Інструкція користувача

«Управління ключами сховища PKCS#12»

Зміст

1. Загальні відомості

1.1. Призначення

Інструмент «Управління ключами сховища PKCS#12» (надалі – Інструмент) призначений для:

- створення файлового сховища PKCS#12 ключів та сертифікатів;
- імпорту/експорту ключів та сертифікатів до/із сховища;
- генерації асиметричної ключовою пари із записом цієї пари до сховища, та створення запиту на сертифікат у форматі PKCS#10;
- генерації сертифікату для ключової пари, що є у сховищі, з підписанням на вибраному ключі у сховищі;
- генерації сертифікату із зовнішнього запиту PKCS#10 (файлу) з підписанням на вибраному ключі у сховищі;
- імпорт сертифікату для ключової пари чи заміна існуючого сертифікату.

1.2. Системні вимоги

Інструмент створено на мові Java як десктоп-інструмент (desktop) робочого столу, що може виконуватися у будь-якому операційному середовищі під управлінням віртуальної машини Java 1.6 та вище.

1.3. Склад Інструменту

Інструмент постачається у складі бібліотек (в папці lib) та командного файлу:

lib\
Pkcs12Tools.bat

Склад бібліотек:

ambapi.jar – бібліотека додаткових інструментів;

ambprovider.jar – криптографічний сервіс провайдер Java JCA/JCE (Java ™ Cryptography Architecture/ Java ™ Cryptography Environment);

PKCS#12.jar – інструмент «Управління ключами сховища PKCS#12».

1.4. Ліцензійні вимоги

Ліцензування є обов’язковим для використання бізнес-користувачами, тобто працівниками державних та комерційних організацій та установ.

Правильність функціонування Інструменту та його супроводження забезпечується тільки для ліцензованого Інструменту.

1.5. Реквізити розробника

ТОВ «Базис»
0304, Україна, м. Київ, вул. Платонівська 18
Тел.: +38 044 244-02-25
tech@itsway.kiev.ua

2. Опис операцій

2.1. Порядок запуску

Програма тестування виконується запуском командного файлу:

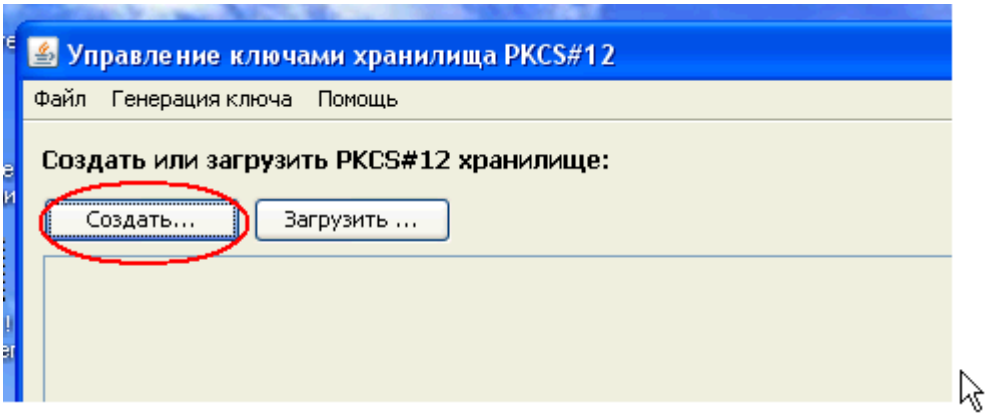
Pkcs12Tools.bat

Файл для Java JRE v1.7:
"C:\Program Files\Java\jre7\bin\java.exe" -Xmx1024m -cp "./lib/PKCS#12.jar;./lib/ambprovider.jar;./lib/ambapi.jar" com.amb.api.pkcs12.PKCS12App

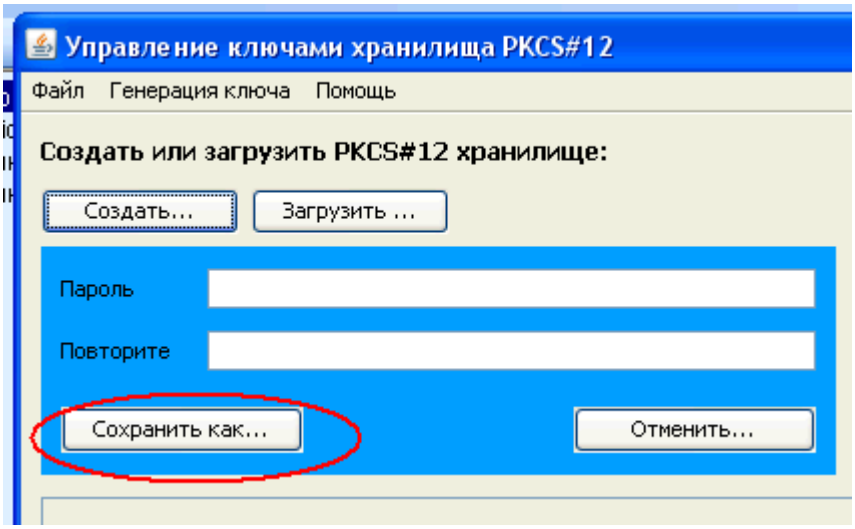
Файл для Java JRE v1.6:
"C:\Program Files\Java\jre6\bin\java.exe" -Xmx1024m -cp "./lib/PKCS#12.jar;./lib/ambprovider.jar;./lib/ambapi.jar" com.amb.api.pkcs12.PKCS12App

2.2. Створення сховища PKCS#12

В основному вікні Інструменту вибрати кнопку «Створити…»



