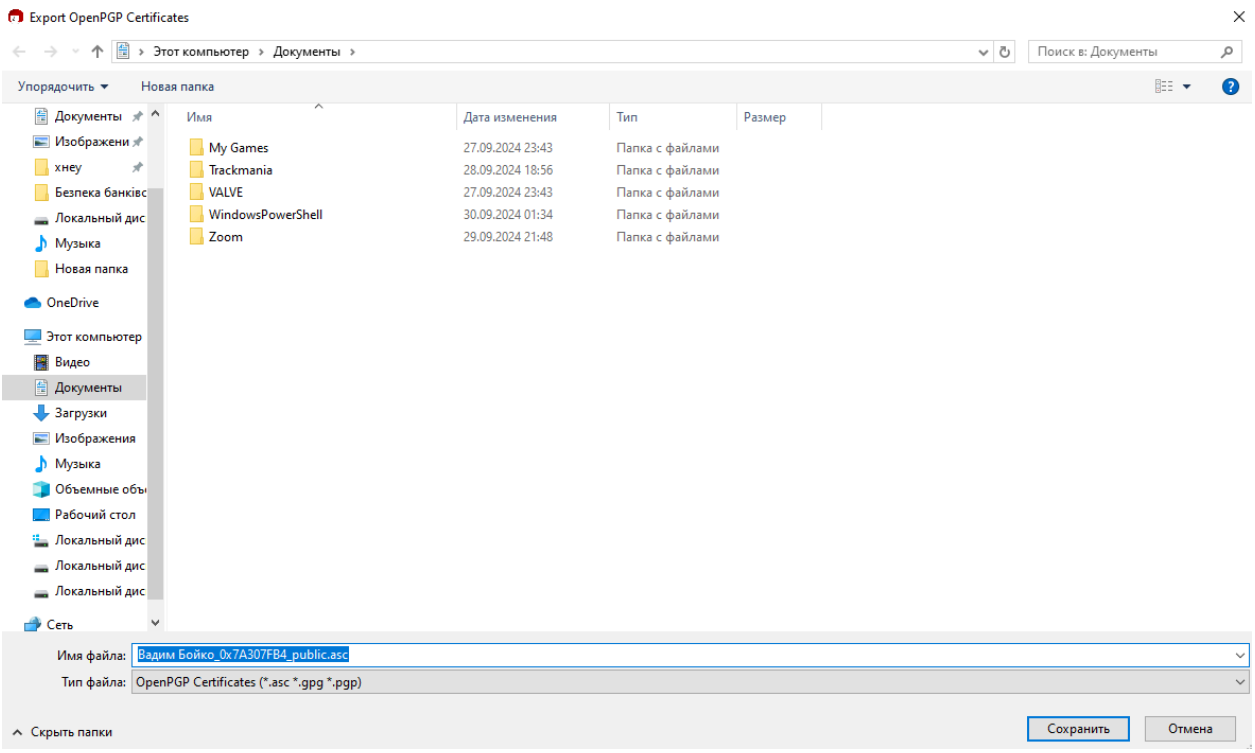
В результаті пароль було змінено



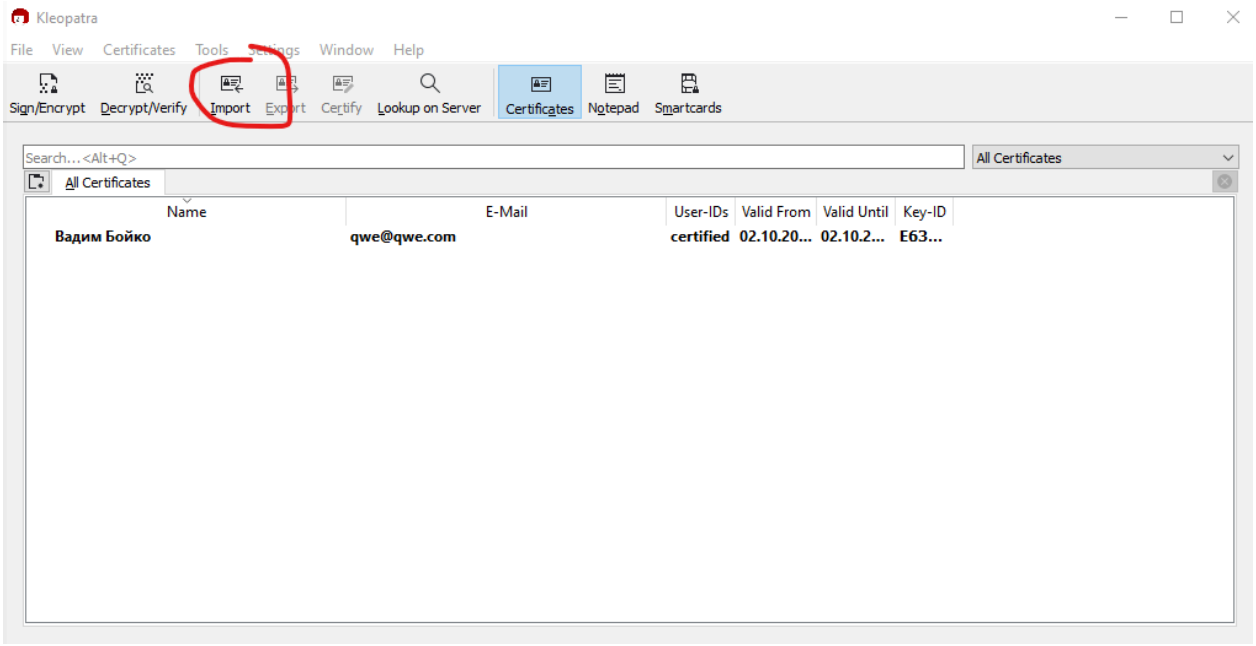
Тепер зроблю Експорт ключіів, для цього натисну на “Export”



