Login mit einem ssh-Key

Manchmal hat man das starke Bedürfnis, sich per `ssh` an einem entfernten Rechner anzumelden, ohne jedes Mal das Passwort anzugeben. Das muss doch auch anders gehen... geht es auch: man benutzt die Authentifizierung durch einen selbst generierten SSH-Schlüssel.

Schlüssel erzeugen

Der Befehl (auf der Befehlszeile einzugeben) lautet beispielsweise

```
ssh-keygen -t rsa -f ~/.ssh/mein-neuer-key
```

Darauf antwortet die Software mit dem Generieren eines Schlüssels, was etwa so aussieht:

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/wflamme/.ssh/mein-neuer-key.
Your public key has been saved in /home/wflamme/.ssh/mein-neuer-key.pub.
The key fingerprint is:
67:d1:21:c2:18:66:30:fa:0a:bb:8c:35:ce:0d:9b:e9 flamme@klops
The key's randomart image is:
+--[ RSA 2048]----+
|    o.++. . .    |
|     =. .. o .   |
|.     .   . .    |
| *   .     .     |
|* . .   S o      |
|.+ .     o       |
|.E=              |
|oo o             |
|o.               |
+-----------------+
```

Ob da nun eine Passphrase eingegeben wird, ist jedem selbst überlassen. Ohne Passphrase geht das Anmelden schneller, aber der Schlüssel ist ungeschützt: jeder, der ihn erhält, kann sich damit identifizieren! Sicherer ist es deshalb, eine Passphrase zu verwenden – etwa nach den Vorschlägen von http://imgs.xkcd.com/comics/password_strength.png 🙂

Schlüssel verteilen

Um den Schlüssel einsetzen zu können, muss er auf dem entfernten Rechner in der Datei `~/.ssh/authorized_keys` des Remote-Nutzers vorkommen. Dazu gibt es umständliche und

einfache Methoden  . Aus Gründen der Bequemlichkeit nehme ich die einfache...

Wenn der entfernte Rechner `knurps.example.org` heißt und der Nutzer dort `ottokar`, kann man den Schlüssel mit dem folgenden Befehl übertragen:

```
ssh-copy-id -i ~/.ssh/mein-neuer-key ottokar@knurps.example.org
```

Bei dieser Übertragung muss man zum letzten Mail das Passwort eingeben:

```
Password:
Now try logging into the machine, with "ssh 'ottokar@knurps.example.org'",
and check in:

  ~/.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

Automatik

Damit dieser Key auch jedes Mal benutzt wird, kann man sich seine Datei `~/.ssh/config` entsprechend einrichten:

```
Host knurps.example.org
User ottokar
IdentityFile ~/.ssh/mein-neuer-key
```

Beim nächsten Mal muss man nur noch mit `ssh  knurps.example.org` eingeben, um sich auf der entfernten Maschine anzumelden.