

GnuPG

Виктор БОРИСОВ

May 30, 2016

Contents

1	Цель работы	3
2	Ход работы	3
2.1	Клеопатра	3
2.2	Экспорт сертификата	3
2.3	ЭЦП	4
2.4	Работа с GPG средствами командной строки	4
3	Вывод	7

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

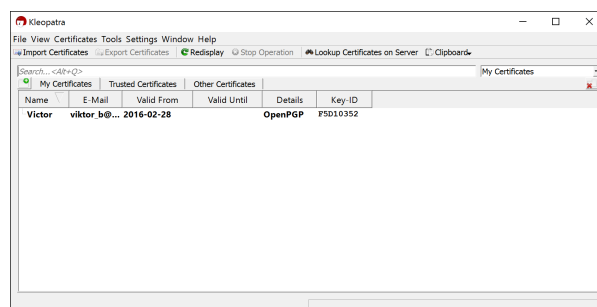


Figure 1: Пользовательский интерфейс Kleopatra.

2.2 Экспорт сертификата

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

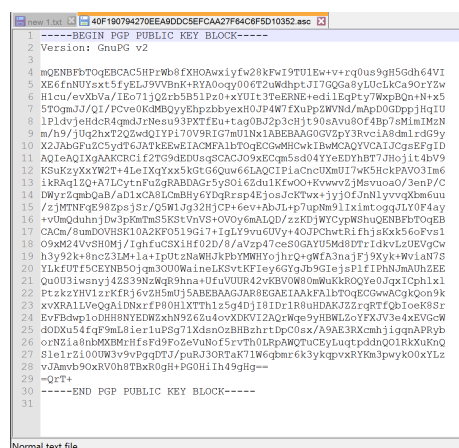


Figure 2: Экспорт сертификата.

2.3 ЭЦП

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

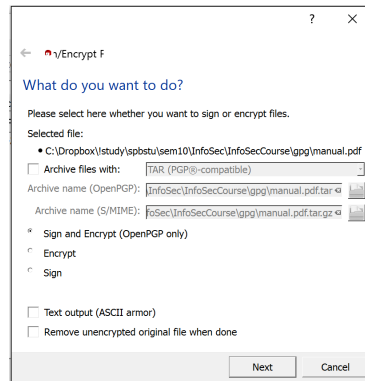


Figure 3: Файл для подписи

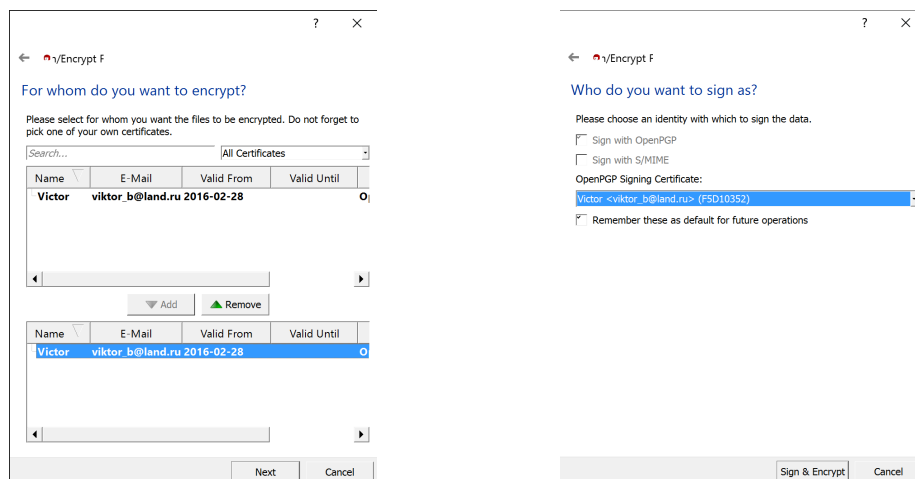


Figure 4: Выбор сертификатов

2.4 Работа с GPG средствами командной строки

Операции, проделанные с помощью графического интерфейса Kleopatra, можно повторить используя 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
```

