Лабораторная работа №3. Программа для шифрования и подписи GPG, пакет Gpg4win

Климов Сергей

21 марта 2016 г.

Оглавление

1 Цель работы

Научиться создавать сертификаты, шифровать файлы и ставить ЭЦП.

2 Описание работы

Цифровой сертификат – это электронный документ, который выдается и заверяется Центром Сертификации (ЦС). Для заверения электронного сертификата используется электронная цифровая подпись доверенного центра, т.е. Центра Сертификации. Цифровой сертификат выдается физическому лицу, который является владельцем закрытого ключа электронной цифровой записи (шифрования), который соответствует открытому ключу. Цифровой сертификат содержит следующую информацию: имя и идентификатор владельца сертификата, открытый ключ подписи, имя, идентификатор и цифровую подпись Центра Сертификации, серийный номер, версию и срок действия сертификата. Владелец сертификата может быть уверен, что информация, которая передается им электронным способом, не будет прочитана, похищена или подменена во время ее передачи через интернет. securitylab.ru

Шифрование – метод, используемый для преобразования данных в шифрованный текст для того, чтобы они были прочитаны только пользователем, обладающим соответствующим ключом шифрования для расшифровки содержимого. Шифрование используется тогда, когда требуется повышенный уровень защиты данных - при хранении данных в ненадежных источниках или передачи данных по незащищенным каналам связи. В зависимости от структуры используемых ключей, среди методов шифрования выделяют симметричное шифрование и асимметричное шифрование. Симметричное шифрование предусматривает доступность алгоритма шифрования посторонним лицам, однако ключ (одинаковый для отправителя и получателя) остается неизвестным. При ассиметричном шифровании посторонним лицам известен алгоритм шифрования и открытый ключ, однако закрытый ключ известный только получателю. securitylab.ru

Электронная цифровая подпись (ЭЦП) - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе, а также обеспечивает неотказуемость подписавшегося. russika.ru

При выполнении лабораторной работы для создания сертификатов, шифрования и создания ЭЦП используется пакет Gpg4win. Он включает в себя:

- версию GnuPG — свободная программа для шифрования информации и создания электронных цифровых подписей;
- Kleopatra (менеджер сертификатов для OpenPGP и X.509);
- GPA (альтернативный менеджер сертификатов (GNU) для OpenPGP и X.509);

- другие компоненты.

3 Ход работы

Для работы будем использовать графическую оболочку **"Kleopatra"**.

3.1 Создание ключевой пары openPGP

Для создания новой ключевой пары OpenPGP была выполнена команда *"File -> New Certificate"*. После чего была введена персональная информация: имя сертификата, адрес электронной почты пользователя.

После этого созданный сертификат был импортирован в рафическую оболочку **"Kleopatra"** (рисунок 1).

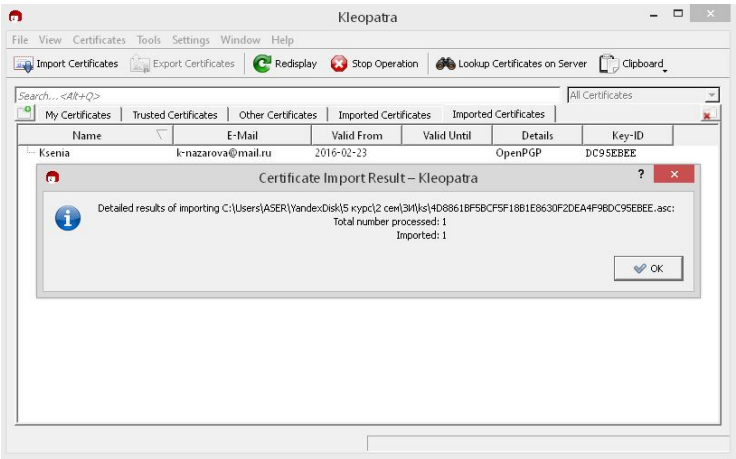

Рис. 1: Окно для ввода персональных данных.

3.2 Экспорт сертификата

Для экспорта сертификата выполним команду *"File -> Export Certificate"*.

