GnuPG

Виктор Борисов

May 30, 2016

Contents

1 Цель работы

Научиться создавать сертификаты, шифровать файлы и ставить ЭЦП.

2 Ход работы

2.1 Kleopatra

- это графический интерфейс для GPG. Для ОС Windows доступен с пакетом Gpg4win.
Пользовательский интерфейс с созданной ключевой парой представлен на рисунке 1

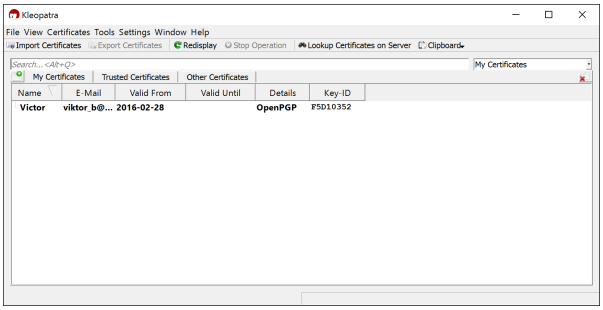

Figure 1: Пользовательский интерфейс Kleopatra.

2.2 Экспорт сертификата

Экспорт сертификата в файл (File -> Export Certificate) *.asc Содержание файла представлено на рисунке 2

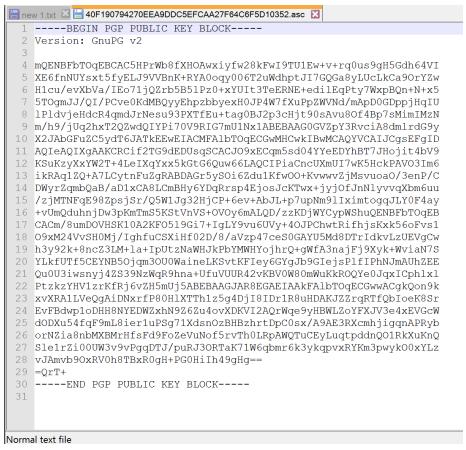

Figure 2: Экспорт сертификата.

2.3 ЭЦП

Поставлена ЭЦП на файл (File -> Sign/Encrypt Files). Шаги процесса отображены на Рисунках 3, 4

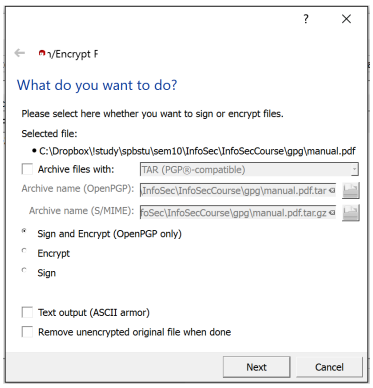

Figure 3: Файл для подписи

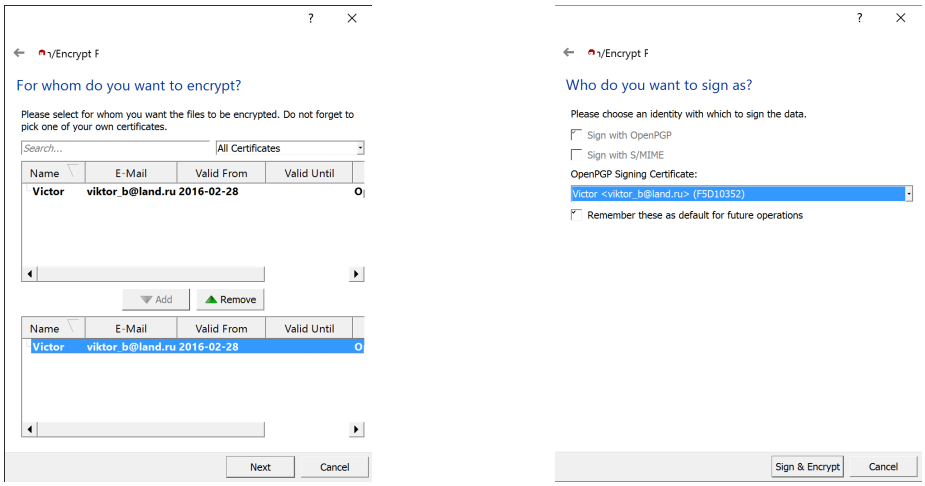

Figure 4: Выбор сертификатов

2.4 Работа с GPG средствами командной строки

Операции, проделанные с помощью графического интерфейса Kleopatra, можно повторить использую лишь консоль.
Создание нового ключа производится с помощью команды (Рисунок 5, 6)

```
gpg --gen-key
```

Для просмотра имеющихся в системе ключей необходимо воспользоваться командой (список ключей отображен на Рисунке 7)

```
gpg --list-keys
```

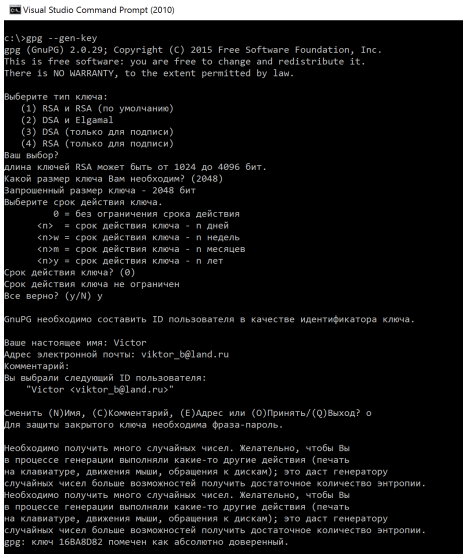

Figure 5: Создание ключа.

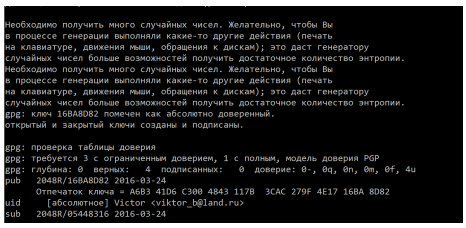

Figure 6: Создание ключа.

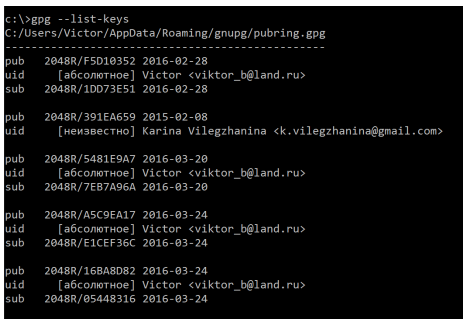

Figure 7: Список ключей.

Экспорт ключей возможен с помощью команды

`gpg --export`

с различными опциями (например, вывод в файл, вид представления, выбор

ключа для экспорта).
Для импорта

```
gpg --import Имя_файла
```

3 Вывод

В ходе работы было изучено средство GPG, позволяющее шифровать и подписывать файлы, проверять электронную подпись