Импорт и экспорт ключей
Цифровая подпись

Экспорт открытого ключа

Для того, чтобы нам могли шифровать файлы/сообщения, а также проверять наши подписи, мы должны экспортировать свой открытый ключ в файл, (либо на ключевой сервер).
Экспорт открытого ключа в текстовый файл:
gpg2 --export --armor 29FEB0EF > mykey.asc
Здесь **0x**29FEB0EF — отпечаток ключа нашей ключевой пары, открытый ключ которой экспортируем,
а mykey.asc — имя файла, в который будет сохранён результат.

Создание электронной цифровой подписи (ЭЦП) файла

GnuPG позволяет использовать несколько типов подписей:

- встроенная в файл:

содержимое файла изменяется так, чтобы в него была добавлена ЭЦП. Чаще всего применяется при отправке подписанных сообщений по электронной почте;

- отсоединённая в текстовом формате:

создаётся файл с расширением *.asc вида mydocument.pdf.asc (где mydocument.pdf — имя оригинального файла);

- отсоединённая в двоичном формате:

создаётся файл с расширением *.sig вида mydocument.pdf.sig в бинарном формате.
Для создания ЭЦП файла используется закрытый ключ из нашей ключевой пары, а для проверки — открытый.
Создадим отсоединённую ЭЦП файла mydocument.pdf в текст. формате:
gpg2 --sign --detach-sign --default-key 29FEB0EF --armor mydocument.pdf
Создадим отсоединённую подпись в двоичном формате:
gpg2 --sign --detach-sign --default-key 29FEB0EF mydocument.pdf
на выходе будет получен файл mydocument.pdf.sig
Создадим встроенную в файл подпись в текстовом формате:
gpg2 --sign --default-key 29FEB0EF --armor mydocument.pdf
Создадим встроенную в файл подпись в двоичном формате:
gpg2 --sign --default-key 29FEB0EF mydocument.pdf
При создании встроенных подписей содержимое файла-источника целиком включается внутрь, поэтому использовать данный формат не желательно из-за дублирования и значительного размера. Поэтому отсоединённая ЭЦП является самым популярным вариантом подписи.

Импорт открытого ключа

Для проверки чужой цифровой подписи GnuPG, у нас должны быть:

1. открытый ключ человека, который её создал;
2. оригинальный файл и файл отсоединённой цифровой подписи.

Сначала импортируем ключ респондента, подписавшего файл (если это не было сделано ранее). Это можно сделать любым способом:

- текстовый файл;
- серверы-хранилища ключей;
- буфер обмена (для GUI утилит).

Импортируем открытый ключ из файла:
gpg2 --import mykey.asc
Здесь mykey.asc — имя файла с открытым ключом.
Теперь мы должны установить доверие импортированному ключу, т.к. в противном случае не сможем проверить подпись. Войдём в интерактивный режим:
pg2 --edit-key 29FEB0EF

Установим доверие ключу:
trust
Проверим отпечаток респондента (например посредством телефонного звонка или любым другим способом), затем выберем пункт
Я полностью доверяю (***I trust fully***).

Выходим из интерактивного режима:
quit

Проверка ЭЦП

Файл отсоединённой ЭЦП должен лежать в том же каталоге, что и оригинальный файл, иначе выполнить проверку его подлинности будет невозможно.
Проверка отсоединённой подписи файла:
gpg2 --verify mydocument.pdf.sig

Экспорт/импорт на ключевые сервера

Изучите вопросы экспорта (и импорта) ключей и их связок на ключевые сервера, реализуйте данные способы экспорта/импорта на выбранный сервер, отобразив результаты в отчете .

По возможности, также, опробуйте встраивание средств GnuPG в какую-либо среду коммуникаций, например, в почтовый клиент Thunderbird или др.