HOWTO zur schlÃ¼sselbasierten SSH-Anmeldung per Putty unter Windows

$Id: putty-anmeldung-ohne-passwort-HOWTO.txt,v 1.13 2019/11/26 19:37:07 tsbirn Exp $

Dieses Dokument beschreibt die Einrichtung einer schlÃ¼sselbasierten sicheren Verbindung zwischen Putty-Client auf einem Windows-Rechner und SSH-Dienst auf eine UNIX/Linux-Rechner.

INHALTSVERZEICHNIS

0) Installation
1) SchlÃ¼sselpaar fÃ¼r Authentifizierung erzeugen
2) Ã–ffentlichen SchlÃ¼sselteil auf Ziel-Rechner eintragen
3) Verbindung zum Ziel-Rechner aufnehmen
4) Probleme bei der Verbindungsaufnahme lÃ¶sen
5) Passwortbasierte Authentifizierung abschalten
6) Weitere Informationen

---

0) Installation

Das Installationspaket "putty-0.XX-installer.exe" von der ORIGINAL-Webseite

  http://www.chiark.greenend.org.uk/~sgtatham/putty

holen und installieren (NICHT von einer anderen Webseite!)

1) SchlÃ¼sselpaar fÃ¼r Authentifizierung erzeugen

Das Programm "PuttyGen" aus Start --> Programme --> Putty aufrufen und ein SchlÃ¼sselpaar erzeugen: Dazu Button "Generate" drÃ¼cken und die Maus solange beliebig bewegen, bis genÃ¼gend Zufall zur SchlÃ¼sselgenerierung erzeugt ist. Der grÃ¼ne Balken signalisiert den Fortschritt bei der SchlÃ¼sselgenerierung (lÃ¤uft 2x durch).

2) Ã–ffentlichen SchlÃ¼sselteil auf Ziel-Rechner eintragen

Den im Textfeld oben von "PuttyGen" angezeigten (langen) Ã¶ffentlichen SchlÃ¼ssel (public key) "ssh-rsa AAAA... == rsa-key-20140409" kopieren (ACHTUNG: wirklich ALLE Zeichen, z.B. per "Rechte Maustaste --> Alles auswÃ¤hlen" + "Rechte Maustaste --> Kopieren") und auf dem Ziel-Rechner bei einem Benutzer (z.B. "kurs") in die Datei "~/.ssh/authorized_keys" eintragen (EINE Zeile!).

```
  /home/kurs/.ssh/authorized_keys    # Benutzer "kurs"
```

ACHTUNG: Ein mit "PuttyGen" gespeicherter Ã¶ffentliche SchlÃ¼ssel (Button "Save Public Key") ist leider nicht unter UNIX/Linux verwendbar (hat falsches Format).

Falls auf dem Ziel-Rechner im Heimatverz. "/home/kurs" von Benutzer "kurs" das Verz. ".ssh" oder die Datei ".ssh/authorized_keys" nicht existiert, diese anlegen + verrechten:

```
  mkdir ~/.ssh                       # Verstecktes Verz. (wg. fÃ¼hrendem Punkt)
  touch ~/.ssh/authorized_keys       # Tippfehler vermeiden
  chown -R kurs.kurs ~/.ssh          # Besitzer(Gruppe) (-R=Rekursiv)
  chmod 755 ~/.ssh                   # Zugriffsrechte (--> rwxr-xr-x)
  chmod 644 ~/.ssh/authorized_keys   # Zugriffsrechte (--> rw-r--r--)
```

ACHTUNG: Den Namen der Datei "authorized_keys" ohne Tippfehler schreiben und die Verrechtung des Verz. "~/.ssh" und der Datei "authorized_keys" kontrollieren, d.h.:

```
  ls -ld ~/.ssh ~/.ssh/authorized_keys   # -l=long, -d=directory only
```

MUSS folgende Ausgabe liefern:

```
  rwxr-xr-x kurs kurs ... /home/kurs/.ssh
  rwxr--r-- kurs kurs ... /home/kurs/.ssh/authorized_keys
```

