My Keys

tropf

ABSTRACT

list of my keys and short usage

1. My Keys

I use SSH keys to sign stuff if I need to. The following keys are mine:

Name	Note	Valid Since	Link	Full Text
`tropf.pub`	default key	2025	download ⟨`../blob/tropf.pub`⟩	
`tropf_secondary.pub`	backup key	2025	download ⟨`../blob/tropf_secondary.pub`⟩	

By default, you will encounter `tropf.pub`; however in case I ever lose it the backup key is equally valid as a replacement.

1.1. Cross-signed

This table lists signatures of keys on each other. Download the signatures using the links in the table, the referenced keys can be retrieved above. Additional keys may appear here to establish their authenticity.

Signing Key	Signed Key	Signature
`tropf.pub`	`tropf_secondary.pub`	`tropf_secondary.pub.sig` ⟨`../blob/tropf_secondary.pub.sig`⟩
`tropf_secondary.pub`	`tropf.pub`	`tropf.pub.sig` ⟨`../blob/tropf.pub.sig`⟩

2. Usage

2.1. Signing

To sign a file `FILE` with the SSH key `KEY` use the following command:

```
ssh-keygen -Y sign -f KEY -n file FILE
```

The result will be written into `file.name.sig`.

› The argument `file` is the so-called "namespace". It is hard-coded and does not refer to any specific file.

2.2. Verifying Signatures

Use this command to validate that the public key `KEY.pub` created the signature `FILE.sig` for the file `FILE`:

```
ssh-keygen -Y check-novalidate -f KEY.pub -n file -s FILE.sig < FILE
```

There are two commands in `ssh-keygen` to check signatures. As `verify` requires a key database (an extra file with its own format) prefer `check-novalidate` which only validates a signature against exactly one key.

3. See also

- **ssh-keygen**(1): Tool to create and check signatures
- cheat sheet for FIDO2 SSH key generation ⟨`https://gist.github.com/Kranzes/be4fffba5da3799ee93134dc68a4c67b`⟩