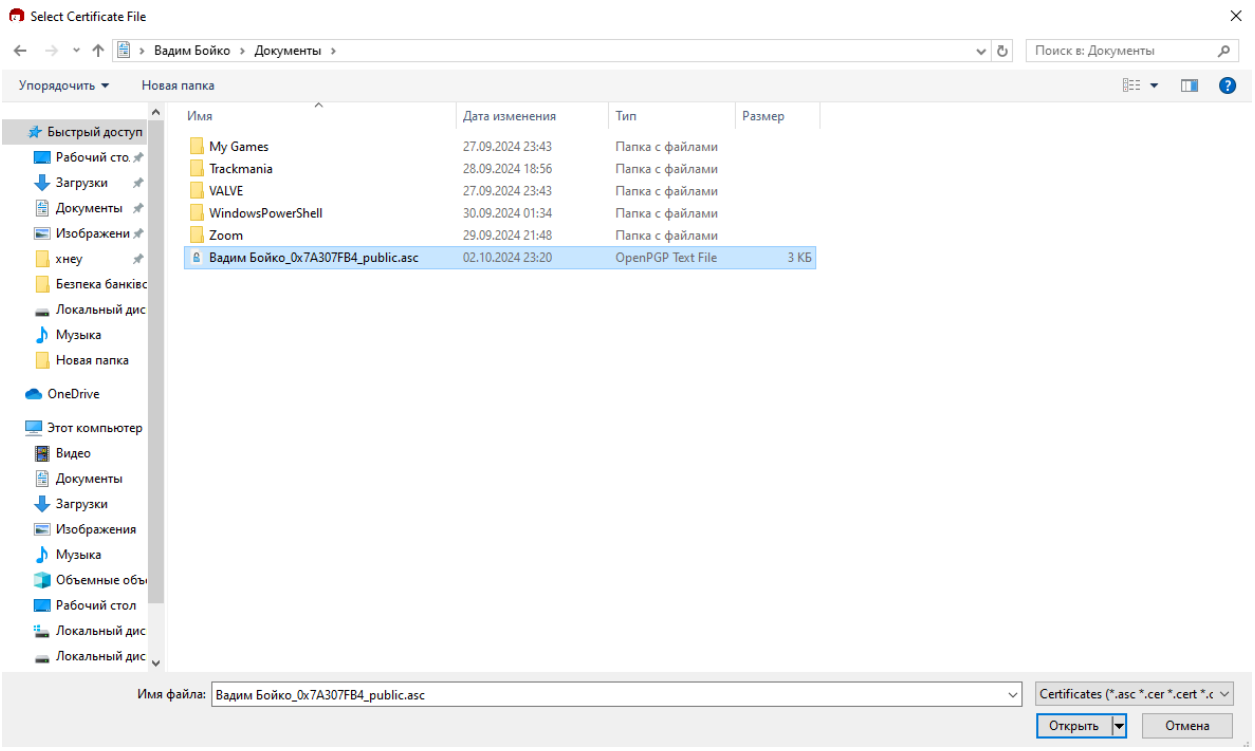
Й збережу ключ



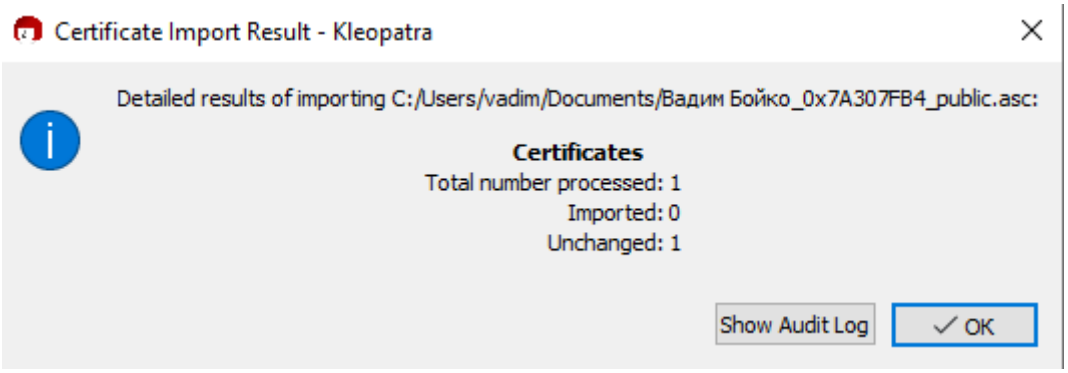
Наступном кроком зроблю імпорт, натиснувши на “Import”



