**Інструкція**

**щодо налаштування та здійснення електронного документообігу**

Публічним акціонерним товариством "Розрахунковий центр з обслуговування договорів на фінансових ринках" (далі – Розрахунковий центр) на базі програмного продукту GPG впроваджено систему електронного документообігу (далі - Система), що протягом вже більш ніж двох років дозволяє успішно здійснювати обмін електронними документами (далі - ЕД) з операторами організованого ринку та депозитаріями.

ЕД, які сформовані в Системі, згідно до узгоджених сторонами документів, мають юридичну силу документів складених у паперовій формі і передбачають забезпечення безумовного виконання даних ЕД Розрахунковим центром та відправниками або отримувачами даного ЕД.

ЕД генеруються у форматі, що визначається попередньо погодженим сторонами регламентом, за допомогою програмного забезпечення відправників, та підписуються наданим іншою стороною відкритим ключем, що сформовано з використанням програмного продукту GPG (далі - GPG). Обмін підписаними та зашифрованими файлами між операторами організованого ринку та депозитаріями і Розрахунковим центром здійснюється за допомогою FTP-серверу Розрахункового центру, до якого учасники клірингу отримують відповідний доступ. Для отримання доступу до FTP-серверу Розрахункового центру учасник клірингу надає Розрахунковому центру заяву (за визначеною формою) на підключення до FTP-серверу, заява на підключення до FTP-серверу може бути також подана у електронній формі.

GPG створено як альтернатива PGP, випущено під ліцензією GNU General Public License для вільного використання та являє собою безкоштовне програмне забезпечення для шифрування інформації та створення електронних підписів.

Відповідні файли - налаштування, що забезпечують роботу GPG та самої Системи, а також консультації щодо їх впровадження та підключення до FTP-серверу будуть надані Розрахунковим центром.

Додатки: Короткий опис програмного продукту GPG на (Додаток 1),

Інструкція з встановлення та використання GPG для MS Windows (Додаток 2).

Контактні дані:

Дубенчук Сергій Леонідович тел. (**044) 585-42-42 (вн.** 1066), [dsl@settlement.com.ua](NULL)

## Додаток 1

**Короткий опис програмного продукту GPG**

**Використання**

GPG використовується як для симетричного шифрування, так і для асиметричного шифрування. При асиметричному шифруванні Користувач GPG створює ключову пару: відкритий і закритий ключ. При генерації ключів задаються їх власник (назва організації та адреса електронної пошти), тип ключа, довжина ключа і термін його дії. Відкритий ключ використовується для шифрування і перевірки цифрового підпису його можна передати тим, хто буде надсилати вам зашифровані повідомлення. Закритий ключ-для декодування і створення цифрового підпису.

Основним інтерфейсом GPG є командний рядок. Також існують зовнішні додатки, які роблять доступною функціональність цього програмного продукту з використанням графічного інтерфейсу.

GPG-працює майже на всіх операційних системах: від Microsoft Windows і GNU / Linux до Mac OS X, FreeBSD, OpenBSD, NetBSD і т. д.

У більшості дистрибутивів GNU / Linux GPG вже встановлено.

Для користувачів операційної системи Microsoft Windows розробниками проекту GPG випускається Gpg4win (GNU Privacy Guard for Windows) - інсталяційний пакет, який включає в себе:

- GnuPG для Windows (ядро пакета, сам засіб шифрування);

- Kleopatra (менеджер сертифікатів для OpenPGP і X. 509);

- GPA (альтернативний менеджер сертифікатів (GNU) для OpenPGP і X. 509);

- GpgOL (плагін для Outlook);

- GpgEX (плагін для Провідника Windows для шифрування файлів);

- Claws Mail (поштова програма з підтримкою функцій GnuPG - починаючи з версії 2.2.6 видалений з пакета);

- документацію англійською та німецькою мовою.

По суті Gpg4win - це офіційна версія GnuPG для платформи Windows і всі включені в цей пакет компоненти також безкоштовні.

**Особливості**

- Повна альтернатива PGP.

- Не використовує патентовані алгоритми.

- Поширюється під GNU General Public License.

- Повна реалізація OpenPGP.

- Робота з асиметричним шифруванням RSA, ELG, DSA, ECDH, ECDSA, EDDSA (довжина ключа від 1024 до 4096 біт).

- Підтримка алгоритмів стиснення: ZIP, ZLIB, BZIP2.

- Хеш-функції: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224

- Легка реалізація нових алгоритмів за допомогою додаткових модулів.

- Підтримка прострочених ключів і підписів.

- Розшифрування і автентифікація поштових повідомлень, створених за допомогою PGP 5, 6 і 7.

