Erzeugen eines ssh - Schlüsselpaares mit Putty unter Windows

Oft ist es mühsam immer wieder sein Passwort eingeben zu müssen, insbesondere für das SSH-Protokoll. Nach der Installation des Programms **putty** (http://www.putty.org) stehen einige Tools zur Verfügung, mit deren Hilfe statt einer Passwort-basierten Anmeldung ein zuvor erzeugtes Schlüsselpaar (öffentlicher/privater Schlüssel) verwendet werden kann, um eine häufige Eingabe oder Klartextspeicherung des Passworts zu vermeiden. Die folgende Anleitung dient dazu, solch ein Schlüsselpaar zu erzeugen und für die Verwendung mit SSH einzurichten.

ssh key erzeugen

Zunächst einmal startet man das Programm **Puttygen**. In dem Dialog sollte man den Wert für „Number of bits in a generated key“ möglichst hoch setzen; z.B. auf 4096 (Abbildung 1).

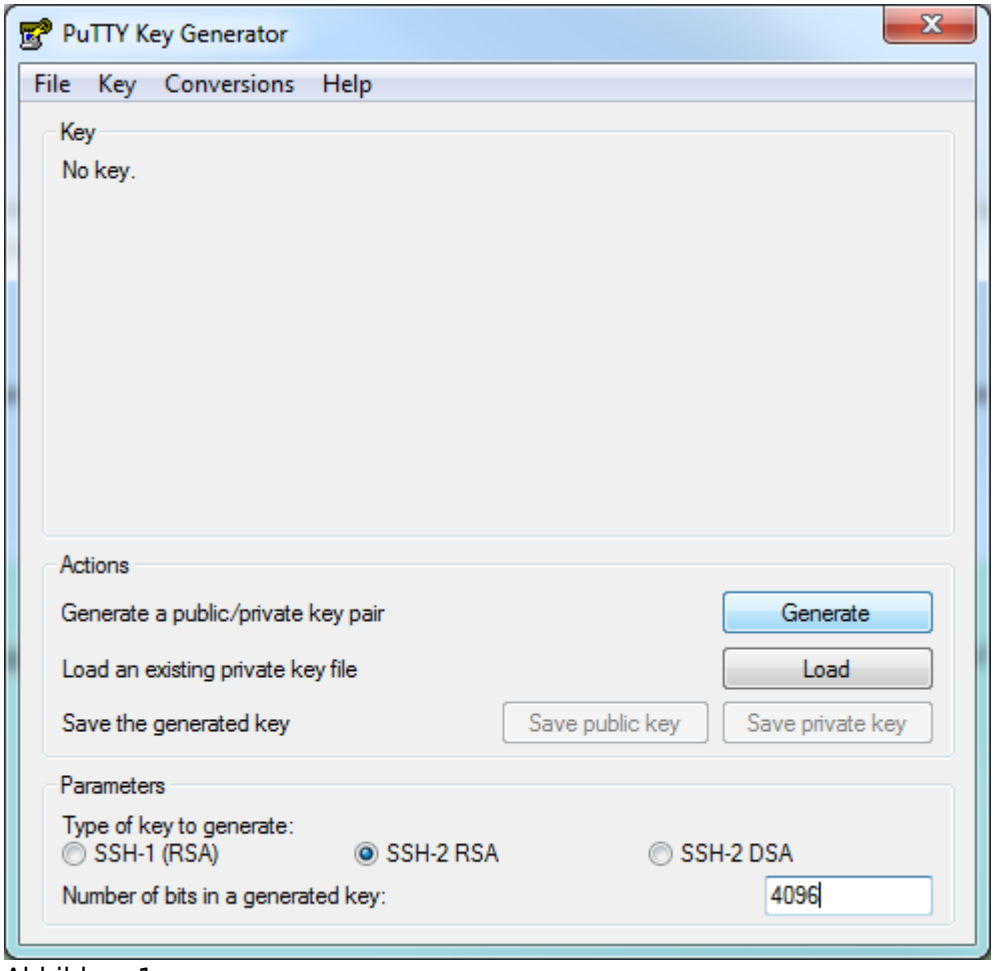

Abbildung1

Dann klickt man auf die Taste „Generate“, um den Schlüssel zu erzeugen. Dabei muss man den Mauszeiger kontinuierlich über den Dialog bewegen. Das erzeugt eine gewisse Zufälligkeit, was der Zufallsgenerator unter Windows nicht vermag (Abbildung 2).