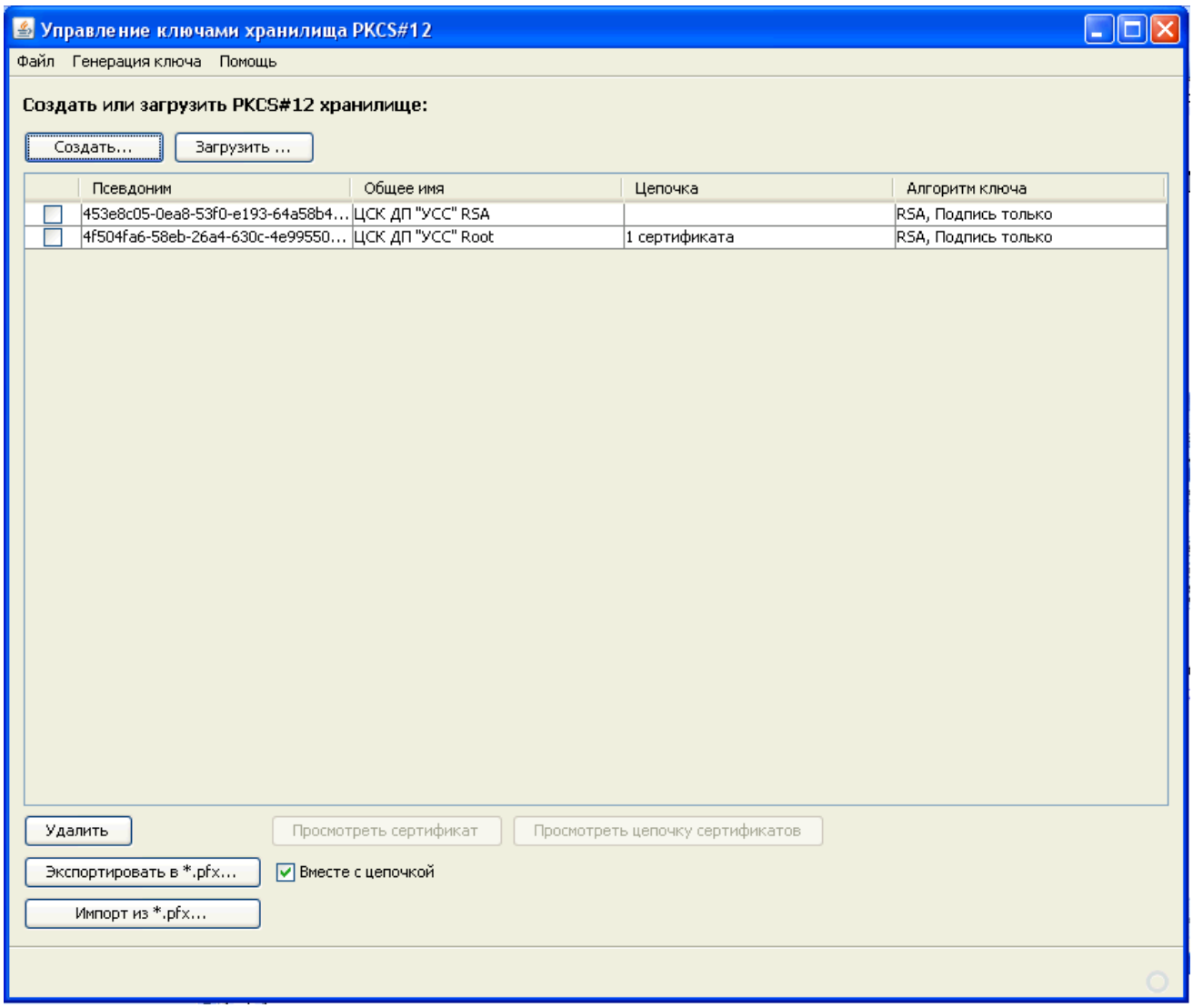
Ввести пароль доступу до сховища (та повторити його), і вибравши команду «Зберегти як…» записати сховище до файлу:



2.3. Завантаження сховища PKCS#12

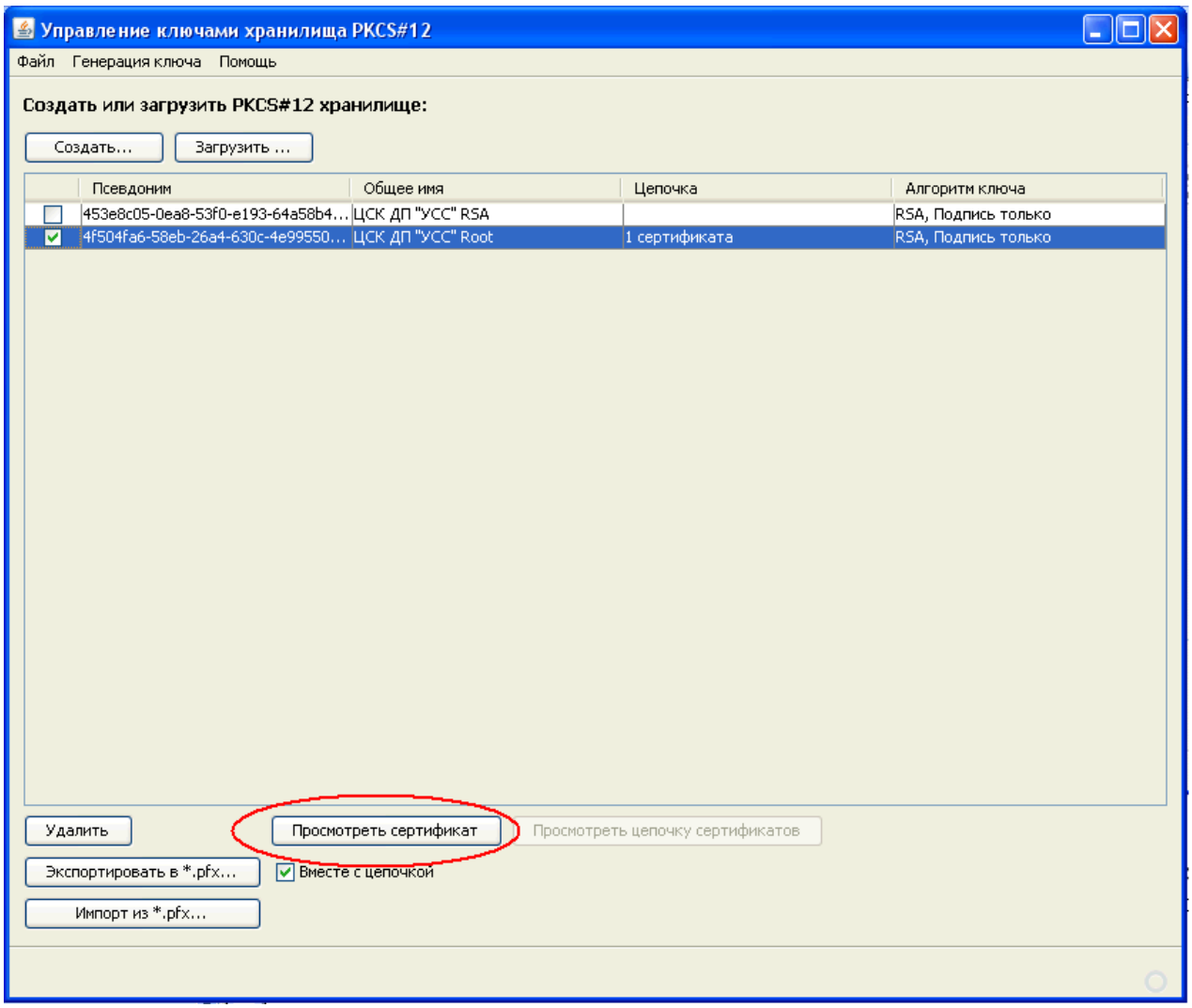
Якщо сховище вже існує, то в основному вікні Інструменту вибрати кнопку «Завантажити…», та після вибору файлу ввести пароль доступу:

При наявності у сховищі ключів та сертифікатів вони будуть відображені у таблиці:



У стовпці «Ланцюг» (сертифікатів) показано скільки сертифікатів з ланцюга міститься у сховищі. Якщо запис пустий, то ця ключова пара не має сертифікату – це пара, на яку сформовано запит PKCS#10 на отримання сертифікату.

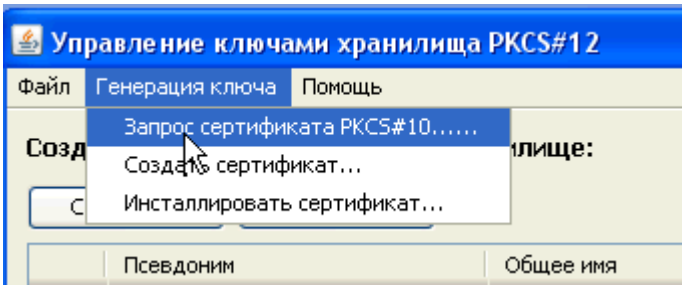
Якщо сертифікат присутній, то його можна переглянути, вибравши конкретний запис та потім натиснувши кнопку «Подивитися сертифікат»:



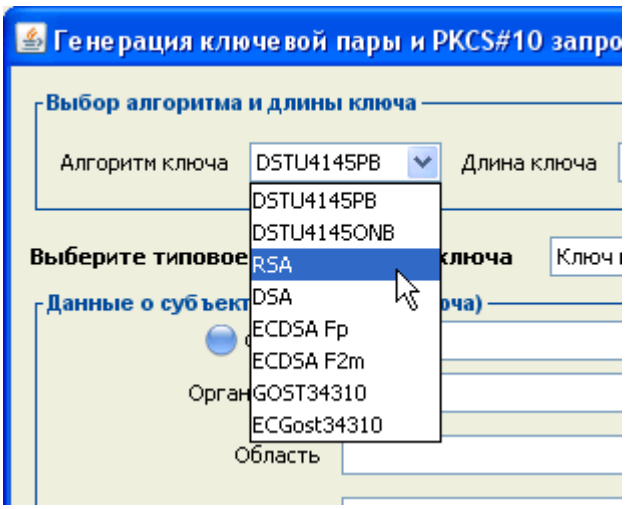
2.4. Генерація ключа та запиту PKCS#10

Генерація ключа виконується у відкритому сховищі (див. п.2.3.).

Для генерації ключа та одночасно запиту (чи само підписаного сертифікату) вибрати меню «Генерація ключа/ Запит сертифікату PKCS#10…»:



У новому вікні генерації вибрати алгоритм ключа із доступних у списку алгоритмів:



де

DSTU4145PB – стандарт ДСТУ 4145-202, поліноміальний базис;

DSTU4145ONB – стандарт ДСТУ 4145-202, оптимальний нормальний базис;

RSA – стандарт RFC 3447:2003, FIPS 186-3:2009, PKCS #1 v2.1;

DSA – стандарт FIPS 186-3:2009, ДСТУ ISO/IEC 14888-3:2002;

ECDSA Fp – стандарт FIPS 186-3:2009, ДСТУ ISO/IEC 14888-2:2002;

ECDSA F2m – стандарт FIPS 186-3:2009, ДСТУ ISO/IEC 14888-2:2002;

GOST34310 – стандарт ГОСТ 34.310-95;

ECGost34310 –стандарт ГОСТ 34.310-2004.

Для стандарту **ECDSA** підтримуються еліптичні криві, визначені такими стандартами:

SEC2 - Standards for Efficient Cryptography (SEC), SEC 2: Recommended Elliptic Curve Domain Parameters - September 20, 2000, Version 1.0, Certicom Corp.