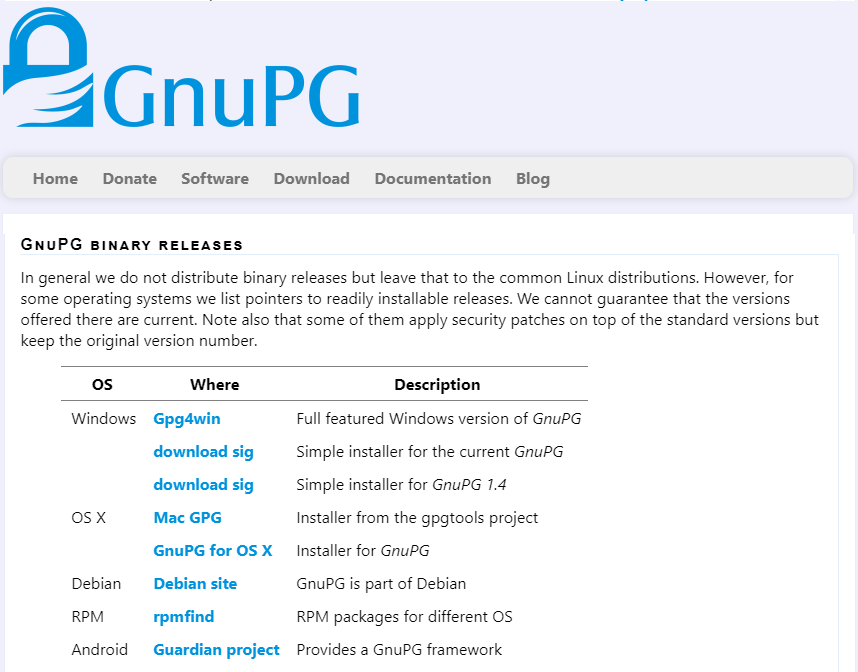
- Інтегрована підтримка HKP серверів ключів.

- Вбудований сервер і клієнт для поширення відкритих ключів.

## Додаток 2

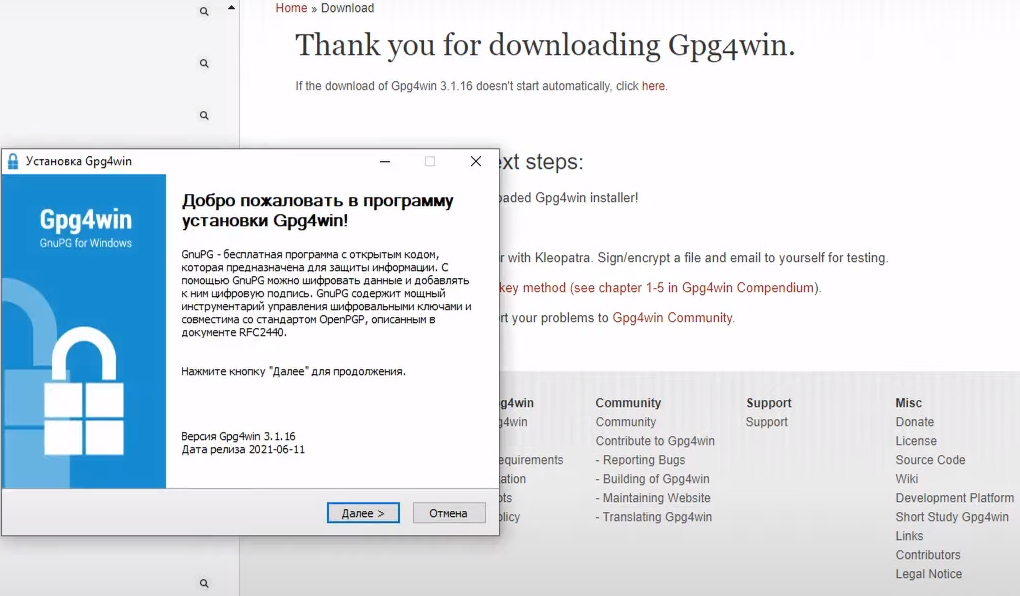
**Інструкція з встановлення та використання GPG для Microsoft Windows**

Інсталяційний пакет Gpg4win можна отримати за посиланням https://www.gnupg.org/download/index.html

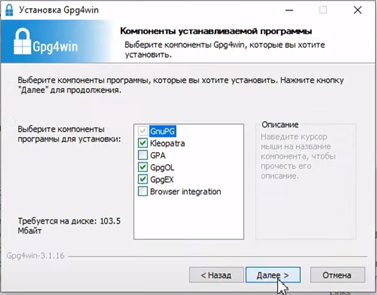


або може бути переданий Розрахунковим Центром.

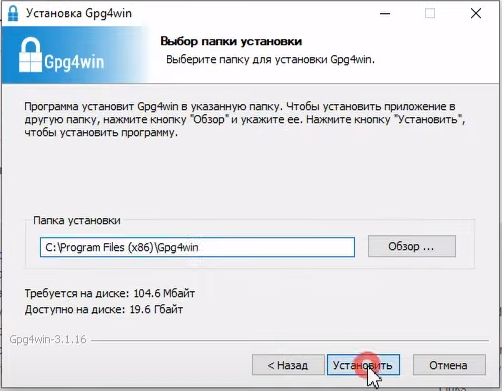
Для початку процесу інсталяції запускаємо дистрибутив Gpg4win