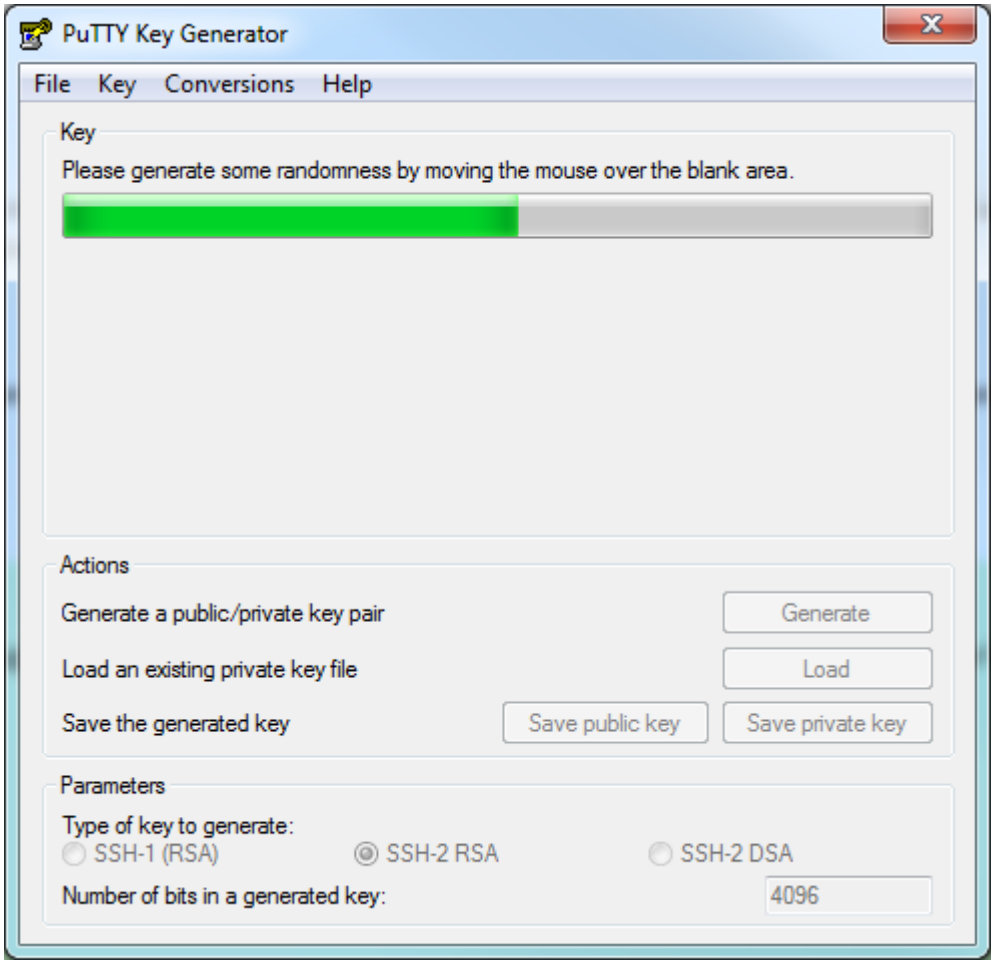

Abbildung2

Wenn der Fortschrittsbalken durchgelaufen ist, den Dialog nicht schließen und noch nichts speichern. Zunächst muss der öffentliche Schlüssel aus dem Fenster kopiert und gespeichert werden. Das ist notwendig, weil das Dateiformat, in dem Windows seine Schlüssel abspeichert, nicht mit Linux kompatibel ist. Eine manuelle Konvertierung wäre etwas mühselig. Dazu markiert man den gesamten Text in dem Fenster (Abbildung 3) und kopiert die Daten in die Zwischenablage (Strg-c).