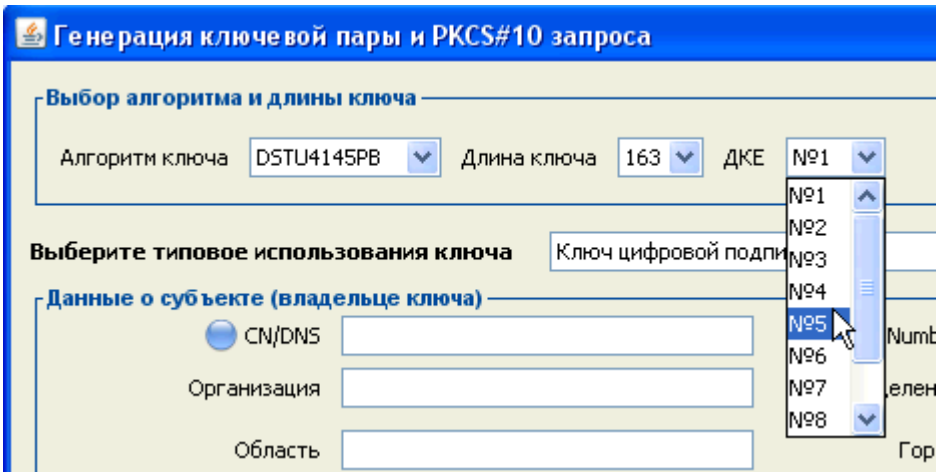
NIST - FIPS 186-3: Digital Signature Standard (DSS); Annex D.1 NIST Recommended Elliptic Curves - June, 2009

X9.62 - X9.62-2005: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

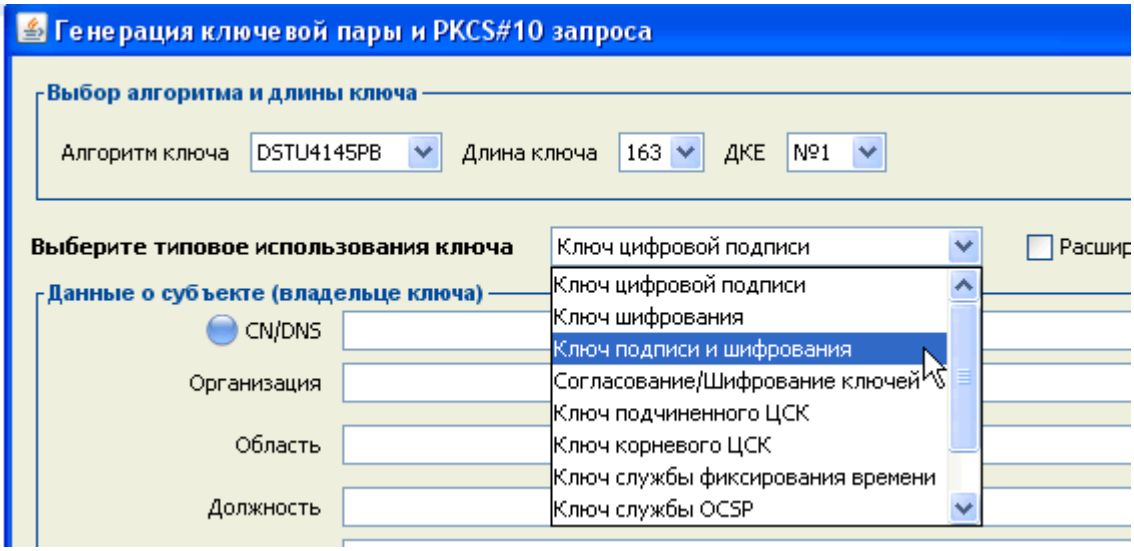
Brainpool - ECC Brainpool:

1) ECC Brainpool Standard Curves and Curve Generation, Version 1.0, 2005. - http://www.ecc-brainpool.org/ecc-standard.htm; and
2) **BSI** TR-03111: Technical Guideline TR-03111. Elliptic Curve Cryptography, Version 1.11" – BSI (Bundesamt fur Sicherheit in der Informationstechnik), 2009 - https://www.bsi.bund.de/cae/servlet/contentblob/471398/publicationFile/30909/BSI-TR-03111_pdf.pdf;
3) ECC Brainpool Standard Curves and Curve Generation - RFC draft-lochter-pkix-brainpool-ecc-03, March 6, 2009.