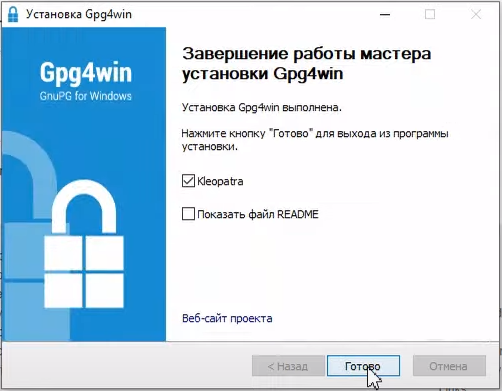
Обираємо компоненти, що встановлюються:

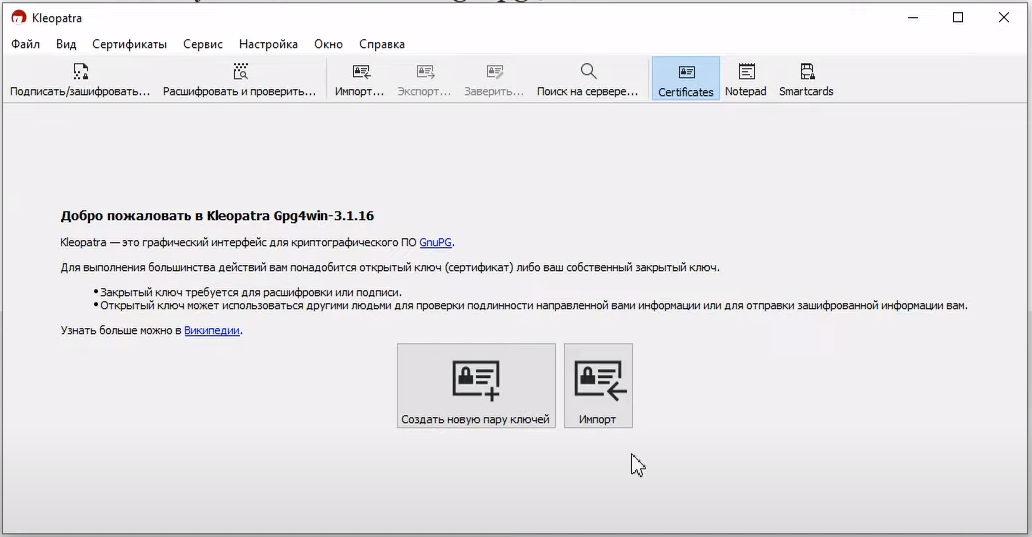


Обираємо папку для встановлення:



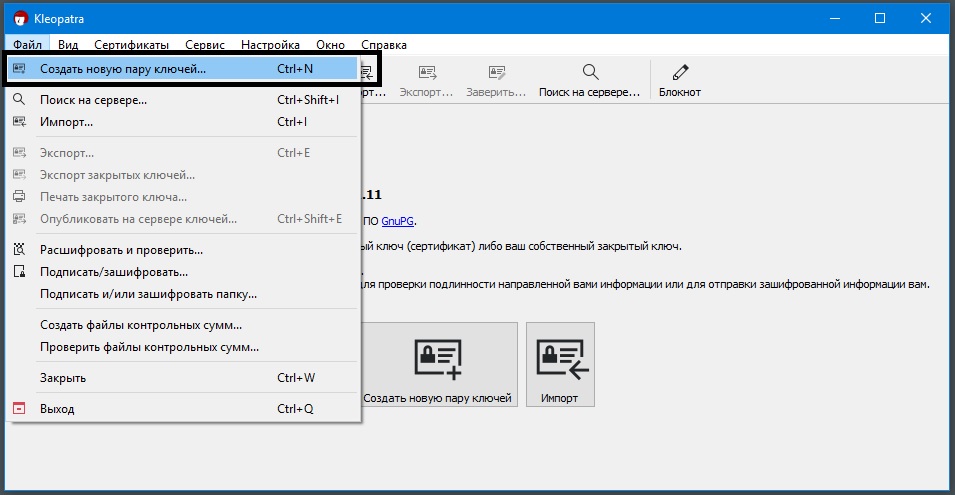
Запускаємо менеджер сертифікатів Kleopatra:



Зовнішній вигляд менеджера сертифікатів Kleopatra:

Перший крок у використанні GPG-створення своєї пари ключів. Публічний (відкритий) ключ надається всім бажаючим, а секретний зберігається в надійному місці і служить для підписання інформації від імені його власника і розшифрування адресованої йому інформації.

Створення пари ключів:



На вибір пропонуються типи ключів X. 509 (практично застосовується в корпоративному середовищі) і OpenPGP. Вибираємо OpenPGP. Вводимо дані, які будуть відображатися у всіх власників нашого відкритого ключа.