3.3 Поставить ЭЦП на файл

Для того, что бы поставить ЭЦП на файл была выполнена команда *"File -> Sign/Encrypt Files"*, затем был выбран файл, на который необходимо поставить ЭЦП.

После выберем одно из трех предложенных действий.

- Sign and Encrypt
- Encrypt
- Sign

Был выбран пункт *Sign and Encrypt* - создание цифровой подписи и шифрование файла (рисунок 2).

Был выбран открытый ключ получателя (рисунок 3).

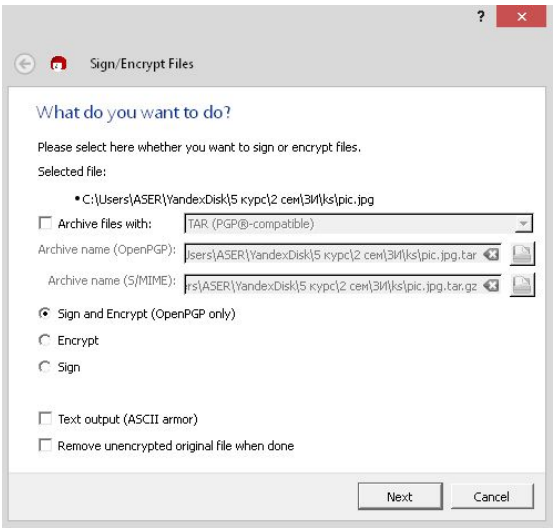

Рис. 2: Поставить ЭЦП на файл и зашфровать

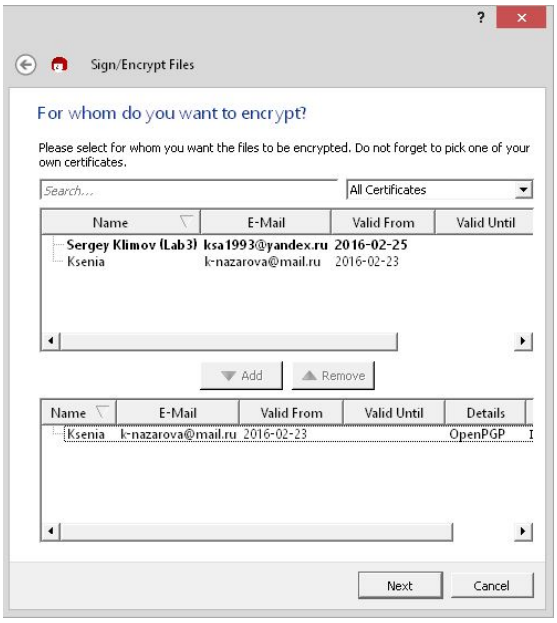

Рис. 3: Выбор открытого ключа получателя

Был выбран стандарт OpenPGP для подписи и сертификат, созданный ранее (рисунок 4).