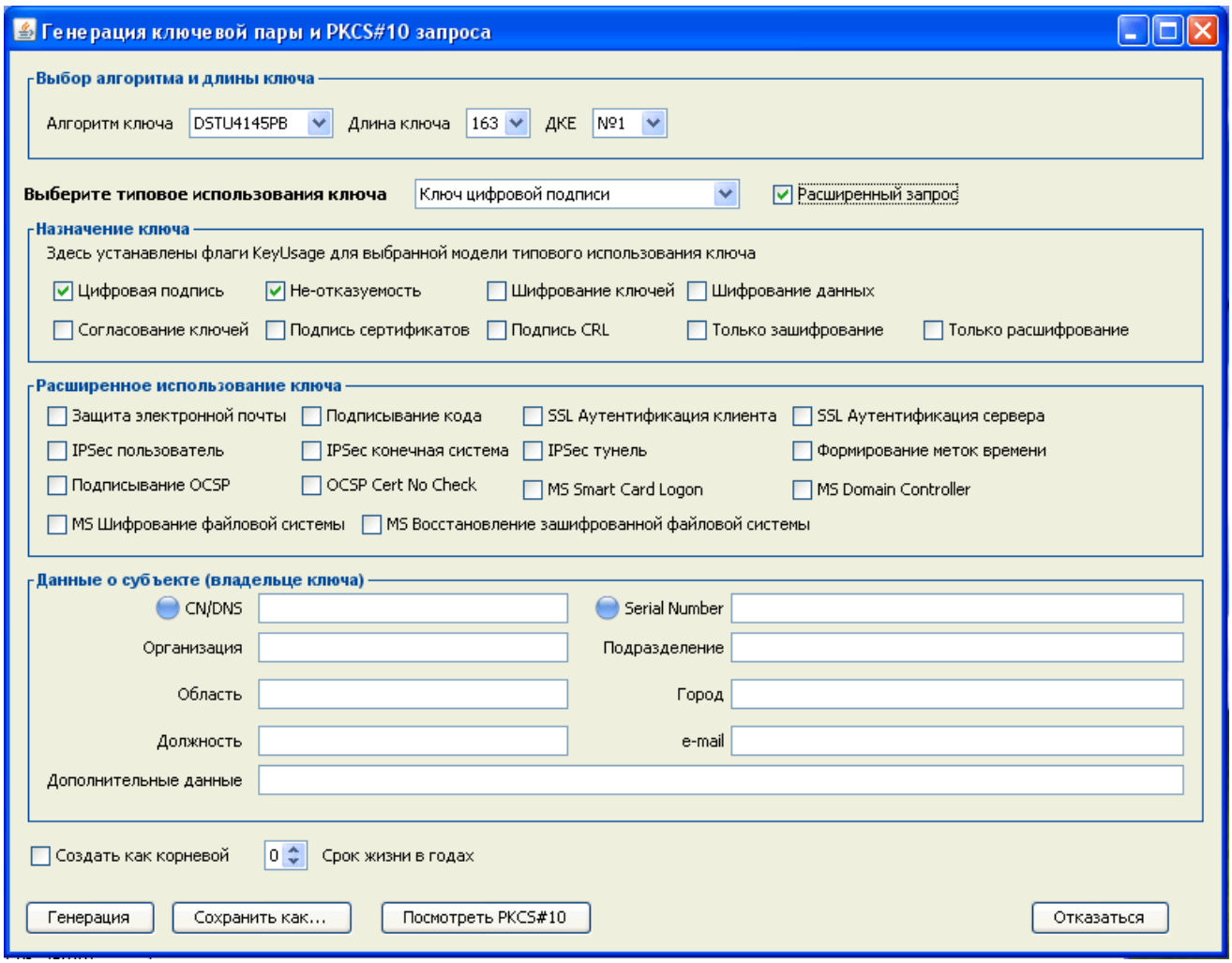
Вибрати довжину ключа чи еліптичну криву (за назвою чи ідентифікатором). Для ДСТУ ключів додатково вибрати ДКЕ (довготривалий ключовий елемент):



Вибрати типове використання ключа:



Якщо необхідно, вибрати «Розширений запит», та встановити розширення запиту:



Заповнити реквізити підписувача (власника ключа).

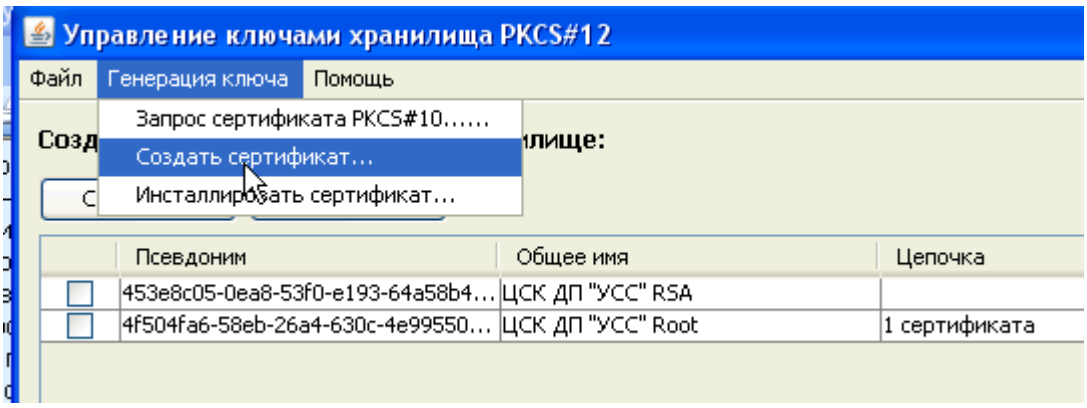
На завершення, встановити прапорець «Створити як кореневи», якщо треба додатково створити само підписаний сертифікат (за записати його в сховище), а також визначити термін дії сертифікату в роках.

Після цього вибрати кнопку «Генерація».

Кнопкою «Зберегти як..» треба виконати збереження запиту PKCS#10 у файл.