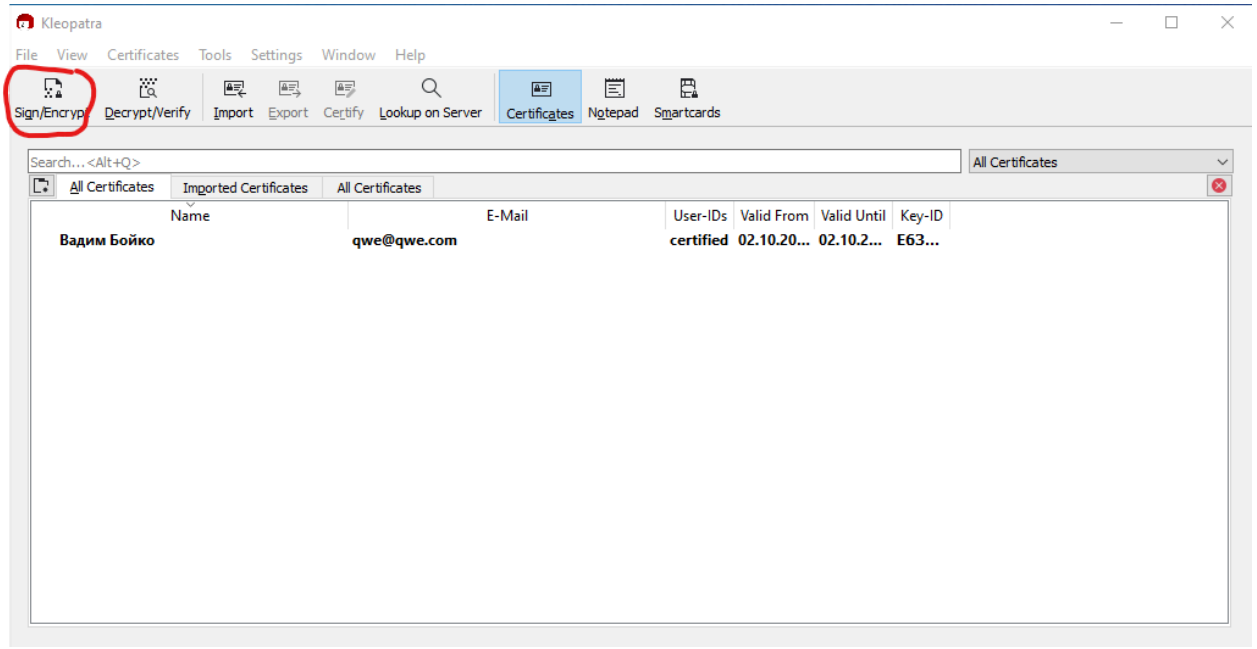
Й оберу свій ключ



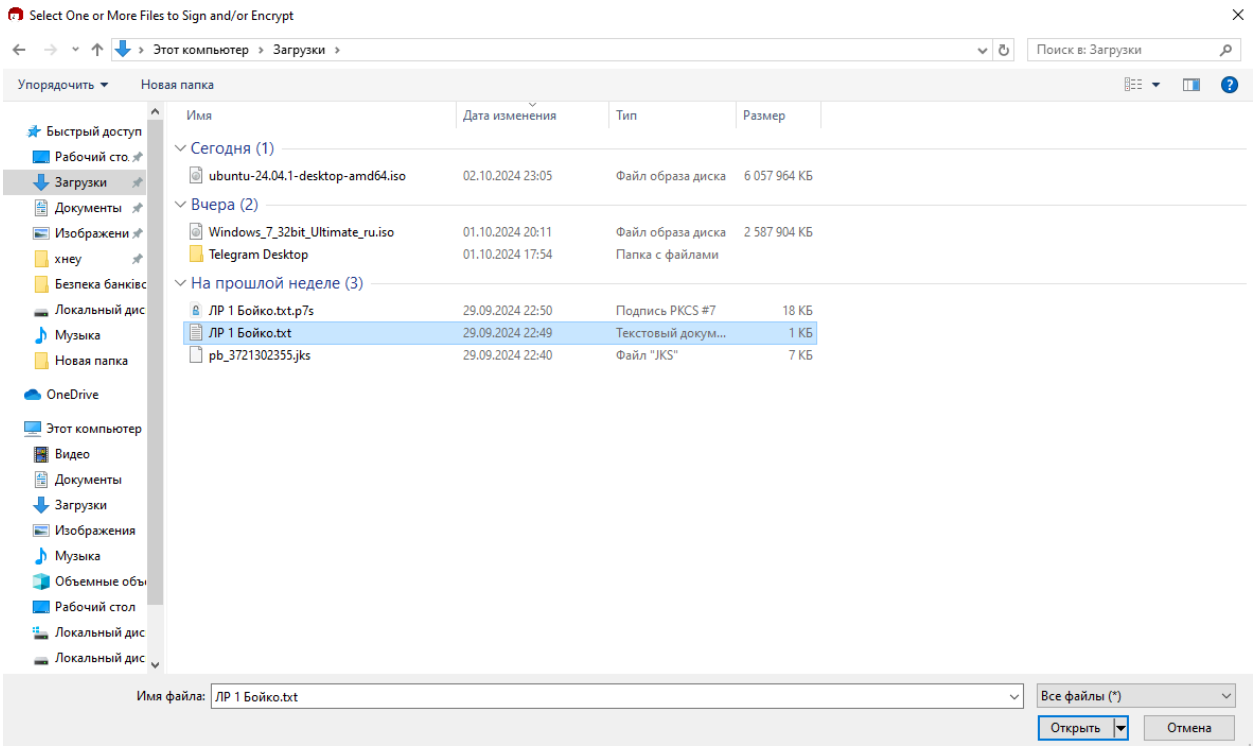
В рнзультаті сертифікат було імпортовано



