SSH

Links

- Simplified Guide: Secure Shell (SSH)
- Wikibooks: SSH Multiplexing
- Debian Forum: X-Anwendungen mit SSH forwarden
- stribika: Secure Secure Shell (or how to make SSH secure)
- Stack Exchange: Does getting disconnected from an SSH session kill your programs?
- Ryan Lue: Using a GPG key for SSH Authentication
- ArchWiki SSH-Authentifizierung mit Schlüsselpaaren
- *OpenBSD* Manual Page: ssh_config - OpenSSH SSH client configuration files
- *OpenBSD* Manual Page: sshd_config - OpenSSH SSH daemon configuration file

Commands

- generate a SSH key:[1] `ssh-keygen -t rsa -b 4096 -C "user@domain"`
- change the private key passphrase: `ssh-keygen -p -f ~/.ssh/id_rsa`
- show (own) SSH public key fingerprint: `ssh-keygen -l`
- publish (own) SSH public key to user@server:[2] `ssh-copy-id -f -i ~/.ssh/id_rsa.pub user@server`
- list public key(s) of known host/server: `ssh-keygen -F <host> -l`
- list hashes of **all** known host/server: `ssh-keygen -l -f ~/.ssh/known_hosts`
- remove key of host/server from *known_hosts* file: `ssh-keygen -R <host>`
- show certificate information directly from server/host: `ssh-keyscan <host>`
- X11 forwarding: `ssh -x user@domain`



On a SSH server you should add this firewall rule (for example using the Uncomplicated Firewall):

```
sudo ufw allow proto tcp from 192.168.178.0/24 to any port 22
```

or simply (allow from everywhere):

```
sudo ufw allow ssh; sudo ufw reload
```

Files

- `~/.ssh/config`: client configuration (possibly different from server to server, see *Linux* manual page ssh_config(5))
- `~/.ssh/known_hosts`: known host(s) public key fingerprint (SSH will never ask you again, to accept the associated public key when SSL/TLS session key agreement is running)

- `~/.ssh/id_rsa.pub`: RSA public key[3)]
- `~/.ssh/id_dsa.pub`: DSA public key[4)]
- `~/.ssh/id_ecdsa.pub`: ECDSA public key
- `~/.ssh/id_ed25519.pub`: (Bernstein) Curve *ed25519* public key
- `~/.ssh/id_rsa`: RSA private key

Example

See below for a `~/.ssh/config` example, which uses client keep-alive and connection multiplexing (for a particular host).

```
Host <name>
    HostName <host>
    IdentityFile ~/.ssh/id_rsa
    User <user>
    EscapeChar none
# multiplexing
    ControlPath ~/.ssh/controlmasters/%r@%h:%p
    ControlMaster auto
    ControlPersist 3h
# keep-alive
    TCPKeepAlive yes
    ServerAliveInterval 15
    ServerAliveCountMax 4
```

1)
This can be performed with *seahorse* too.
2)
Finally places the contents of `id_rsa.pub` into file `~/.ssh/authorized_keys`.
3)
Add this content at server side to (a single line of) `~/.ssh/authorized_keys`!
4)
DSA is deprecated.

From:
https://wiki.rho62.de/ - **rho62 Wiki**

Permanent link:
https://wiki.rho62.de/doku.php?id=linux:utilities:ssh

Last update: **2026/09/09 14:43**