После ввода пароля выводится сообщение об успешном создании подписи

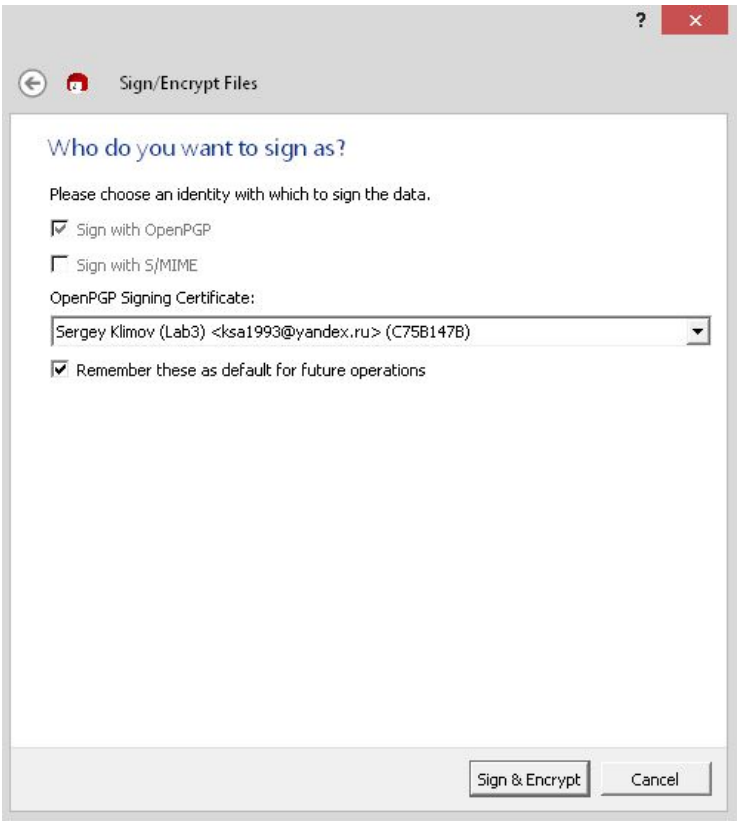

Рис. 4: Выбор стандарта OpenPGP и сертификата для ЭЦП

на файл (рисунок 5).

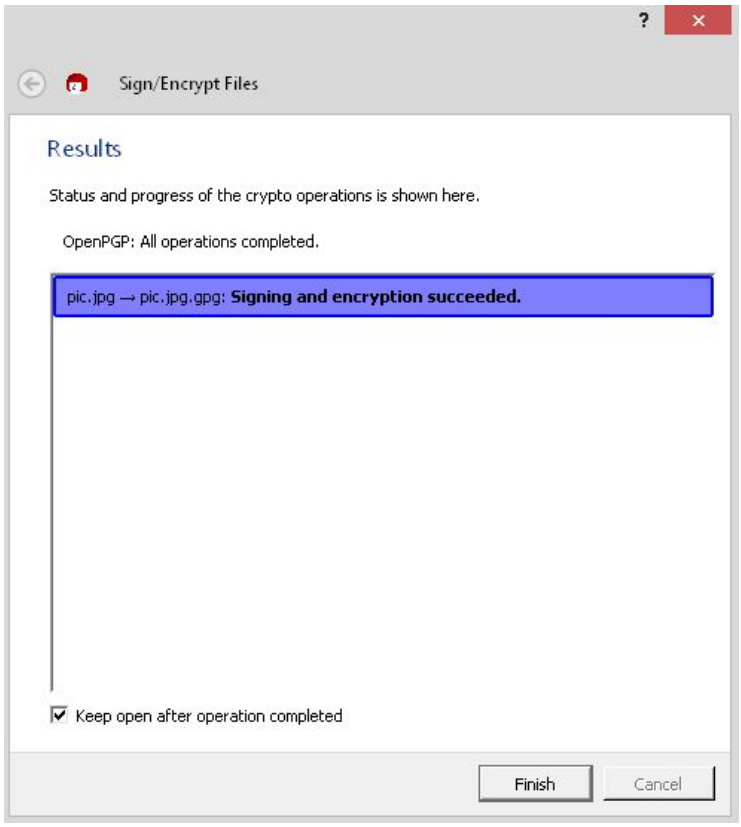

Рис. 5: Успешная подпись файла

3.4 Работа с чужим сертификатом

Был импортирован сторонний сертификат, после этого с его помощью был зашифрован и подписан документ *pic.jpg*. Далее зашифрованный файл *pic.jpg.gpg* был отправлен коллеге для расшифровки.
Далее от коллеги был получен файл *hello.txt.gpg*, который был подписан при помощи моего открытого ключа. Затем командой *File -> Decrypt/Verify Files* расшифруем документ (рисунок 6).

После ввода пароля видим окно с сообщением об удачном расшифровании файла (рисунок 7), также появился файл *hello.txt*, который можно прочитать.

