

# ssh-keygen generating an elliptic key

---

```
$ ssh-keygen -a 256 -t ed25519 ❶ -C "$(hostname) - $(date +%d-%m-%Y)"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/foo/.ssh/id_ed25519):
Created directory '/home/foo/.ssh'.
Enter passphrase (empty for no passphrase): ❷
Enter same passphrase again:
Your identification has been saved in /home/foo/.ssh/id_ed25519 ❸
Your public key has been saved in /home/foo/.ssh/id_ed25519.pub ❹
...
```

# Result of ssh-keygen execution

---

```
~/ssh$ cd ~/.ssh
/home/foom/.ssh cp id_ed25519.pub authorized_keys
mi student@w10m ~/.ssh$ ls -al
total 24
drwxrwx---+ 2 student mi 0 Oct 17 17:45 .
drwx-----+ 32 student mi 0 Oct 17 17:44 ..
-rwxrwx---+ 1 student mi 396 Oct 17 17:45 authorized_keys ❶
-rwxrwx---+ 1 student mi 1675 Oct 17 17:38 id_ed25519 ❷
-rwxrwx---+ 1 student mi 396 Oct 17 17:38 id_ed25519.pub ❸
```

- ❶ Allowed keys to log on to current machine.
- ❷ Private key
- ❸ Corresponding public key

# Extended ACLs, ways too open

---

```
mi student@w10m ~/.ssh$ getfacl authorized_keys
# file: authorized_keys
# owner: mi student
# group: mi
user::rwx
user:mi student:rwx
group: ---
group: users: ---
mask: rwx
other: ---
```

# Revoking permissions using **setfacl**

---

```
foo@w10m ~/.ssh$ setfacl -m user:foo:--- authorized_keys
foo@w10m ~/.ssh$ setfacl -m user::rw authorized_keys
foo@w10m ~/.ssh$ getfacl authorized_keys
...
user::rw
user:foo:---
group:---
group:users:---
mask:---
other:---

foo@w10m ~/ssh$ ls -al authorized_keys
-rw-----+ 1 foo mi 396 Okt 17 17:45 authorized_keys
```

# Corrected permissions

---

```
foo@w10m ~/.ssh$ ls -al
total 32
drwx-----+  2 mi student mi      0 Okt 17 17:44 .
drwx-----+ 32 mi student mi      0 Okt 17 17:44 ..
-rw-----+   1 mi student mi 1132 Okt 17 17:40 authorized_keys
-rw-----+   1 mi student mi 1679 Okt 11 14:46 id_ed25519
-rw-r--r--+   1 mi student mi   396 Okt 11 14:46 id_ed25519.pub
-rw-----+   1 mi student mi   442 Okt 11 14:49 known_hosts
```

# Logging in

---

```
ssh root@sdi14a.mi.hdm-stuttgart.de
```

```
The authenticity of host 'sdi14a.mi.hdm-stuttgart.de (141.62.75.114)' can't be established.
```

```
ED25519 key fingerprint is SHA256:sEagSHefcv9CkiFi bKI ZFl PL/4FxbO+9kvJnwkV7l t U
```

```
This key is not known by any other names
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

```
Warning: Permanently added 'sdi14a.mi.hdm-stuttgart.de' (ED25519) to the list of known hosts.
```