gpg

tags `gpg` `secure` `keys` `keyserver`
date 2020-10-31 00:17

> GPG (также известный как GnuPG) создавался как свободная альтернатива несвободному PGP. GPG используется для шифрования информации и предоставляет различные алгоритмы (RSA, DSA, AES и др.) для решения этой задачи.

Генерация ключа

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

Экспорт ключа

```
gpg --export-secret-keys >~/.gnupg/secring.gpg
```

Просмотр ключей

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

Экспорт ключа на сервер

```
gpg --keyserver certserver.pgp.com --recv-key
418AB804154FA73EE5F74374F8E83547B8A3FA10
```

Basic commands

Public keys

```
gpg -k
```

Private keys

```
gpg -K
```

Sign

```
gpg --clearsign 1.txt
```

Encrypt

```
gpg -r johenews --armor --encrypt 1.txt
```

Decrypt

```
gpg -d 1.txt.asc
```

Examples

```
gpg -a -r 0x12345678 -e decrypted.txt > encrypted.gpg
```

Зашифровать файл decrypted.txt в файл encrypted.gpg ключом 0x12345678. При этом готовый файл будет текстовым, а не бинарным.

```
gpg -r 0x12345678 -d encrypted.gpg > decrypted.txt
```

Расшифровать файл encrypted.gpg ключом 0x12345678 и сохранить его в файл decrypted.txt.

```
gpg -u 0x12345678 -s message.txt > sign.asc
```

Подписать файл message ключом 0x12345678 и сохранить подпись в файл sign.asc.

```
gpg -r 0x12345678 --clearsign message.txt > message.gpg
```

Подписать файл message.txt ключом 0x12345678 и записать сообщение с подписью в файл message.gpg.

```
gpg --verify message.asc message.txt
```

Проверить подпись файла message.txt, которая записана в файле message.asc.

```
gpg --import pubkey.gpg
```

Импортировать публичный ключ из файла pubkey.gpg.

Commands

Keys

```
gpg --expert --edit-key johenews
```

- addkey
- save

Backup secret

```
gpg -a --export-secret-key johenews > secret_key
```

Revocation

```
gpg -a --gen-revoke johenews > revocation_cert.gpg
```

Export public

```
gpg -a --export johenews > public_key.gpg
```

Export subkeys

```
gpg -a --export-secret-subkeys johenews > secret_subs.gpg
```

Remove secret

```
gpg --delete-secret-keys johenews
```

Import priv subkeys

```
gpg --import secret_subs.gpg
```

Server GPG

Отправить публичный ключ на сервер

```
gpg --keyserver <URL> --send-keys <KeyID>
```

Получить публичный ключ с идентификатором ключа с сервера

```
gpg --keyserver <URL> --recv-keys <KeyID>
```

Получить обновления ключей с сервера

```
gpg --keyserver <URL> --refresh-keys
```

Найти ключ на сервере

```
gpg --keyserver <URL> --search-keys <UID или KeyID>
```

Для удобства можно прописать адрес сервера ключей в gpg.conf, чтобы не прописывать его в командах

```
keyserver <URL>
```

Сервера ключей

```
pgp.mit.edu
keyserver.pgp.com
```

Vocabulary

rsa — Алгоритм шифрования RSA.
2048 — Длина ключа.
1970-01-01 — Дата создания ключа.
2BB680...E426AC — Отпечаток ключа. Его следует сверять при импортировании чужого публичного ключа — у обоих сторон он должен быть одинаков.
uid — Идентификатор (User-ID).
pub и sub — Типы ключа:

pub — Публичный ключ.
sub — Публичный подключ.
sec — Секретный ключ.
ssb — Секретный подключ.

[SC] и [E] — Предназначение каждого ключа. Когда вы создаёте ключ, вы получаете аж 4 криптоключа: для шифрования, расшифровки, подписи и проверки подписи:

S — Подпись (Signing).
C — Подпись ключа (Certification). Об этом пойдёт речь чуть позже.
E — Шифрование (Encryption).
A — Авторизация (Authentication). Может использоваться, например, в SSH.