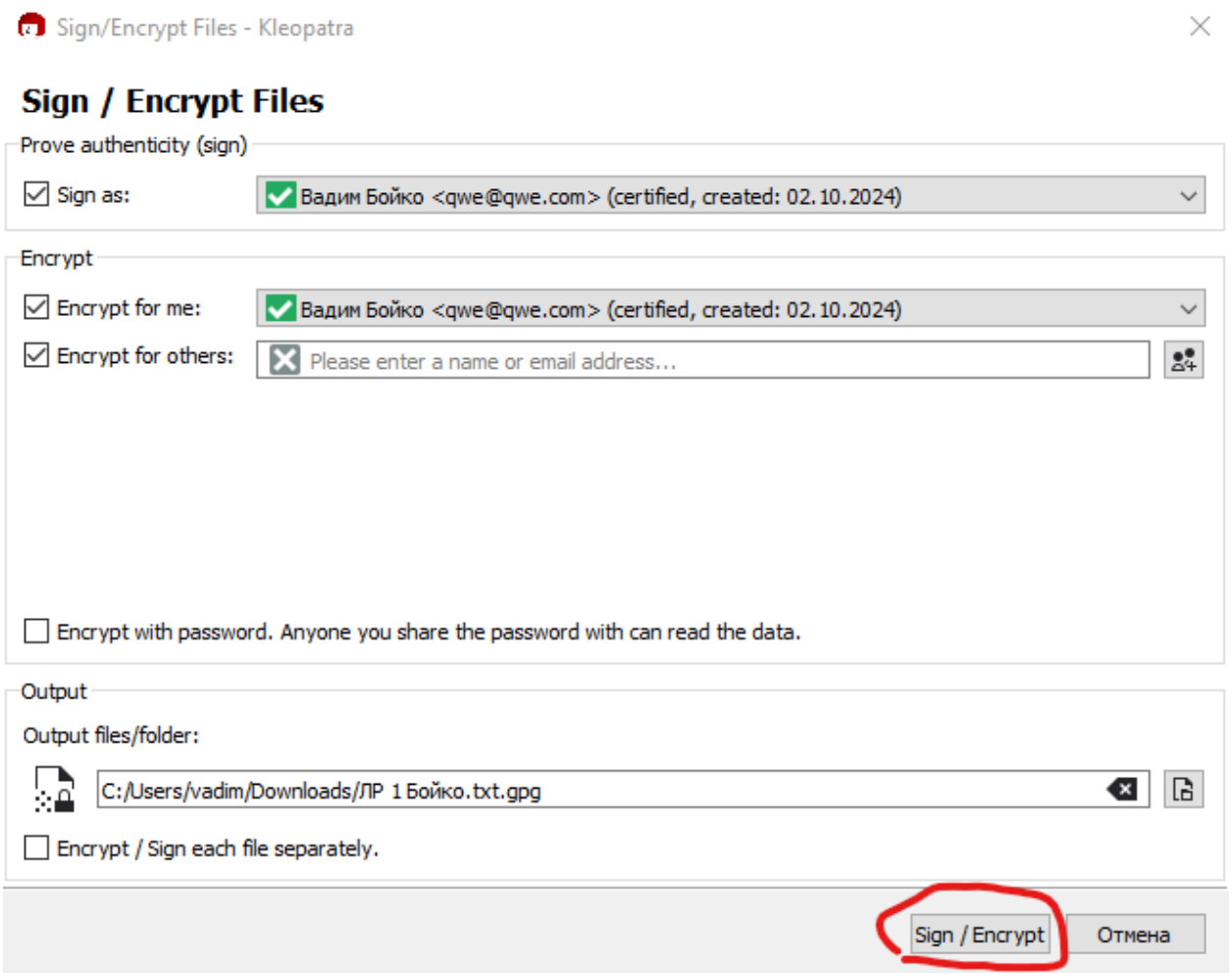
Тепер підпигу файл, для цього натисну на “Sign\Encrypt”