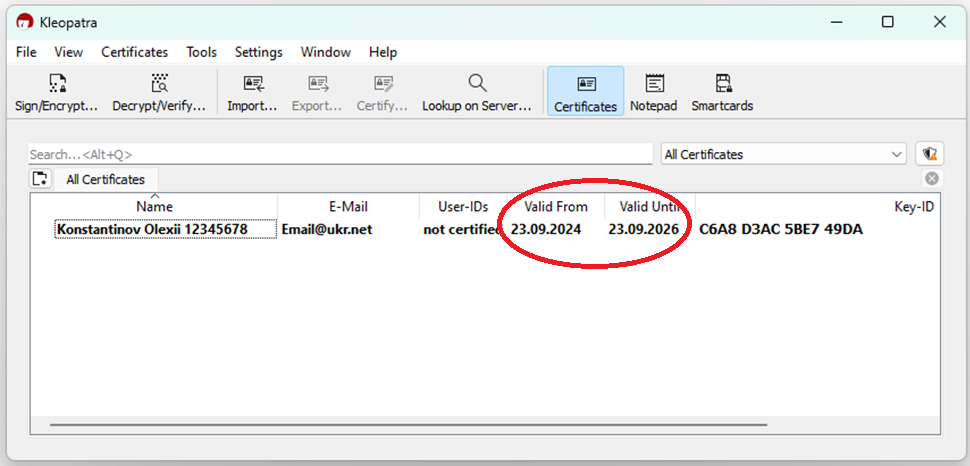
Потрібно вказати реквізити, що мають відповідати полям з позначкою **дані, що внесені до ключа**, які вказані у Заяві на підключення до Системи електронного документообігу з учасниками клірингу Користувача (особи, яка має право підпису), згідно Додатку 1 до Положення про систему електронного документообігу з учасниками клірингу публічного акціонерного товариства "Розрахунковий центр з обслуговування договорів на фінансових ринках" а саме:

* у першому полі - **Прізвище Ім'я** (латиницею) **ЄДРПОУ** (8 цифр). Реквізити: Прізвище, Ім'я, ЄДРПОУ віддокремлюються пробілом;
* у другому полі – **E-Mail**.

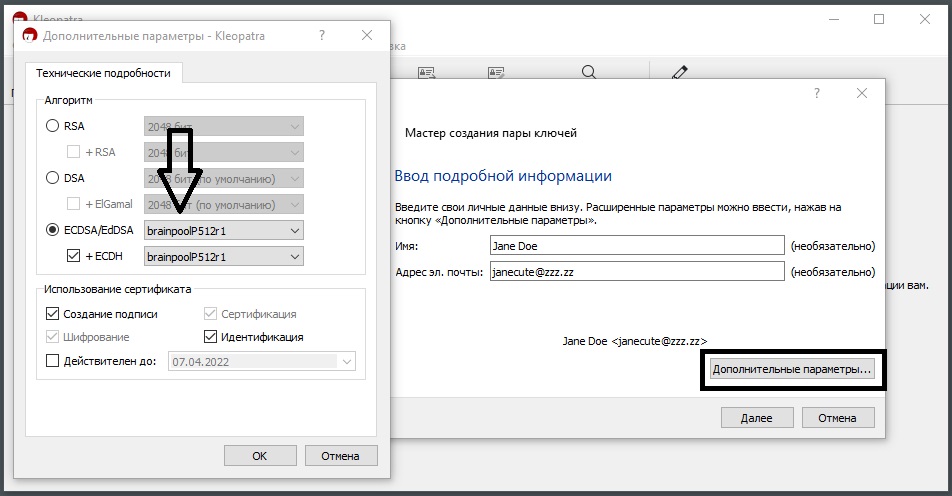
Зображення, що містить текст, електроніка, знімок екрана, монітор

Автоматично згенерований опис

Термін дії кожного особистого ключа Учасника клірингу / Розрахункового центру не повинен перевищувати **2 роки** з дня його генерації.



За замовчуванням використовується шифрування RSA з довжиною ключа в 2048 біт. В даний час себе добре зарекомендувало використання криптографії на еліптичних кривих. Подібні алгоритми мають відмінну криптостійкість і хорошу продуктивність, завдяки невеликій довжині ключа.



Щоб створити пару ключів (як приклад) на еліптичних кривих, переходимо в додаткові параметри. Пункт ECDSA / EdDSA-те, що нам треба. Додатковий чекбокс (галочка)" +ECDH" дасть ключу можливість шифрувати, без неї сертифікат можна буде використовувати тільки для підпису та ідентифікації, так як ECDSA/EdDSA — алгоритми підпису, а не шифрування.

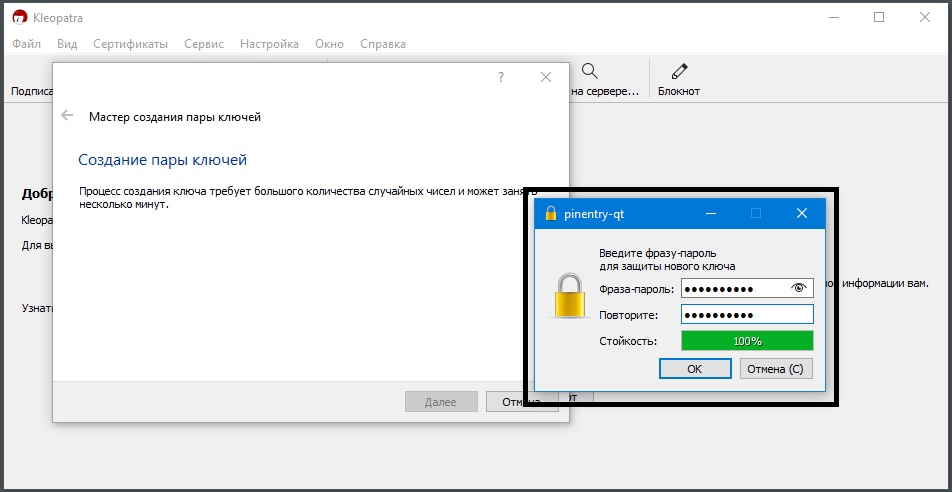
У списках, що випадають пропонується вибрати один з алгоритмів: ed25519, brainpool і NIST.

