



Глава 1. Верификация цифровой подписи Tor Browser

1.1. Подписи OpenPGP

1.2. Установка GnuPG

1.3. Импорт ключа разработчиков Tor

1.4. Верификация подписи

1.5. Обновление PGP-ключа

1.6. Альтернативные методы

Глава 1. Верификация цифровой подписи Tor Browser

1.1. Подписи OpenPGP

В этой инструкции описано, как удостовериться в подлинности скачанного Tor Browser с помощью цифровой подписи. Цифровая подпись гарантирует, что файл исходит от указанных разработчиков и не подвергался изменениям со стороны третьих лиц.

- На странице загрузки каждому файлу соответствует одноимённая ему подпись в расширении `.asc` (например, файлу `torbrowser-install-win64-12.5_ALL.exe` соответствует файл подписи `torbrowser-install-win64-12.5_ALL.exe.asc`). Файлы `.asc` представляют собой подписи OpenPGP, подтверждающие аутентичность файла. **Обратите внимание:** до верификации датировка файла подписи должна совпадать с датировкой удостоверяемого ею файла. Для загрузки файла подписи кликните на него правой кнопкой мыши, нажмите **"Сохранить как"** и выберите папку **"Загрузки"** ("Downloads").

Далее описан процесс проверки цифровой подписи в зависимости от вашей операционной системы. Обратите внимание, что имена файлов в инструкции даны условные.

1.2. Установка GnuPG

Для верификации подписей необходимо установить программное обеспечение GnuPG.

- **Windows:** скачайте и установите [Gpg4win](#). Для верификации подписи введите указанные далее команды в командную строку (cmd.exe).
- **MacOS:** скачайте и установите [GPGTools](#). Для верификации подписи введите указанные далее команды в терминал.
- **GNU/Linux:** на большинстве дистрибутивов GnuPG предустановлен. Для верификации подписи введите указанные далее команды в терминал.

1.3. Импорт ключа разработчиков Tor

Новые версии Tor Browser подписаны **ключом разработчиков** (0xEF6E286DDA85EA2A4BA7DE684E2C6E8793298290). Его необходимо импортировать.

- Введите команду:

```
gpg --auto-key-locate nodefault,wkd --locate-keys torbrowser@torproject.org
```

В случае успешного импорта ключа вы увидите следующее сообщение:

```
gpg: key 4E2C6E8793298290: public key "Tor Browser Developers (signing key) <torbrowser@torproject.org>" imported
gpg: Total number processed: 1
gpg:             imported: 1
pub   rsa4096 2014-12-15 [C] [expires: 2025-07-21]
      EF6E286DDA85EA2A4BA7DE684E2C6E8793298290
```

```
uid      [ unknown] Tor Browser Developers (signing key) <torbrowser@torproject.org>
sub      rsa4096 2018-05-26 [S] [expires: 2020-12-19]
```

- В случае возникновения ошибки попробуйте импортировать ключ способом, описанным в разделе [1.6](#).
- После импорта ключа вы можете сохранить его в файл (для идентификации служит отпечаток) командой:

```
gpg --output ./tor.keyring --export 0xEF6E286DDA85EA2A4BA7DE684E2C6E8793298290
```

- Убедитесь, что файл ключа успешно сохранён в текущей папке `./tor.keyring`.

1.4. Верификация подписи

После загрузки файла и соответствующего .asc-файла подписи выполните соответствующую вашей системе команду для верификации подписи.

- **Windows:**

```
gpgv --keyring .\tor.keyring Downloads\torbrowser-install-win64-12.5_ALL.exe.asc Downloads\torbrowser-install-win64-12.5_ALL.exe
```

- **macOS:**

```
gpgv --keyring ./tor.keyring ~/Downloads/TorBrowser-12.5-macos_ALL.dmg.asc ~/Downloads/TorBrowser-12.5-macos_ALL.dmg.dmg
```

- **GNU/Linux:**

```
gpgv --keyring ./tor.keyring ~/Downloads/tor-browser-linux64-12.5_ALL.tar.xz.asc ~/Downloads/tor-browser-linux64-12.0.7_ALL.tar.xz
```

В случае успешной верификации подписи вы увидите следующее сообщение:

```
gpgv: Good signature from "Tor Browser Developers (signing key) <torbrowser@torproject.org>"
```

- Если произошла ошибка и появляется сообщение **"No such file or directory"**, убедитесь в правильности написания имён файлов или в корректности импорта ключа разработчиков в предыдущих шагах.

1.5. Обновление PGP-ключа

Вы можете обновить ваш локальный ключ разработчиков с сервера ключей, а также получить новые сабключи.

- Введите следующую команду:

```
gpg --refresh-keys EF6E286DDA85EA2A4BA7DE684E2C6E8793298290
```

1.6. Альтернативные методы

- Если вам не удалось верифицировать ключ разработчиков указанным в инструкции способом, вы можете использовать [открытый ключ разработчиков](#) Tor Browser по ссылке или ввести следующую команду:

```
curl -s https://openpgpkey.torproject.org/.well-known/openpgpkey/torproject.org/hu/kounek7zrdx745qydx6p59t9mqjpuhdf |gpg --import -
```

- Открытые ключи разработчиков также доступны на сайте keys.openpgp.org: <https://keys.openpgp.org/vks/v1/by-fingerprint/EF6E286DDA85EA2A4BA7DE684E2C6E8793298290>.

Если вы используете MacOS или GNU/Linux, введите команду:

```
gpg --keyserver keys.openpgp.org --search-keys EF6E286DDA85EA2A4BA7DE684E2C6E8793298290
```