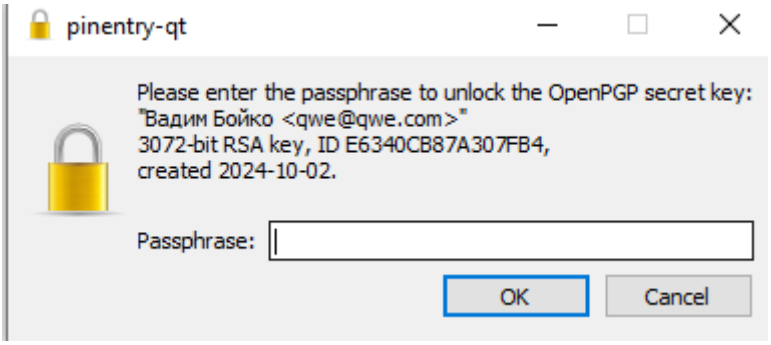
Й оберу файл



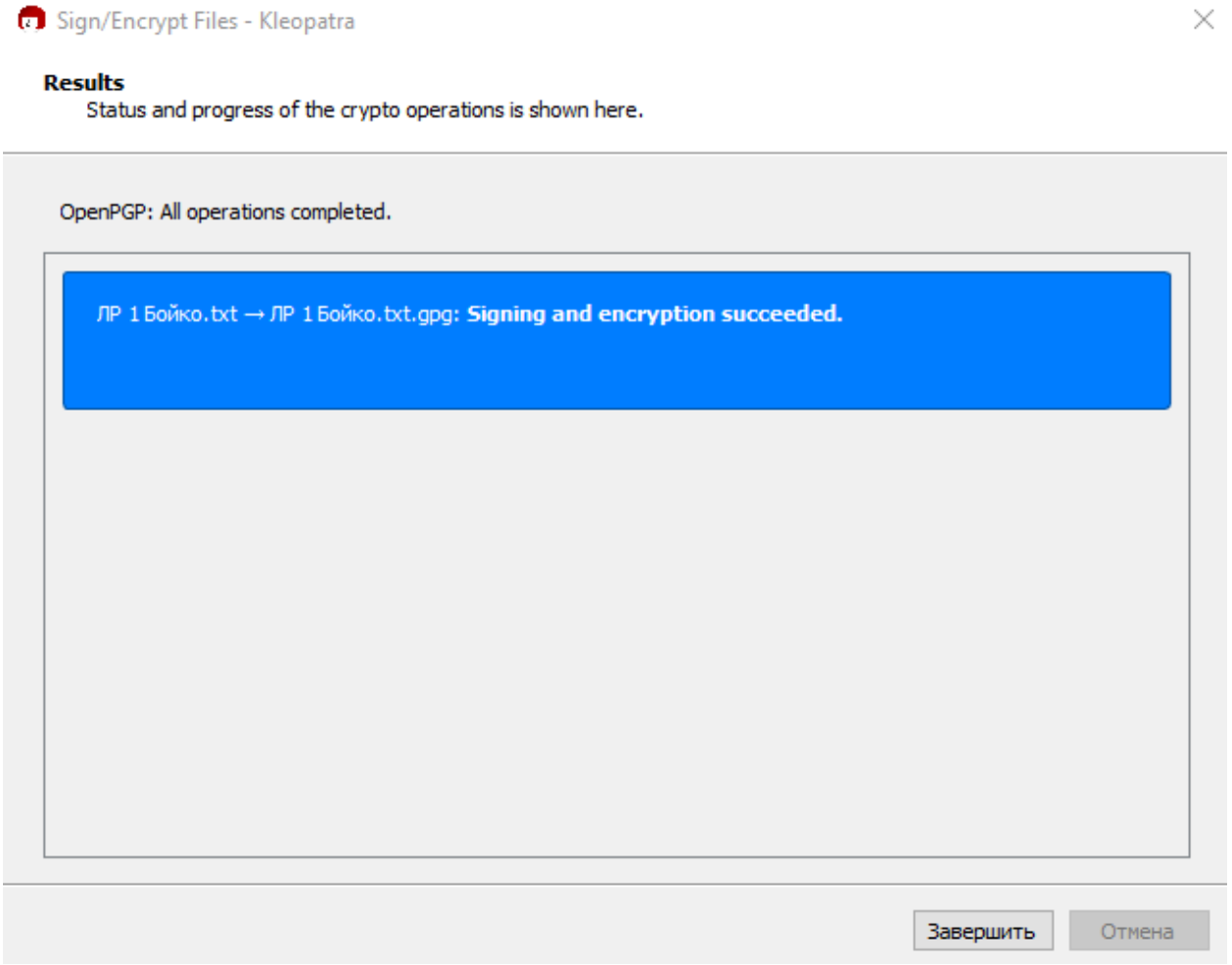
Й натисну “Sygn\Encrypt”