1. ed25519 (Curve25519)-еталонна і непатентована реалізація криптографії на еліптичній кривій, має 128-бітну довжину. Є ключем EdDSA - найактуальнішим алгоритмом цифрового підпису (вважається, що без закладок від силових структур будь-яких країн).

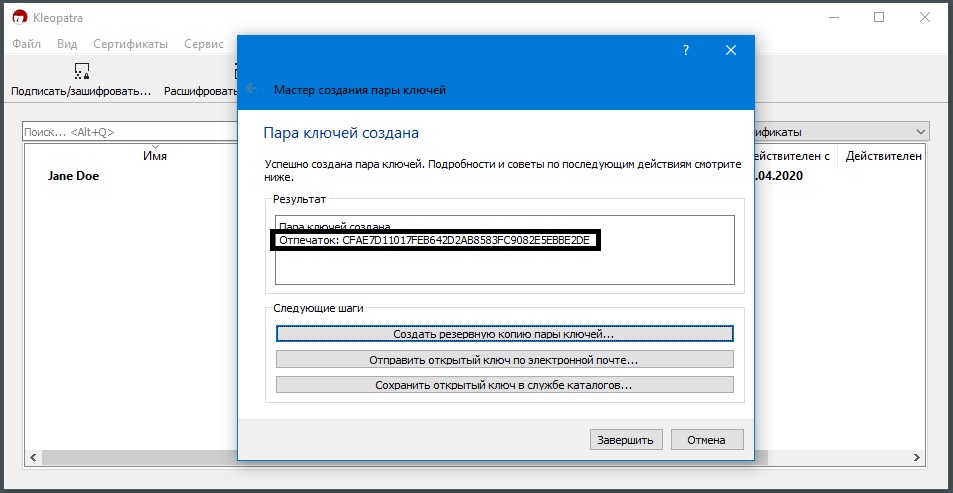
2. brainpool-алгоритм, розроблений німецьким співтовариством криптографів, в число яких входять університети, державні відомства та комерційні організації, наприклад, компанія Bosch. Підтримує довжини в 256, 384 і 512 біт. При підписі використовує дещо застарілий алгоритм ECDSA.

3. NIST-Американський алгоритм, розроблений Національним інститутом стандартів і технологій. Рекомендований для використання державними органами США. Підтримує довжини в 256, 384 і 521 біт. За оцінкою деяких фахівців, NIST краще brainpool по продуктивності. При підписі використовує дещо застарілий алгоритм ECDSA.

Для прикладу в обох випадках використовується алгоритм brainpool з максимальною довжиною ключа. За замовчуванням ключ створюється з терміном придатності в два роки. Цей параметр можна змінити, або зовсім відключити, тоді ключ буде безстроковим.

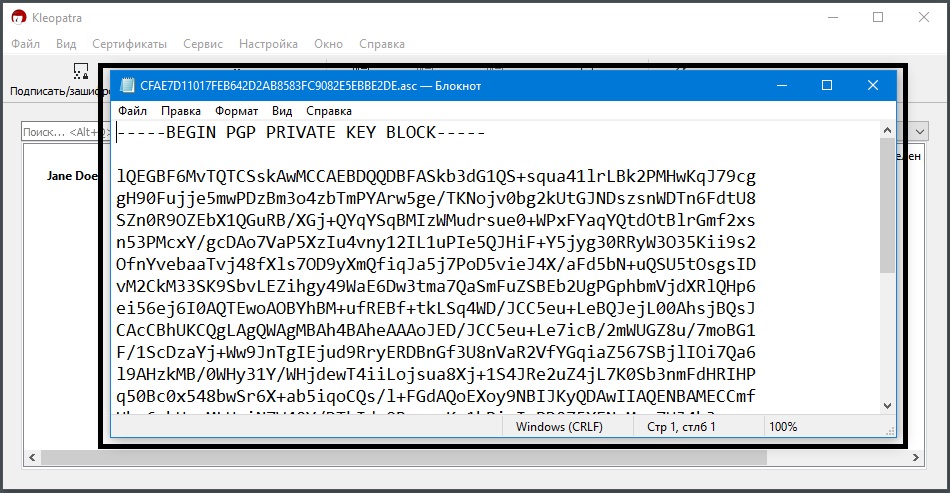


На наступному кроці задається пароль, який є останнім кордоном захисту секретного ключа. **Для використання GPG у фоновому режимі пароль не задавати не потрібно.**



Отже, пара ключів створена! Зверніть увагу на відбиток, це унікальний ідентифікатор вашого ключа. Навіть якщо хтось захоче представитися вами, створивши ключ з такими ж ім'ям і електронною поштою, його відбиток буде відрізнятися. Саме тому важливо звіряти відбитки одержуваних ключів.

