

# GnuPG

Stefan Hornburg (Racke)



# Contents

- Commands** **3**
- Show public keys . . . . . 3
- Export public key . . . . . 3
- Import public key . . . . . 3
- Show keys in a keyring . . . . . 3
  
- Files** **4**
  
- Agent** **5**
- Show socket locations . . . . . 5
- Forwarding . . . . . 5
  - Setup on the remote server . . . . . 5
  - Setup on the local machine . . . . . 5

# Commands

## Show public keys

```
$ gpg --list-keys  
/home/racke/.gnupg/pubring.kbx  
-----  
pub   rsa4096 2015-03-07 [SC]  
      D6814975A277774C98D0DFEF5B93015BFA2720F8  
uid     [ unknown] Stefan Hornburg (Racke) <racke@linuxia.de>  
sub   rsa4096 2015-03-07 [E]
```

## Export public key

```
$ gpg --armor --export racke@linuxia.de > racke.asc
```

## Import public key

```
$ gpg --import racke.asc  
gpg: key 5B93015BFA2720F8: public key "Stefan Hornburg (Racke) <racke@linuxia.de>" imported  
gpg: Total number processed: 1  
gpg:          imported: 1
```

## Show keys in a keyring

```
$ gpg --no-default-keyring --keyring /usr/share/keyrings/runner_gitlab-runner-archive-keyring.gpg --  
gpg: /home/vagrant/.gnupg/trustdb.gpg: trustdb created  
/usr/share/keyrings/runner_gitlab-runner-archive-keyring.gpg  
-----  
pub   rsa4096 2020-03-02 [SC] [expires: 2024-03-01]  
      F6403F6544A38863DAA0B6E03F01618A51312F3F  
uid     [ unknown] GitLab B.V. (package repository signing key) <packages@gitlab.com>  
sub   rsa4096 2020-03-02 [E] [expires: 2024-03-01]
```

# Files

Encrypt file for another person:

```
$ gpg --encrypt --sign --armor -r beta@example.com secrets.txt
```

# Agent

## Show socket locations

```
$ gpgconf --list-dir agent-socket  
/run/user/1000/gnupg/S.gpg-agent  
$ gpgconf --list-dir agent-extra-socket  
/run/user/1000/gnupg/S.gpg-agent.extra
```

## Forwarding

GnuPG agent forwarding is similar to SSH forwarding and allows to use your private key on remote servers.

Typical use cases are signing Git commits or Debian packages.

## Setup on the remote server

Ensure that GnuPG is installed on the remote server.

Import your public key as shown above.

You also need to prevent that GnuPG starts the agent when you use it on the remote host. This can be done by disabling agent autostart in (`~/.gnupg/gpg.conf`) on the remote server:

```
# prevent start of local GnuPG agent  
no-autostart
```

## Setup on the local machine

The forwarding is configured in SSH configuration file (`~/.ssh/config`):

```
Host build.linuxia.de  
RemoteForward /run/user/1000/gnupg/S.gpg-agent /run/user/1000/gnupg/S.gpg-agent.extra
```

The *RemoteForward* directive specifies the remote socket and the local (extra) socket.

Linuxia Wiki

Stefan Hornburg (Racke)  
GnuPG

**wiki.linuxia.de**