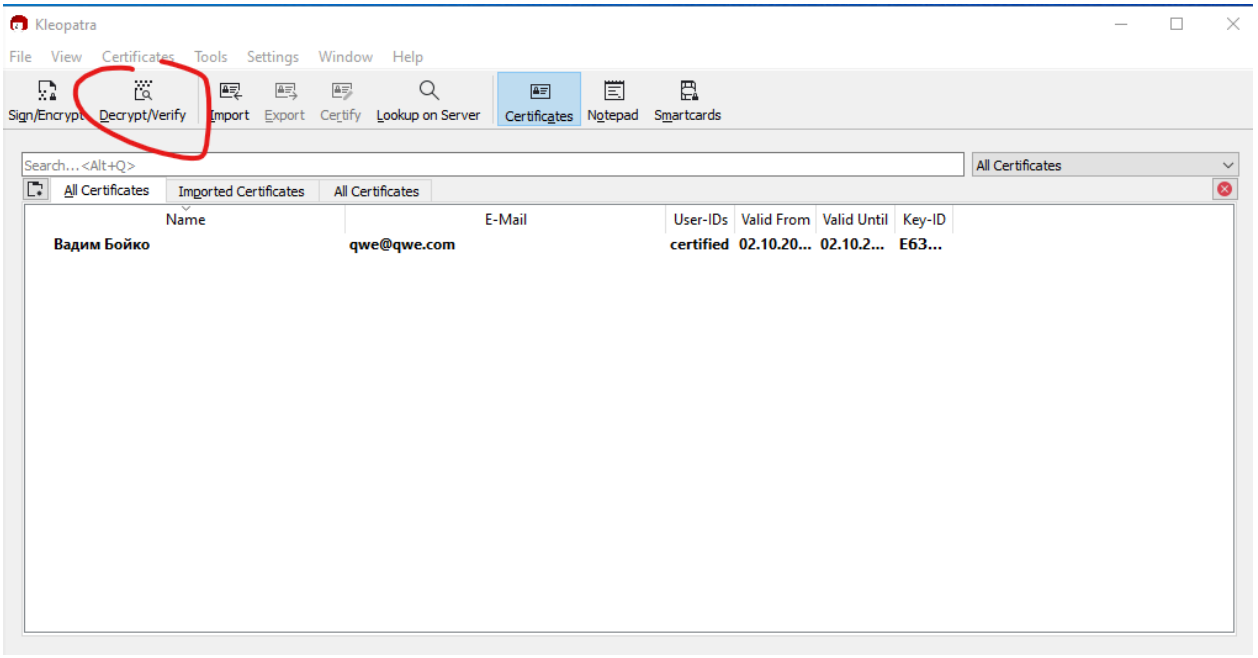
Й введу пароль



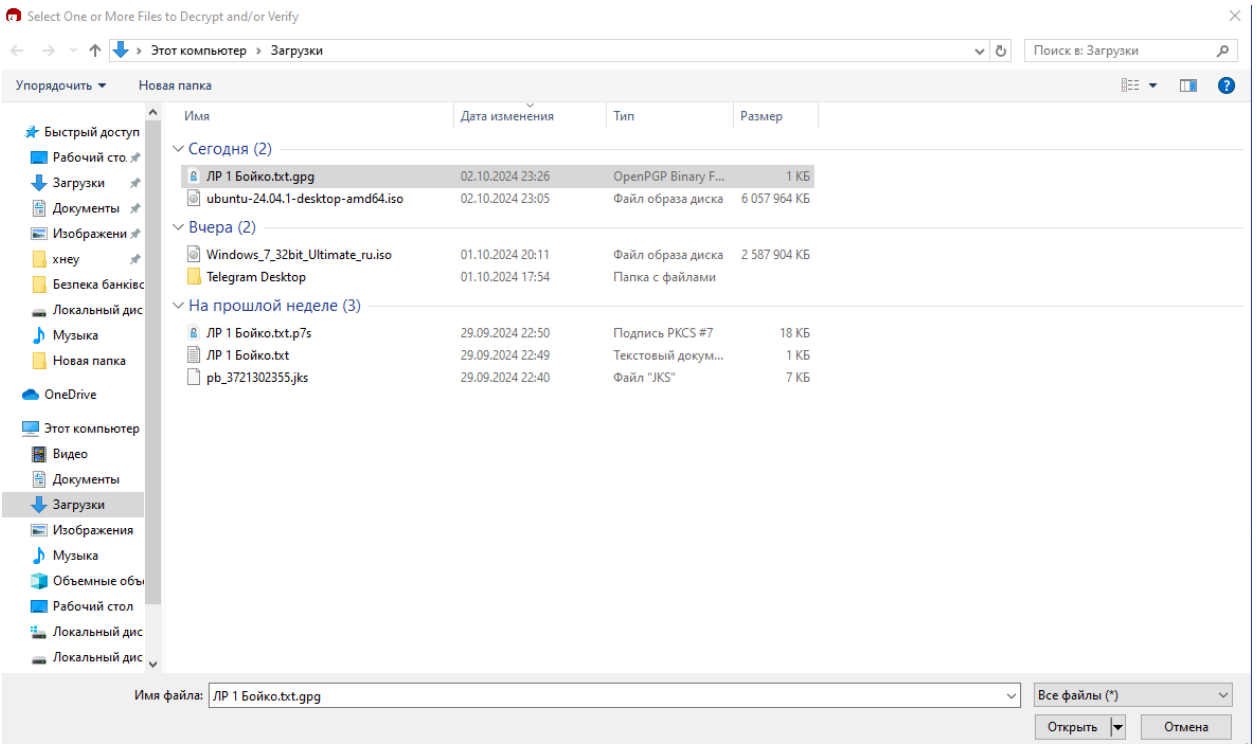
Й отримаю повідомлення, що файли були підписані