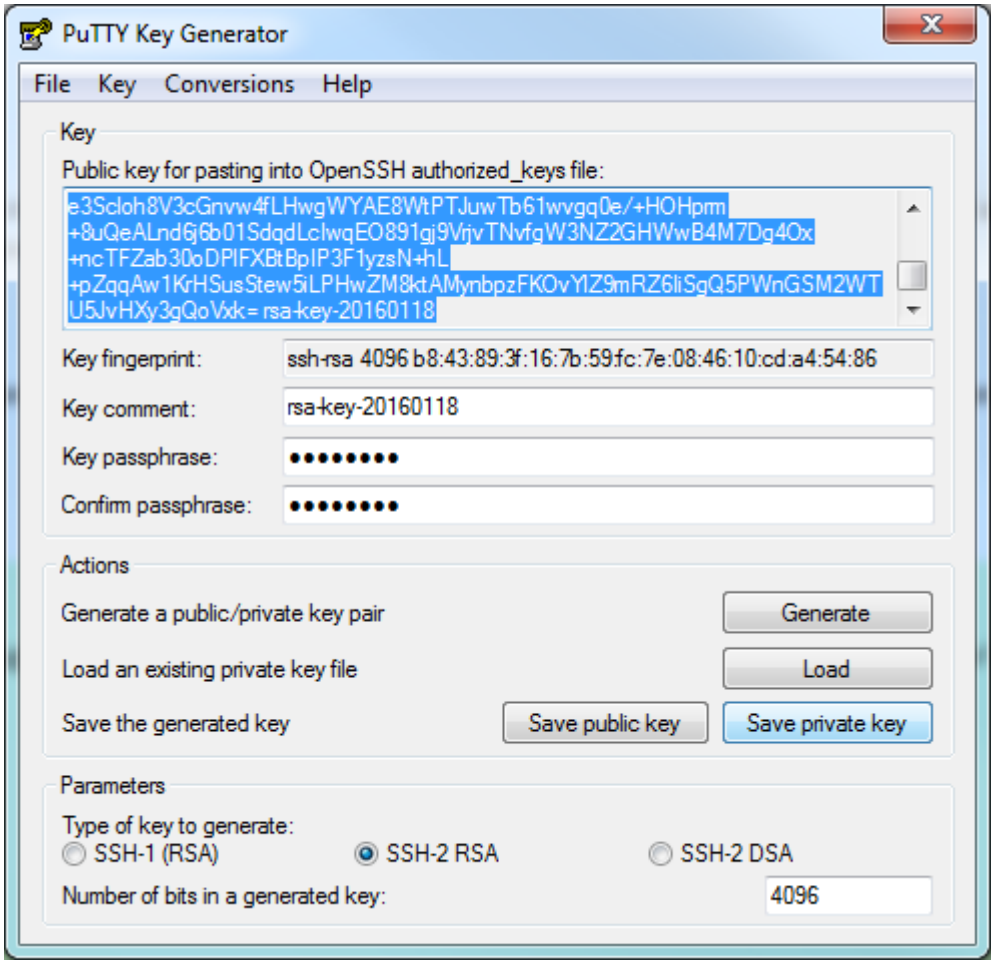

Abbildung3

Der markierte Text muss nun in die Datei `authorized_keys` eingefügt werden. Diese muss auf dem persönlichem Bereich (im AI-Labor im Z-Laufwerk) unter

```
Z:\.ssh\
```

stehen. Sollten das Verzeichnis oder die Datei noch nicht vorhanden sein, müssen sie angelegt werden. Einen versteckten Ordner legt man im Windows-Explorer an, indem am Ende des Namens einen Punkt gesetzt wird (`.ssh.`). Alternativ kann die „Eingabeaufforderung“ (cmd/ DOS-Box) oder ein Filetransferprogramm wie z.B. filezilla (http://filezilla.de) benutzt werden. Für die `authorized_keys` (ohne jegliche Endung) einfach per Rechtklick → Neu → Textdokument klicken, den korrekten Namen eingeben (und die Endung `.txt` entfernen) und bei der Warnung zur Namensänderung (Abbildung 4) „Ja“ klicken.