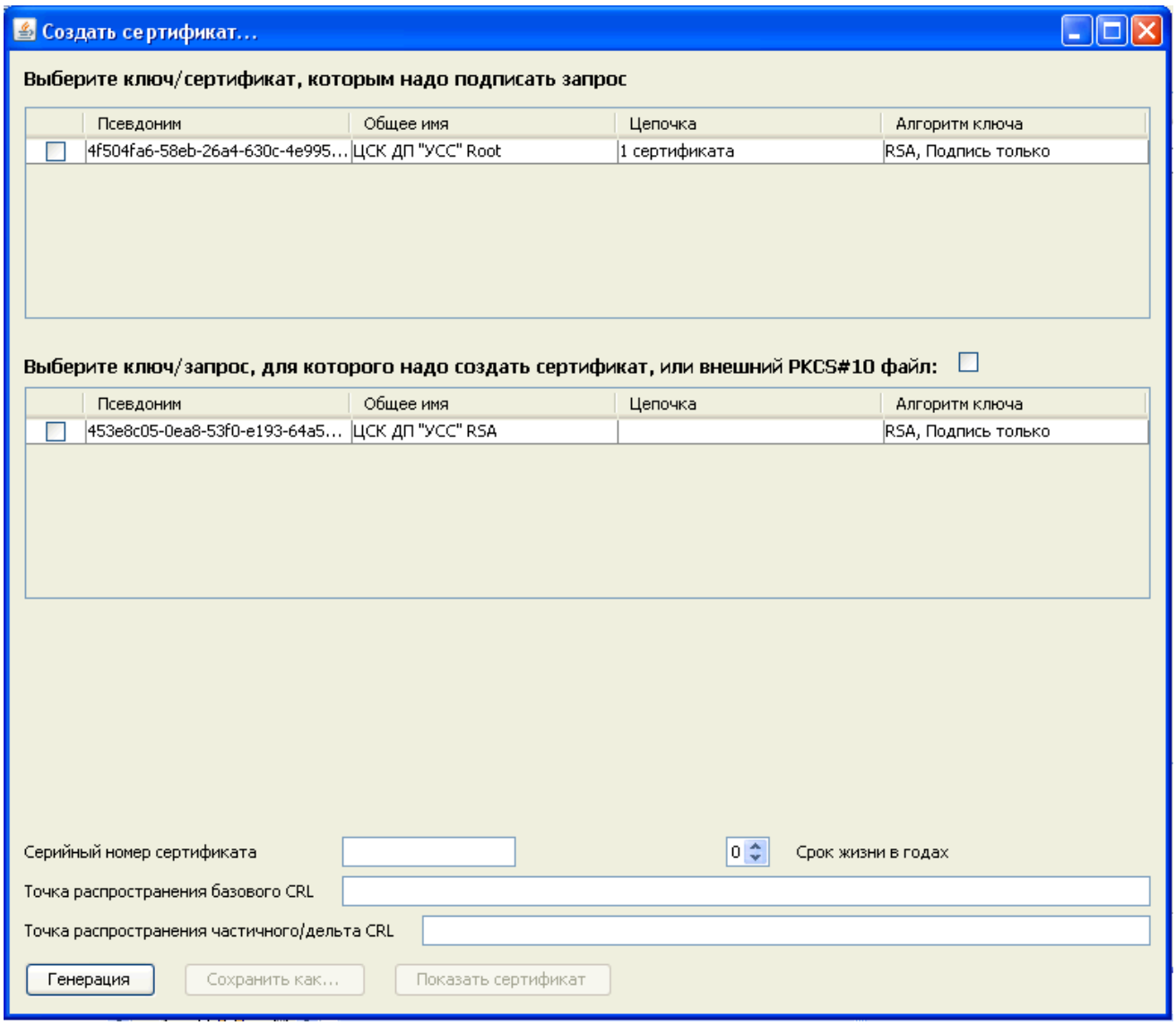
2.5. Створити сертифікат

Меню «Створити сертифікат» призначається для створення/ генерації сертифікату із запиту PKCS#10:

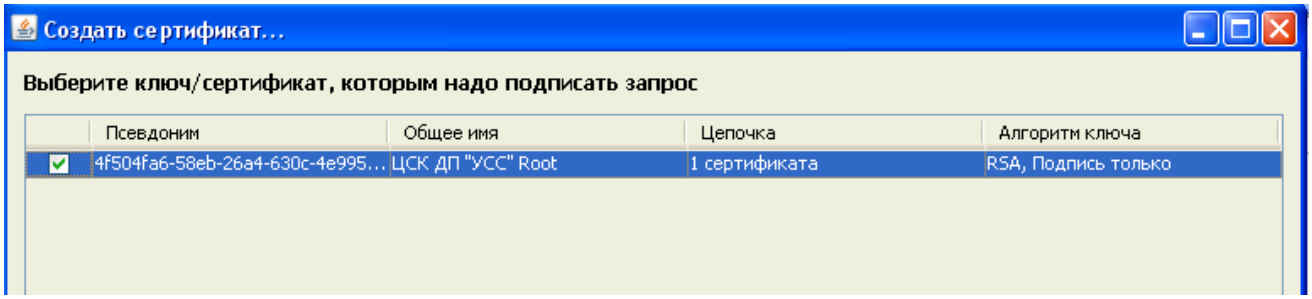


Сертифікат при цьому підписується ключем, який вибирається в сховищі. Отже, створити сертифікат можна лише після створення в сховищі ключової пари та її сертифікату, який може бути само підписаним (див. п.2.4.), або імпортований із файлу ззовні (див. п. «Імпортувати сертифікат»)

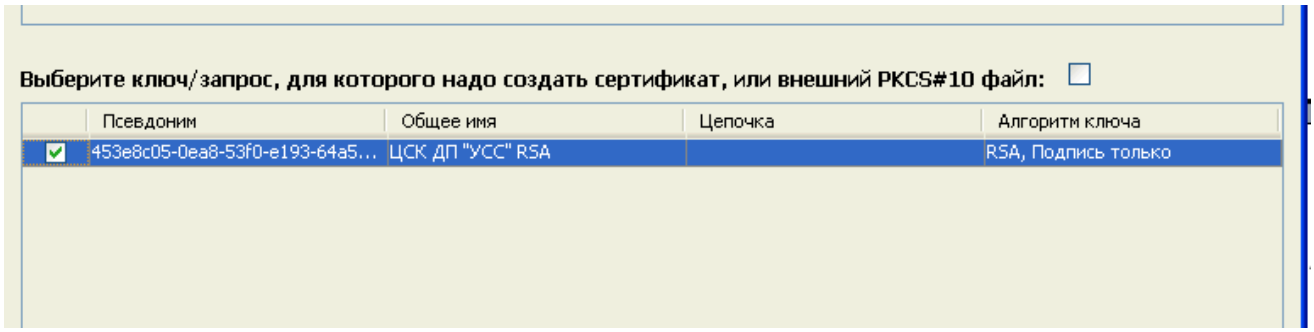
Вікно «Створити сертифікат»:



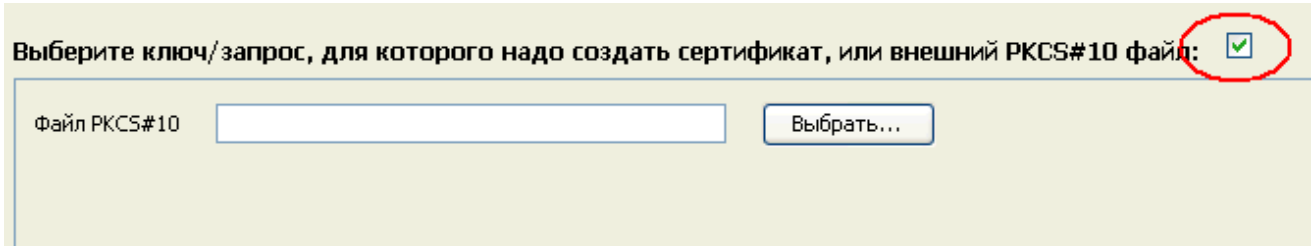
1) Вибрати сертифікат/ ключ, яким слід підписати новий (створюваний) сертифікат



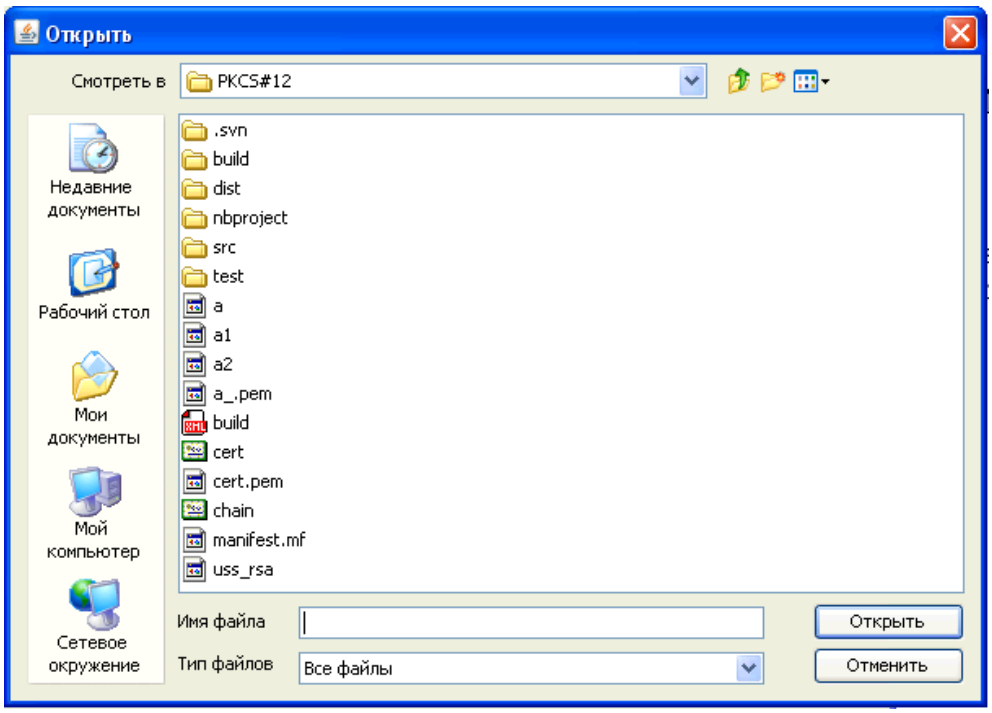
2) Вибрати запит
   a. Якщо сертифікат створюється із запиту для ключової пари, що є у сховищі, то слід вибрати цю пару:



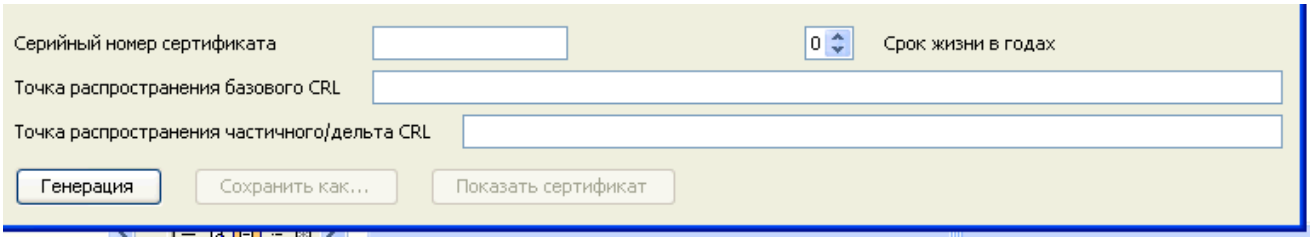
   b. Якщо сертифікат створюється із зовнішнього запиту (файлу), то слід вибрати прапорець зовнішнього файлу та відповідний файл:



вибрати файл:



3) Задати серійний номер для сертифікату, що створюється, та його термін життя/ дії у роках:



Додатково слід ввести точки розповсюдження списків відкликання (основного, та часткового), як URL, наприклад:

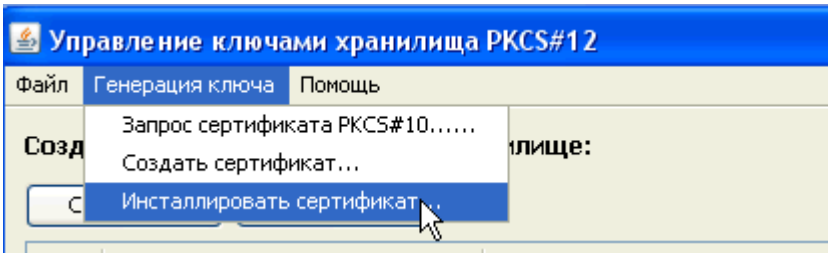
http:://example.com.ua/crllisl.crl – основний CRL
http:://example.com.ua/crllisl+.crl – частковий CRL

На завершення, натиснути кнопку «Генерація».