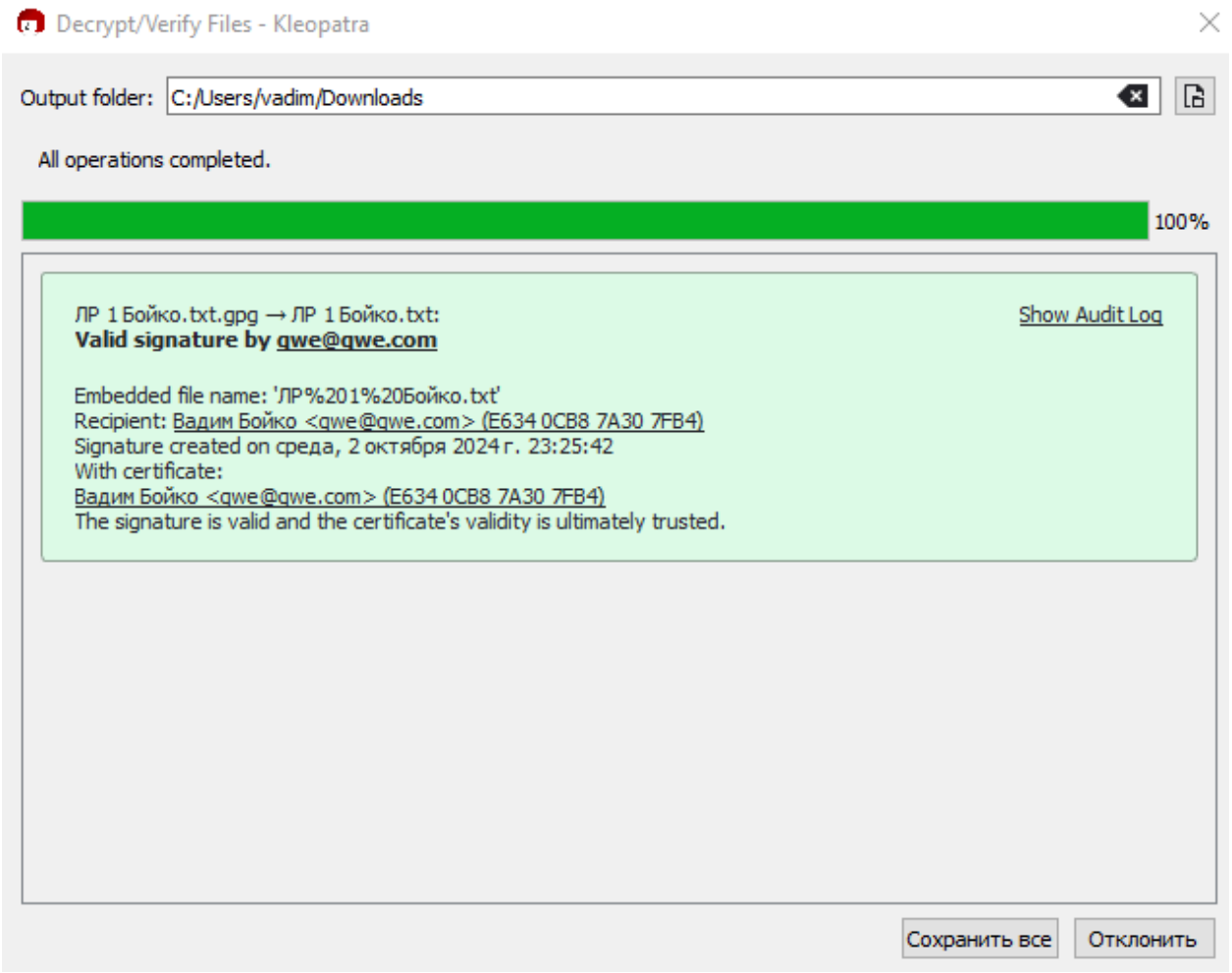
Тепер розшифрую файл, для цьогонатисну на “Decrypt/Verify”



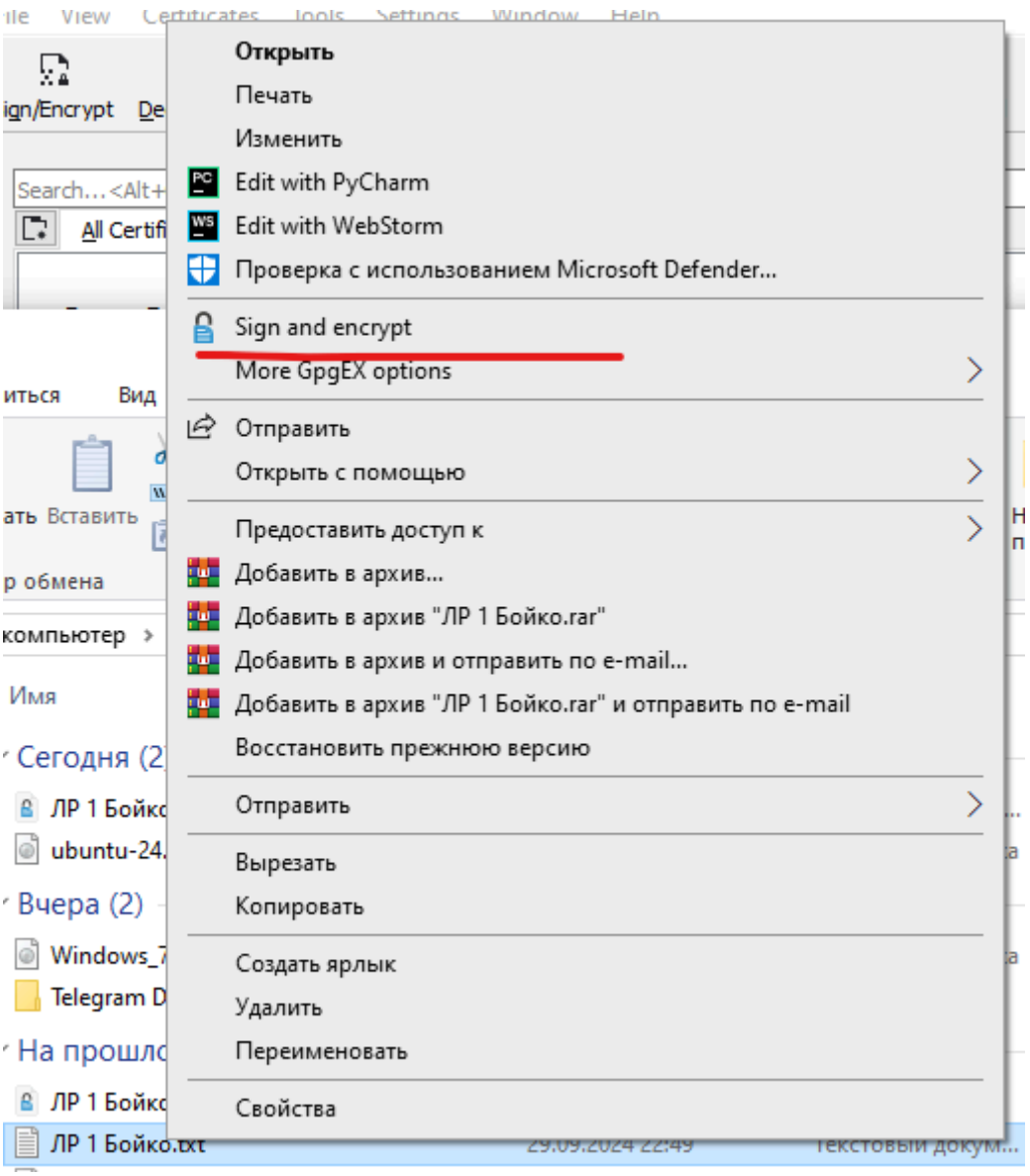
Насутпним крококм відкрию підписаний файл