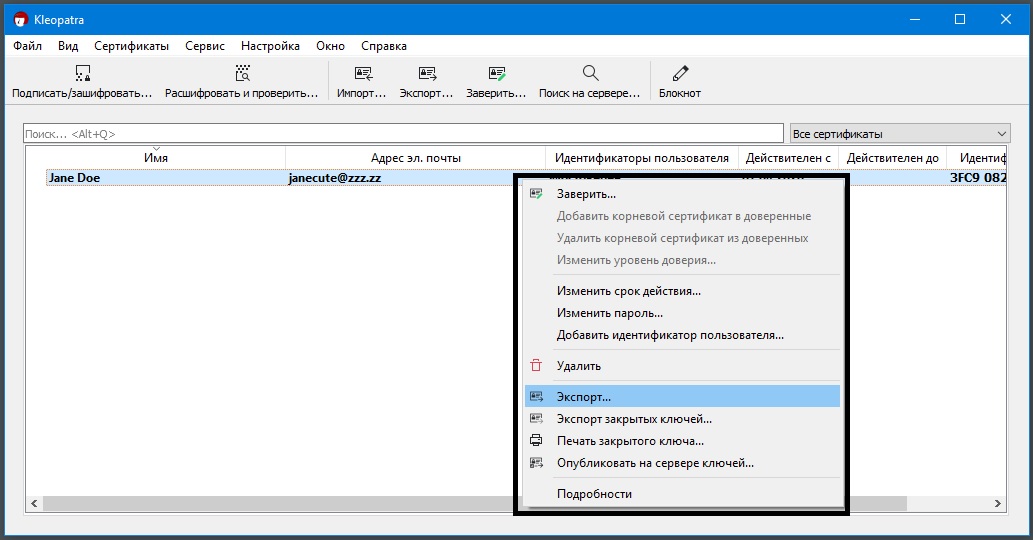
Клеопатра пропонує зробити резервну копію ключів, що за фактом є експортом закритого ключа. Цю операцію в подальшому можна зробити в будь-який момент.



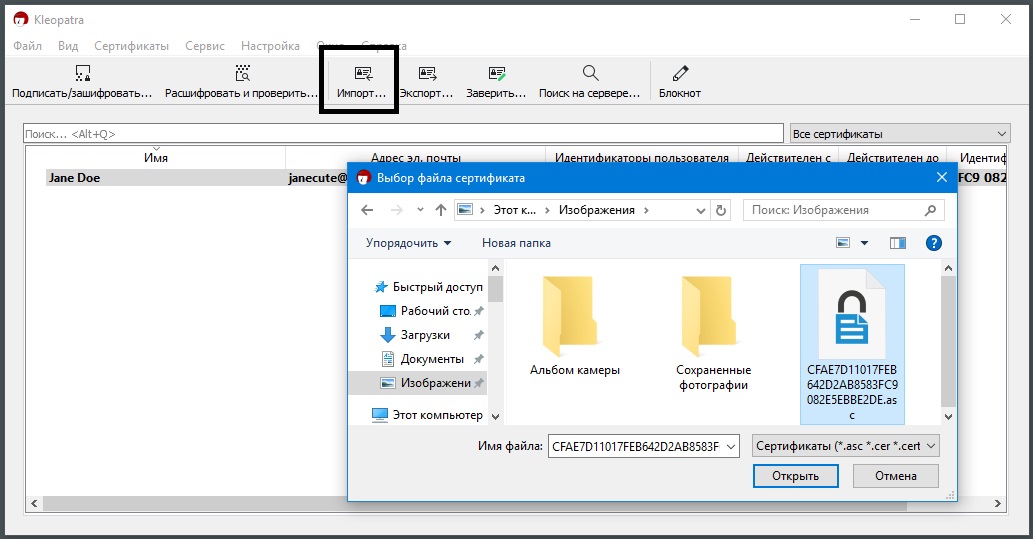
Відкривши експортований ключ в текстовому редакторі, ми побачимо специфічний фрагмент тексту, що починається словами "BEGIN PGP **PRIVATE** key BLOCK". Будьте уважні, щоб не відправити його комусь помилково! Відкриті ключі, призначені для передачі другим особам, починаються зі слів "BEGIN PGP **PUBLIC** key BLOCK".

Зберігати можна тільки приватний ключ, так як при необхідності комусь передати публічний, ми завжди можемо експортувати його з секретного (виводиться математичним шляхом).