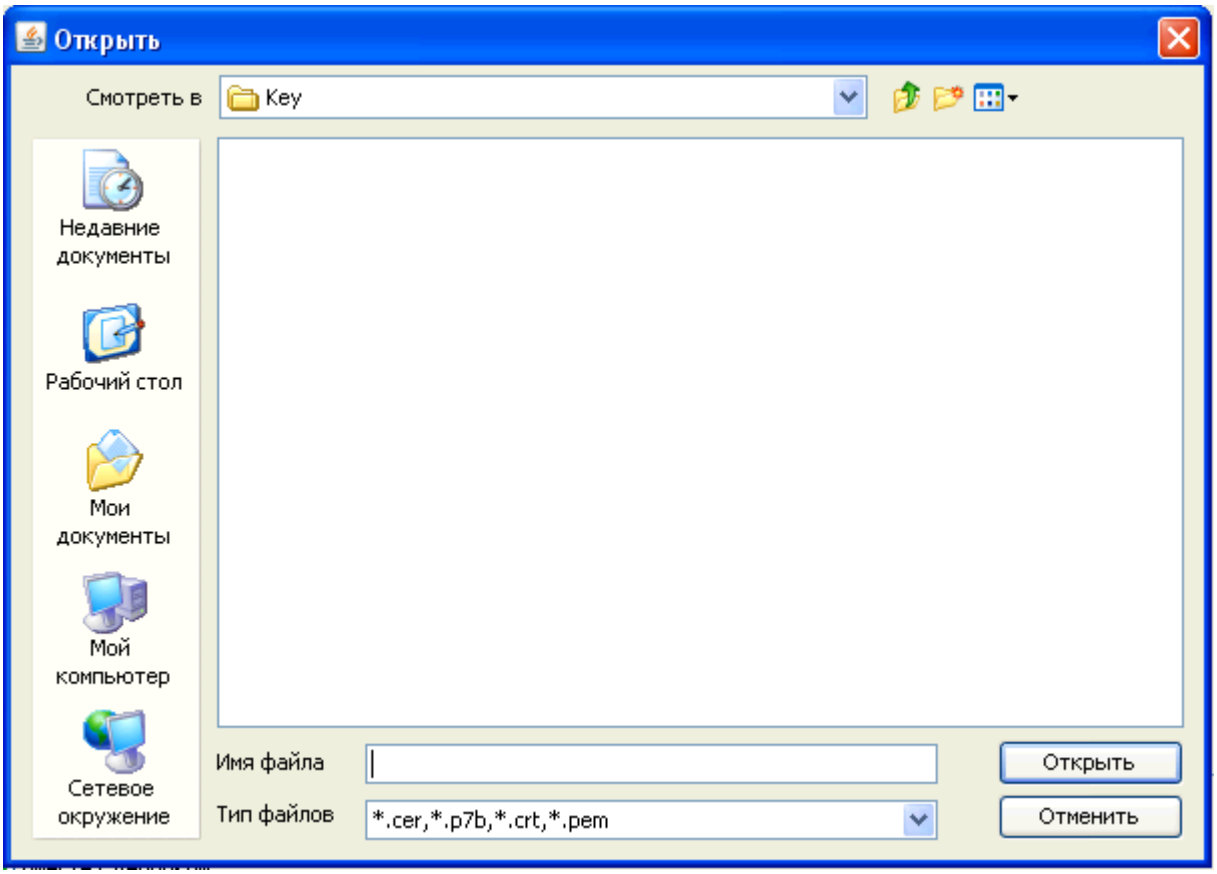
Генерований сертифікат слід зберегти як файл (кнопка «Зберегти як…», та додатково можна переглянути (кнопка «Показати сертифікат»).

2.6. Інсталяція сертифікату

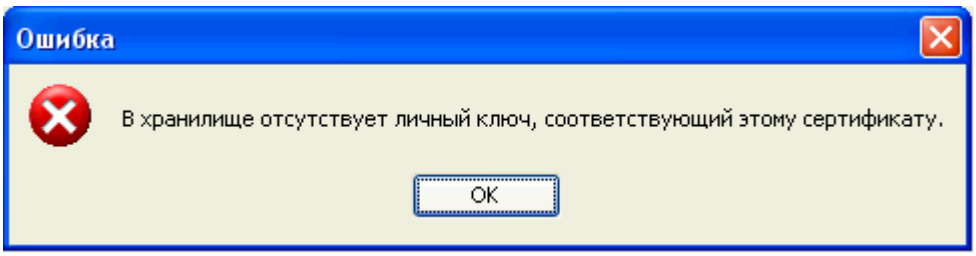
Інсталяція сертифікату виконується за командою меню «Інсталювати сертифікат…»:



Вибрати файл сертифікату:



Після вибору файлу сертифіката, програма виконає пошук відповідної ключової пари у сховищі, і у разі відсутності ключової пари завершиться помилкою:



У разі наявності відповідної ключової пари у сховищі буде виконана операція встановлення сертифікату до знайденої ключової пари. Якщо пара вже має сертифікат, то програма надасть попередження та виконає заміну сертифікату лише за підтвердженням.

2.7. Імпорт/експорт ключів

Нижня частина основного вікна містить команди експорту/ імпорту ключів у форматі файлів *.pfx (PKCS#12 стандарт):