Й отримаю повідомлення, що підписано



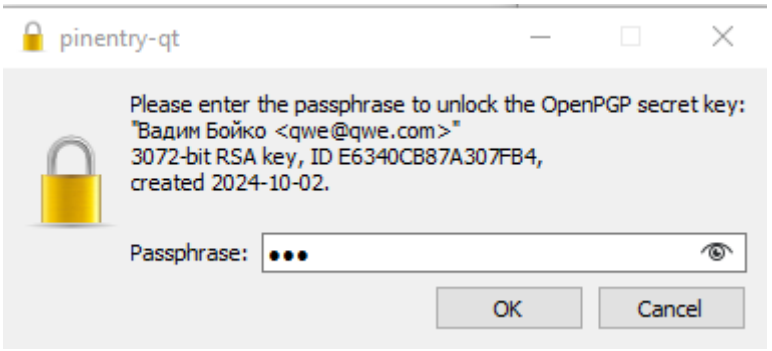
Також можна підписати файл через праву кнопку миші



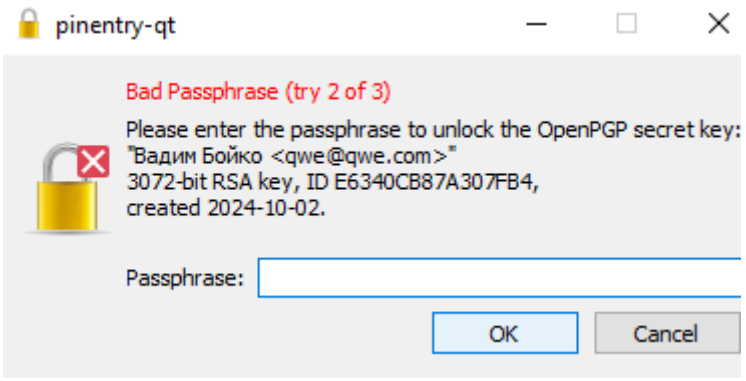
Після чого можна обрати сертифікат, і це те саме, що підписувати через програму

Завдання №3

Пробую підписати не валідним паролем



В результаті отримаю помилку



Завдання №4

Переглянути файли, без дешифрування не має можливості, оскільки вони зашифровані

Відповіді на контрольні запитання:

1. Що являє собою система EDI?

   EDI (Electronic Data Interchange) – це система електронного обміну структурованими даними між різними організаціями. Вона дозволяє автоматизувати обмін комерційною інформацією, такою як замовлення, інвойси, транспортні документи тощо. Замість того, щоб вручну вводити дані з паперових документів, компанії можуть обмінюватися ними в електронному вигляді, що значно прискорює і спрощує бізнес-процеси.

2. Які типи стандартних EDI-документів ви знаєте?

   Існує велика кількість стандартних EDI-документів, які охоплюють різні аспекти бізнес-процесів. Деякі з найпоширеніших типів:

   a. Замовлення: Повідомлення про замовлення товарів або послуг від покупця до постачальника.
   b. Інвойси: Рахунок, який виставляється продавцем покупцю за поставлені товари або послуги.
   c. Транспортні документи: Документи, що супроводжують вантаж під час транспортування (накладна, CMR тощо).
   d. Повідомлення про відправлення: Повідомлення про відправлення товару зі складу продавця.
   e. Повідомлення про отримання: Повідомлення про отримання товару покупцем.

3. Як використовується система EDI в банківській сфері?

   В банківській сфері EDI широко використовується для автоматизації таких процесів, як:

   a. Обмін фінансовою інформацією: Передача виписок, платежів, повідомлень про зміну банківських реквізитів тощо.
   b. Інтеграція з іншими системами: З'єднання банківських систем з системами клієнтів для забезпечення безперебійного обміну даними.

c. Спрощення процесів: Автоматизація рутинних операцій, зменшення кількості помилок, пов'язаних з ручним введенням даних.
d. Підвищення безпеки: Захист конфіденційної інформації за рахунок використання шифрування та інших засобів безпеки.

4. Яке призначення програми GNU Privacy Guard?

   GNU Privacy Guard (GPG) – це безкоштовна програма для шифрування даних, цифрового підпису та автентифікації. Вона використовує алгоритми шифрування з відкритим ключем для забезпечення безпеки електронної комунікації.

5. Яким чином GNU Privacy Guard захищає документи?

   GPG захищає документи за допомогою наступних механізмів:

   a. Шифрування: GPG дозволяє шифрувати файли або повідомлення за допомогою публічного ключа одержувача. Тільки власник відповідного приватного ключа зможе розшифрувати ці дані.
   b. Цифрові підписи: GPG використовує цифрові підписи для підтвердження авторства і цілісності даних. Це означає, що одержувач може бути впевнений, що документ був створений саме тим відправником, який вказаний у підписі, і що він не був змінений під час передачі.
   c. Автентифікація: GPG може використовуватися для автентифікації користувачів в системах, що підтримують цей протокол.