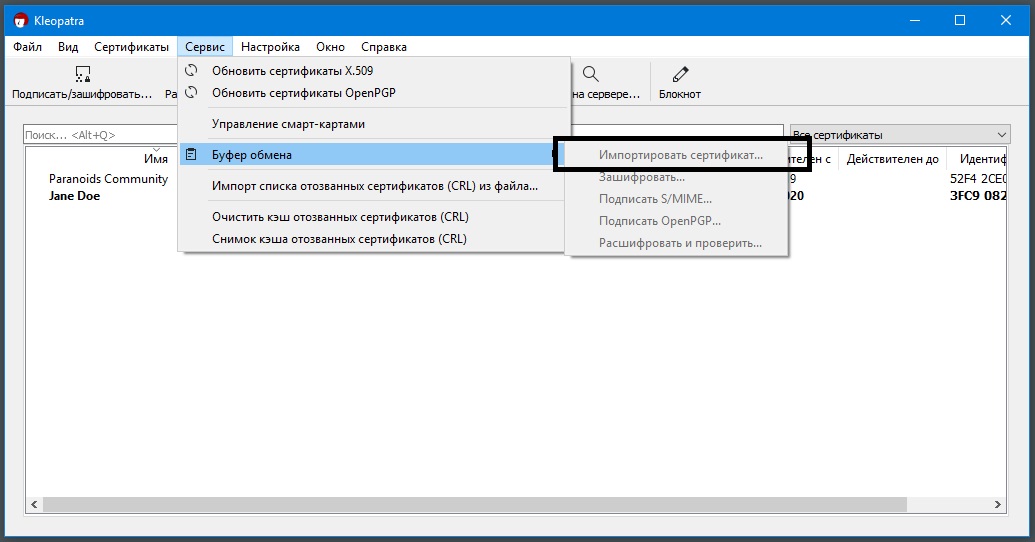
Експорт та імпорт



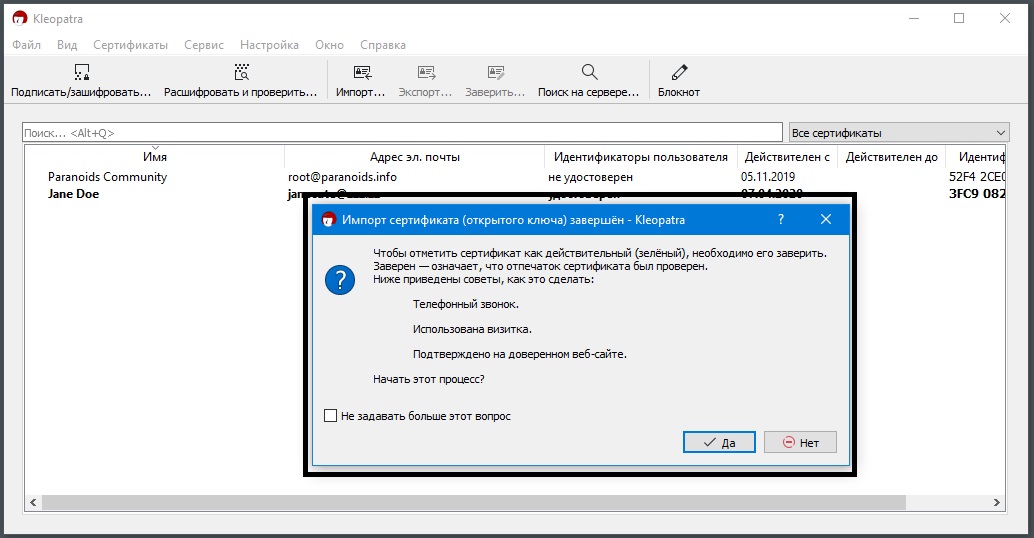
Для операцій з ключем, клацніть по ньому правою кнопкою миші.



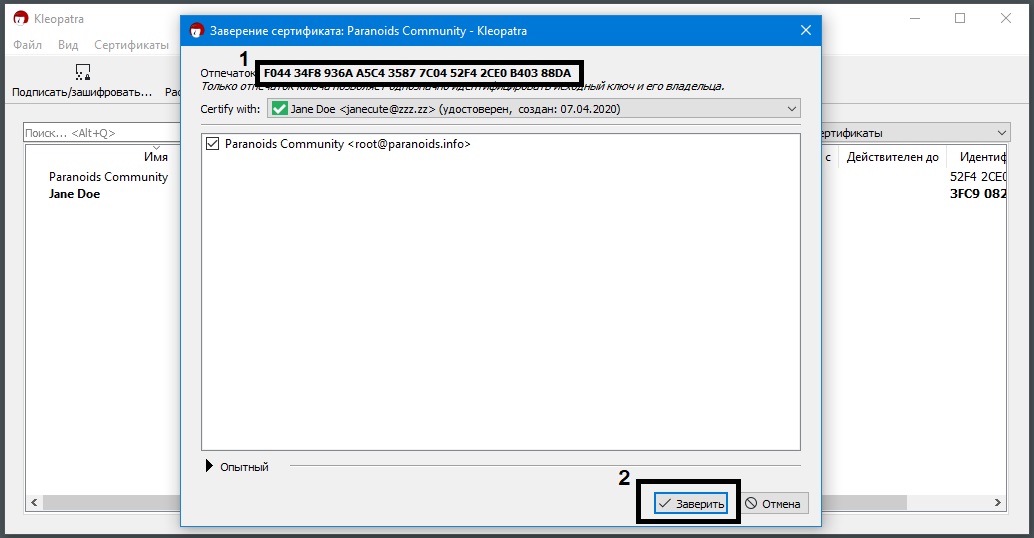
Для імпорту ключів (нашого вже існуючого на новому пристрої або отриманого публічного), скористаємося кнопкою "імпорт". Також можна використовувати подвійний клік по файлу ключа, це автоматично відкриє Клеопатру і імпортує обраний ключ. GPG-файли зустрічаються з розширеннями\*.asc, \*.pgp і\*.gpg. Це не має великого значення, так як розширення потрібно більше для зручності користувача і лише трохи — додатків. Файл буде коректна прочитаний і в разі, коли спеціальне розширення змінено або видалено.