ACHTUNG: Beim Kopieren des Ã¶ffentlichen SchlÃ¼ssels aus dem Fenster von "PuttyGen" kein Zeichen vorne oder hinten vergessen, der SchlÃ¼ssel funktioniert sonst nicht. Das korrekte Format sieht so aus:

```
     Je ein Leerzeichen
        +----------+
        |          |
        v          v
  ssh-rsa AAAA....== rsa-key-20140409   # Zeile in "authorized_keys"
     ^         ^          ^
     |         |          |
  KEYTYP    SCHLUESSEL    KOMMENTAR (endet auf YYYYMMDD)
            (beginnt mit "AAAA" und endet mit "==")


ACHTUNG: Wird der "vi" zum Editieren der Datei "authorized_keys" benutzt, VOR
dem EinfÃ¼gen des SchlÃ¼ssels per Maus in den INSERT-Modus schalten (z.B. per "i"
oder "I" oder "o")! Sonst wird das 1. Zeichen "s" des kopierten SchlÃ¼sseltextes
als "substitute"-Befehl des vi interpretiert und beim folgenden EinfÃ¼gen des
SchlÃ¼ssels im kopierten Text unterschlagen!

ACHTUNG: Die letzte Zeile in "authorized_keys" MUSS mit einem Zeilenvorschub
abgeschlossen werden (sonst Meldung "missing EOL at last line").

   ssh-rsa AAAA...== rsa-key-20140409   # OK (Typ + Key + Kommentar)
   sh-rsa AAAA...== rsa-key-20140409    # Falsch (Typ sh-rsa am Anfang falsch)
   AAAA...== rsa-key-20140409           # Falsch (Typ ssh-rsa am Anfang fehlt)
   ssh-rsa AAAA...                      # Falsch (...== am Keyende fehlt)

ACHTUNG: Das Kopieren per Maus ist NICHT SICHER, da es Ã¼ber Netzwerk erfolgt!
Besser wÃ¤re ein Transport Ã¼ber einen 2. Weg (z.B. als Datei per USB-Stick).
Zumindest sollte dann der Fingerprint des OriginalschlÃ¼ssels (vorlesen lassen)
mit dem Fingerprint der Kopie auf IdentitÃ¤t Ã¼berprÃ¼ft werden.

Den privaten Teil des erzeugten SchlÃ¼ssels (private key) auf dem
Windows-Rechner per Button "Save private key" abspeichern.

Die Passphrase kann leer gelassen werden, allerdings ist der private SchlÃ¼ssel
dann im Klartext auf der Windows-Maschine abgelegt und kann von anderen evtl.
gelesen werden, die Zugriff auf diesen Rechner haben.

Besser ist es daher, eine Passphrase fÃ¼r den privaten SchlÃ¼ssel zu vergeben.
Diese ist dann bei jeder Verbindungsaufnahme per Putty zum Entsperren des
privaten SchlÃ¼ssels einzutippen oder kann mit dem Programm "Pageant"
(Putty-Agent) automatisch zur VerfÃ¼gung gestellt werden.


3) Verbindung zum Ziel-Rechner aufnehmen
----------------------------------------
Putty starten, eine Session zum Ziel-Rechner (hier "192.168.0.201") fÃ¼r den
obigen Benutzer (hier "kurs") neu anlegen oder per "Load" einlesen:

   kurs@192.168.0.201

Im Konfigurationsteil "Connection --> SSH --> Auth" der Sitzung den Pfad zur
Datei mit dem gerade gespeicherten privaten SchlÃ¼ssel eintragen

  "Private key file for authentication:" [...]    "Browse..."

Die Sitzung ordentlich BENENNEN + SPEICHERN nicht vergessen (dazu wieder im
Konfigurationsteil auf "Session" positionieren und "Save" drÃ¼cken")

Nun sollte eine schlÃ¼sselbasierte Verbindung mit dem Ziel-Rechner (ohne
Passwort) mÃ¶glich sein (aber evtl. mit Eingabe der Passphrase).

ACHTUNG: Bei der 1. Verbindungsaufnahme zum Ziel-Rechner erscheint eine Meldung,
dass dieser Rechner noch nie besucht wurde und ein Fingerprint wird angezeigt.
Dieser Fingerprint ist mit dem des Zielrechners manuell zu vergleichen und
die Meldung ist zu bestÃ¤tigen.


4) Probleme bei der Verbindungsaufnahme lÃ¶sen
----------------------------------------------
Bei Problemen mit der Verbindungsaufnahme auf dem Ziel-Rechner die Meldungen
dess SSH-DÃ¤mons "sshd" wÃ¤hrenddessen in der Log-Datei beobachten:

  sudo tail -f /var/log/auth.log

Typische Probleme sind:
* Falsche Verrechtung des Verz./der Datei "~/.ssh/authorized_keys"
  (z.B. Schreibrecht gesetzt fÃ¼r alle oder fehlendes x-Recht fÃ¼r alle)
* Fehler beim Kopieren des SchlÃ¼ssels nach "~/.ssh/authorized_keys"
  (z.B. Windows-Format, SchlÃ¼ssel nicht vollstÃ¤ndig kopiert, "==" am Ende fehlt)
* Falscher Name von Verz./Datei (z.B. "~/.ssh/autorized-key")

Um mehr Log-Informationen zu erhalten, den Log-Level in "/etc/ssh/sshd_config"
```

erhÃ¶hen (nicht vergessen, den SSH-Server danach neu zu starten):

```
  LogLevel  DEBUG            # statt INFO
```

ACHTUNG: Nach der Fehlersuche den Log-Level wieder auf "INFO" zurÃ¼cksetzen (und den SSH-Server neu starten), damit die Menge an Logdaten nicht zu stark wÃ¤chst.

5) Passwortbasierte Authentifizierung abschalten

Sobald die schlÃ¼sselbasierte Anmeldung funktioniert, kann die passwortbasierte Anmeldung abgeschalten werden (erhÃ¶hte Sicherheit). Dazu auf dem Zielrechner in der Konfigurations-Datei "/etc/ssh/sshd_config" des SSH-Daemons den Eintrag

```
  PasswordAuthentication  yes
```

gegen

```
  PasswordAuthentication  no
```

austauschen und den SSH-Daemon neu starten:

```
  sudo /etc/init.d/ssh restart   # SysV
  sudo initctl ssh restart       # Upstart
```

6) Weitere Informationen

Die Ã¶ffentlichen SchlÃ¼ssel der Hosts, mit denen man sich verbindet, landen in der Windows-Registry. Ebenso die Putty-Konfigurations- und Sitzungsdaten:

```
  [HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\*]
  [HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\SshHostKeys]
```

Bei WinSCP landen Sie an folgender Stelle in der Windows-Registry:

```
  [HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Configuration\*]
  [HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Session\*]
  [HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\SshHostKeys]
```

Weitere Hinweise zur Konfiguration von Putty sind zu finden unter:

```
  --> putty-konfiguration-HOWTO.txt
```