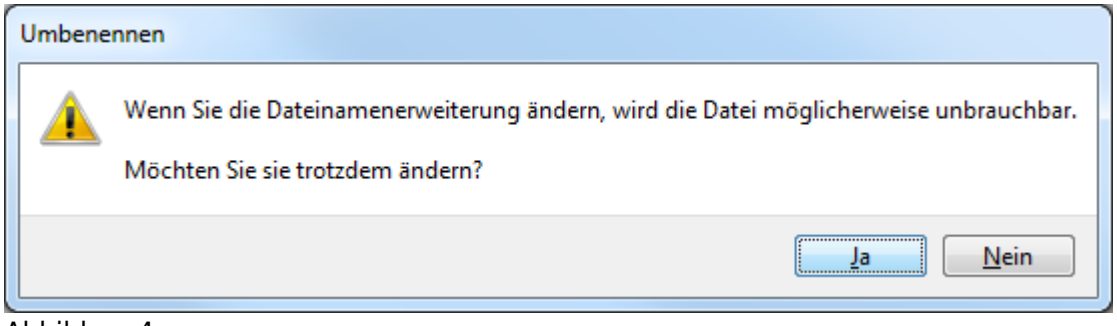

Abbildung4

Die Datei mit einem Editor öffnen und den zuvor kopiertenText unten anfügen. Der markierte Text ist genau eine Zeile, enthält keine Umbrüche, außer am Ende. Nun die Datei `authorized_keys`

speichern.

Jetzt kann der private Schlüssel gespeichert werden. Dazu sollte in den entsprechenden Feldern eine Passphrase (Passwort) eingeben werden, die nochmals zu bestätigen ist. Falls eine Passphrase angegeben wurde, muss diese später bei jedem Zugriff eingegeben werden, um den privaten Schlüssel zur Benutzung freizuschalten (falls kein „ssh key agent“ verwendet wird). Nun auf die Schaltfläche „Save private key“ klicken und den Schlüssel mit einem sprechenden Namen, z.B. `key_20160118.ppk`, in einem privaten Speicherbereich (ggf. USB-Stick) abspeichern. Man kann auch noch den öffentlichen Schlüssel abspeichern, quasi als Kopie. Man darf ihn aber nicht in diesem Format in die `authorized_keys` einfügen. Nun ist das Schlüsselpaar erzeugt und kann benutzt werden. Fast alle SSH-basierten Programme unterstützen die Angabe einer Datei mit einem privaten Schlüssel (der zu einem öffentlichen Schlüssel in der authorized_keys – Datei passen muss) statt einer Passwortabfrage.

ssh key in den Agenten laden

Ein SSH-Agent übernimmt die sichere Verwaltung der privaten Schlüssel und wird mit dem Programm **Pageant** gestartet (dieses steht Ihnen auch im AI-Labor zur Verfügung). Dazu muss der ssh-agent gestartet und der private Schlüssel geladen werden. Wenn der Agent gestartet ist, findet man das dazugehörige Symbol in der Taskleiste (Abbildung 5) – ein PC mit einem Schlapphut. Mit einem rechten Mausklick kann man sich unter „View keys“ die schon geladenen Schlüssel ansehen oder mit „Add key“ einen Schlüssel hinzufügen. Dazu öffnet sich ein Filebrowser, mit dem man die entsprechende Datei auswählen kann; in diesem Fall z.B. `Z:\.ssh\key_20160118.ppk`

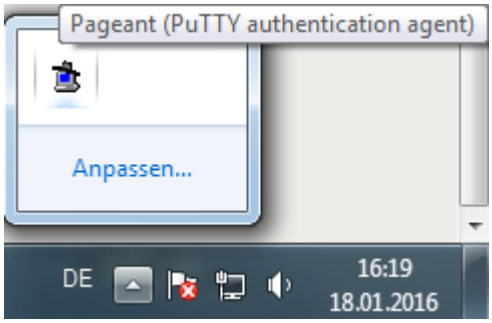

Abbildung5