Дуже часто Ключі поширюються у вигляді текстового блоку. В такому випадку, скопіювавши ключ, можна імпортувати його через меню операцій з буфером обміну.

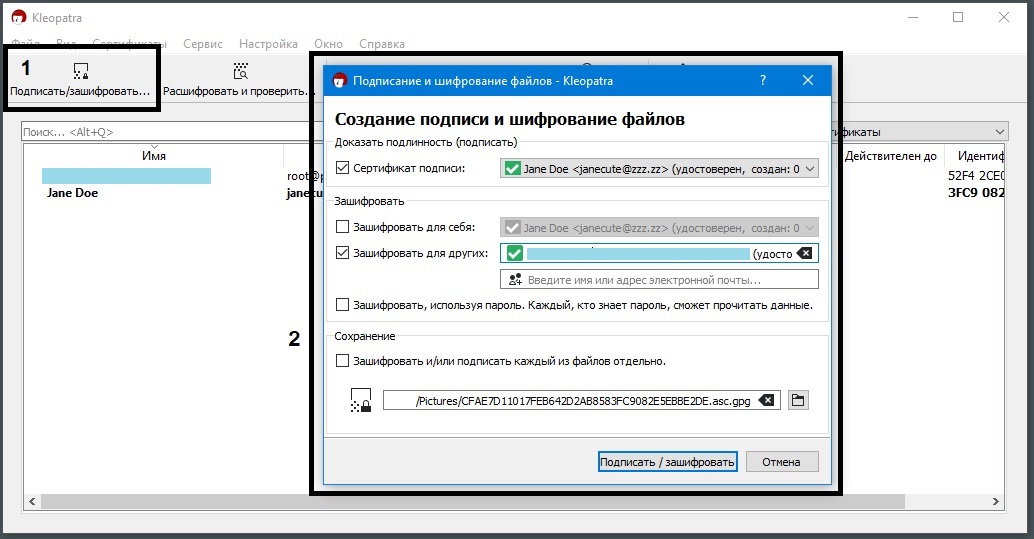


Програма попросить упевнитися в достовірності ключа. В даний час найпростішим і ефективним способом є порівняння відбитка, тому його публікують разом з ключем. Якщо відбиток збігається із заявленим, запевняємо сертифікат.

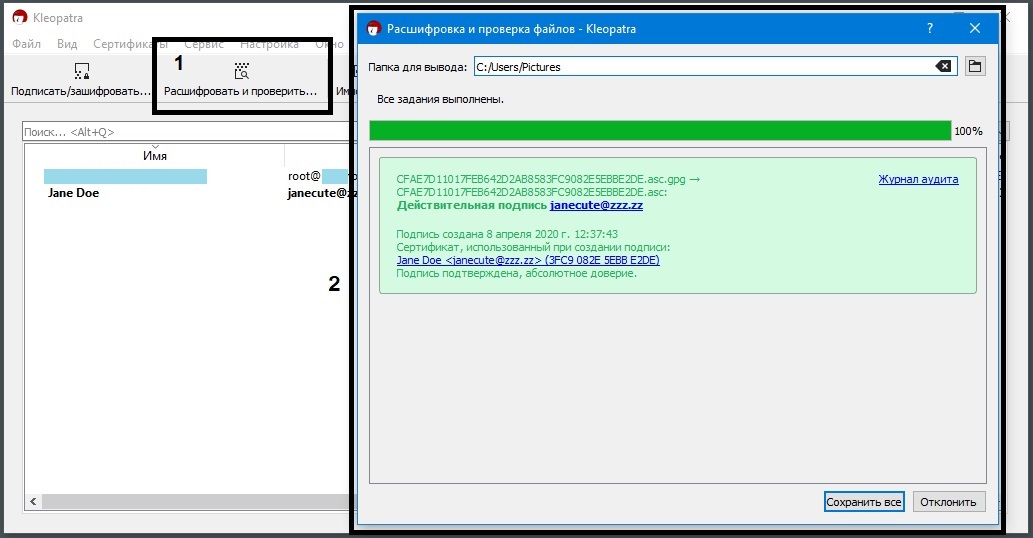


Тепер ми можемо перевіряти підпис власника нового ключа і шифрувати для нього інформацію.

Шифрування та підписання. Щоб зашифрувати і підписати файл, скористаємося відповідним пунктом меню на верхній панелі.



Після вибору файлу, пропонується вибрати потрібні операції. Підпис дозволяє одержувачу переконатися в авторстві файлу.



Всі локальні Ключі централізовано зберігаються на локальному пристрої в спеціальній папці. Всі програми, що взаємодіють з GPG, будуть їх бачити.

Одним з основних позитивних моментів роботи GPG є можливість роботи у фоновому режимі, що дозволяє повністю автоматизувати шифрування, відправку, прийом і дешифрування переданих файлів.