Erledigt Schlüsselbund, Zertificate und SSH

Beitrag von „Griven“ vom 13. Mai 2014, 23:03

Nur, damit ich das verstehe du möchtest Dich über den SSH Client über einen Schlüssel, der auf Deinem USB Stick enthalten ist auf einem entfetten Rechner anmelden, richtig? Ich gehe davon aus, dass Du Dir ein Schlüsselpaar erstellt hast bestehend aus einen privaten und einem öffentlichen Key, richtig? Falls nicht kannst Du das erreichen indem Du wie folgt vorgehst:

1. Terminal öffnen
2. ssh-keygen eingeben und mit Enter bestätigen
3. den Anweisungen auf dem Bildschirm folgen

Wenn das erledigt ist geht es weiter mit der Konfiguration des entfernten Rechners, hierzu wird zunächst der öffentliche Schlüssel auf den entfernten Rechner hochgeladen.

Code

```
1. scp /Pfad/Auf/Dem/Stick/.ssh/id_rsa.pub DEINUSERNAME@ihrserver.de:authorized_keys
```

Ist der Key einmal hochgeladen meldest Du Dich einmalig via ssh mit Passwort Authorisation am Server an

Code

```
1. ssh -l user deinserver
```

und gehst dann im Falle eine Linux Servers wie folgt weiter vor:

1. Im Homeverzeichnis des Users, der sich automatisch mit dem Key einloggen können soll erstellen wir ein Verzeichnis

Code

```
1. mkdir -p .ssh
```

2. Als nächstes verschieben wir auf dem Server die Datei authorized_keys in den eben erstellten Ordner .ssh

Code

```
1. mv authorized_keys .ssh/authorized_keys
```

3. Jetzt noch die Berechtigungen richtig setzen

Code

```
1. chmod 600 .ssh/authorized_keys
```

und das war es schon. Haben wir alles richtig gemacht und der Stick ist gesteckt sollte ein

Code

```
1. ssh -l user deinserver
```

Dich direkt auf die shell bringen, ist der Stick nicht gesteckt erfolgt die Abfrage des Passworts.

&Voila, Ziel erreicht