```
Visual Studio Command Prompt (2010)

c:\>gpg --gen-key
gpg (GnuPG) 2.0.23; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Выберите тип ключа:
  (1) RSA и RSA (по умолчанию)
  (2) DSA и Elgamal
  (3) DSA (только для подписи)
  (4) RSA (только для подписи)
Ваш выбор?
длина ключей RSA может быть от 1024 до 4096 бит.
Какой размер ключа Вам необходим? (2048)
Запрещенный размер ключа - 2048 бит
Выберите срок действия ключа.
  0 = без ограничения срока действия
  <n> = срок действия ключа - n дней
  <n>w = срок действия ключа - n недель
  <n>m = срок действия ключа - n месяцев
  <n>y = срок действия ключа - n лет
Срок действия ключа? (0)
Срок действия ключа не ограничен
Все верно? (y/N) y

GnuPG необходимо составить ID пользователя в качестве идентификатора ключа.

Ваше настоящее имя: Victor
Адрес электронной почты: viktor_b@land.ru
Комментарий:
Вы выбрали следующий ID пользователя:
  "Victor <viktor_b@land.ru>"

Сменить (N)Имя, (C)Комментарий, (E)Адрес или (O)Принять/(Q)Выход? o
Для защиты закрытого ключа необходима фраза-пароль.

Необходимо получить много случайных чисел. Желательно, чтобы Вы
в процессе генерации выполняли какие-то другие действия (печатать
на клавиатуре, движения мыши, обращения к дискам); это даст генератору
случайных чисел больше возможностей получить достаточное количество энтропии.
Необходимо получить много случайных чисел. Желательно, чтобы Вы
в процессе генерации выполняли какие-то другие действия (печатать
на клавиатуре, движения мыши, обращения к дискам); это даст генератору
случайных чисел больше возможностей получить достаточное количество энтропии.
gpg: ключ 16BA8D82 помечен как абсолютно доверенный.
```

Figure 5: Создание ключа.

```
Необходимо получить много случайных чисел. Желательно, чтобы Вы
в процессе генерации выполняли какие-то другие действия (печатать
на клавиатуре, движения мыши, обращения к дискам); это даст генератору
случайных чисел больше возможностей получить достаточное количество энтропии.
Необходимо получить много случайных чисел. Желательно, чтобы Вы
в процессе генерации выполняли какие-то другие действия (печатать
на клавиатуре, движения мыши, обращения к дискам); это даст генератору
случайных чисел больше возможностей получить достаточное количество энтропии.
gpg: ключ 16BA8D82 помечен как абсолютно доверенный.
открытый и закрытый ключи созданы и подписаны.

gpg: проверка таблицы доверия
gpg: требуется 3 с ограниченным доверием, 1 с полным, модель доверия PGP
gpg: глубина: 0 верных: 4 подписанных: 0 доверие: 0-, 0q, 0n, 0u, 0f, 4u
pub 2048R/16BA8D82 2016-03-24
Отпечаток ключа = A6B3 41D6 C300 4843 1178 3C4C 279F 4E17 16BA 8D82
uid [абсолютное] Victor <viktor_b@land.ru>
sub 2048R/95448316 2016-03-24
```

Figure 6: Создание ключа.

```
c:\>gpg --list-keys
C:/Users/Victor/AppData/Roaming/gnupg/pubring.gpg
-----
pub 2048R/F5D10352 2016-02-28
uid [абсолютное] Victor <viktor_b@land.ru>
sub 2048R/10D73E51 2016-02-28

pub 2048R/391EA659 2015-02-08
uid [неизвестно] Karina Vilegzhanina <k.vilegzhanina@gmail.com>

pub 2048R/5481E9A7 2016-03-20
uid [абсолютное] Victor <viktor_b@land.ru>
sub 2048R/7E87A96A 2016-03-20

pub 2048R/A5C9EA17 2016-03-24
uid [абсолютное] Victor <viktor_b@land.ru>
sub 2048R/E1CEF36C 2016-03-24

pub 2048R/16BA8D82 2016-03-24
uid [абсолютное] Victor <viktor_b@land.ru>
sub 2048R/95448316 2016-03-24
```

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