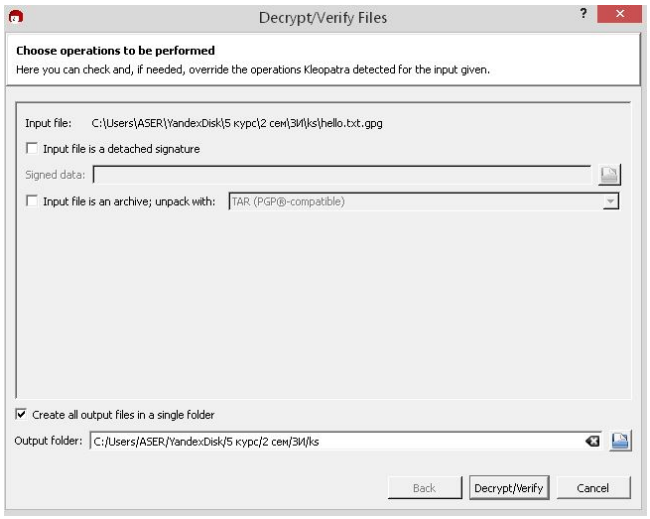

Рис. 6: Расшифровка файла

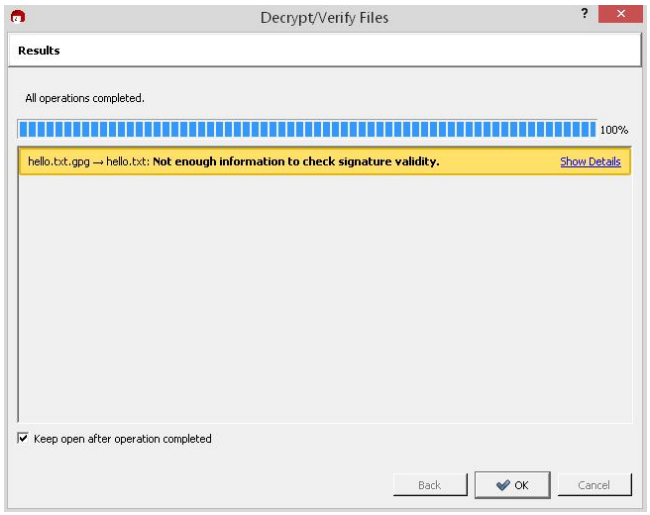

Рис. 7: Успешное расшифрование файла

3.5 Использование GNU Privacy handbook

С помощью GNU Privacy handbook проделаем некоторые действия по использованию gpg через командную строку.
Для создания ключевой пары введем в консоле команду *gpg –gen-key*. Далее выберем тип ключа, его размер, срок действия, укажем ID пользователя, электронную почту, введем пароль, после чего создастся ключевая пара.
Был создан ключ типа RSA, размером 2048, с неограниченным сроком действия (рисунок 8).

Рис. 8: Создание сертификата

Выведем список всех ключей командой *gpg –list-keys* (рисунок 9). Подпишем файл *pic.jpg* (рисунок 10).

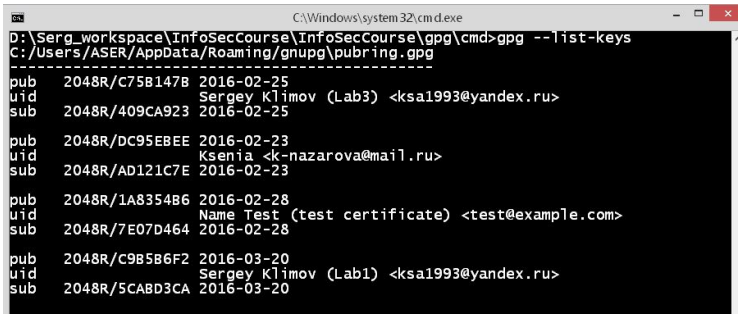

Рис. 9: Список сертификатов

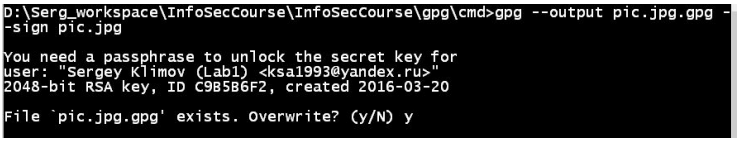

Рис. 10: Создание сертификата

Выведем на консоль содеожимое файла сертификата (рисунок 11).

Рис. 11: Содержимое файла сертификата

4 Вывод

В результате выполнения лабораторной работы был изучен пакет Gpg4win. Были получены практические навыки создания ключевых пар, подписи, шифрования и дешифрования файлов при помощи графической оболчки **Kleopatra**, а также при помощи консольной утилиты **gpg**.