Kann ich das Public-Key-Verfahren für SSH und FTP nutzen?

Um die Sicherheit beim Einloggen auf den Webspace zu erhöhen, kann ein SSH-Key erzeugt werden. Für Windows und Linux gelten dabei unterschiedliche Herangehensweisen, welche wir in diesem FAQ-Beitrag erläutern möchten.

Sicherheitshinweis
Der im Folgenden generierte Private Key darf auf keinen Fall in die Hände von Dritten gelangen und muss daher mit entsprechender Sorgfalt verwahrt werden. Aus Vorsicht vor Diebstahl oder Verlust sollte z.B. auf das Abspeichern des Keys auf Medien wie z.B. USB-Sticks verzichtet werden.

Windows

Das Programm Putty bietet unter Windows hierfür die benötigten Funktionen und ist relativ einfach zu bedienen. Zudem ist das Programm kostenlos und Open Source.

Download Putty

Für die Generierung eines eigenen SSH-Keys wird außerdem PuttyGen benötigt.

Download PuttyGen

Lokale Vorbereitung

Zunächst wird PuttyGen gestartet, welches uns mit dem folgenden Bildschirm begrüßt:

Mit den folgenden Schritten kann nun das Schlüsselpaar erzeugt werden:

1. Der Typ des Schlüsselpaares muss ausgewählt werden: Type of key to generate = SSH RSA
2. Außerdem muss die Number of bits in a generated key = 1024 angeben werden.

Es gilt: je höher die Bitanzahl, desto sicherer der Key. Mögliche Alternativen sind z.B. 2048 oder 3072 Bit.
3. Um den Vorgang abzuschließen, bitte den Generate-Button drücken.
4. Um den Key möglichst zufällig zu generieren, muss der Cursor über das leere Feld bewegt werden.

Im nun folgenden Bildschirm werden weitere Eingaben getätigt:

1. In dem Feld "key passphrase" muss ein Passwort eingegeben werden, dieses muss im Anschluss in dem Feld "confirm passphrase" nochmal bestätigt werden.
2. Nun "Save public key" wählen und den Key lokal unter einem beliebigen Namen und der Endung .txt speichern.
3. Den privaten Schlüsselteil über den Button "Save private key" speichern. Die Dateiendung muss .ppk lauten.
4. Abschließend muss der public key aus dem Puttygen abkopiert werden, damit dieser gleich auf dem Webhosting-Speicherplatz hinterlegt werden kann. Alternativ kann dieser Key auch später aus der erstellten .txt abkopiert werden.
5. PuttyGen schließen.

Public Key auf dem Webspace hinterlegen

Der soeben generierte Key kann mit Hilfe von Putty auf Ihrem Webspace hinterlegt werden.

1. Starten Sie zunächst Putty.
2. Geben Sie in diesem Feld Ihren Domain- oder Servernamen ein.
3. Der Port 22 sollte bereits ausgewählt sein.
4. Gleiches gilt für den Connection type: SSH.
5. Über den Button Open kann nun die Sitzung gestartet werden.

Beim Verbindungsaufbau wird Ihr Benutzername und Kennwort abgefragt, geben Sie hier die Zugangsdaten Ihres Haupt-FTP-Benutzers an.

Hinweis: Bei Eingabge des Passworts wird sich der Cursor nicht bewegen.

Nachdem Sie sich erfolgreich angemeldet haben, erstellen Sie einen neuen Ordner .ssh und vergeben die korrekten Berechtigungen:

```
mkdir ~/.ssh
chmod 700 ~/.ssh
```

Mit Hilfe eines Texteditors muss nun der zuvor erstellte Public Key auf dem Speicherplatz abgelegt werden. Öffnen Sie dazu eine neue Datei mit folgendem Befehl:

```
pico ~/.ssh/authorized_keys
```

Fügen Sie den im vorherigen Abschnitt kopierten Key mit einem Klick der rechten Maustaste in die Textdatei ein. Mit den Tastenkombinationem Strg+o,Enter,Strg+x speichern Sie die Datei und verlassen den Editor wieder.

Damit niemand Unberechtigtes auf diese wichtige Datei zugreifen kann, ändern Sie auch hier die Zugriffsrechte mit diesem Befehl:

```
chmod 600 ~/.ssh/authorized_keys
```

Die Vorbereitungen sind damit abgeschlossen. Putty muss nur noch so eingerichtet werden, dass der eingerichtete Schlüssel für die SSH-Verbindung verwendet wird.

Private Key in Putty hinterlegen

1. Starten Sie Putty.
2. Unter Category –> Connection –> SSH wählen Sie den Punkt "Auth" aus.
3. Klicken Sie auf der rechten Seite neben Private key file for authentication auf "Browse" und wählen Sie Ihren Private Key aus.

Nun wechseln Sie wieder auf die Hauptseite (Session) und geben im Feld "Host Name" Ihren FTP-Benutzernamen, gefolgt von @ihredomain.de ein. Im Feld Saved Sessions können Sie einen Namen für diese konfigurierte Sitzung vergeben und mit einem Klick auf "Save" abspeichern. Bei einem erneuten Aufruf von Putty können Sie so die Sitzung inkl. Ihrer Einstellungen laden.

Zu guter Letzt können Sie sich jetzt durch einen Klick auf "Open" mit Ihrem Speicherplatz verbinden. Sie werden nun nach der Passphrase gefragt, die Sie beim Erstellen des Schlüssels definiert haben.

Linux

Die Generierung eines Schlüsselpaares gestaltet sich unter Linux ein wenig anders, da in der Regel die benötigten Arbeiten mit den Bordmitteln durchgeführt werden können.

Öffnen Sie eine Konsole und erstellen Sie, sofern noch nicht vorhanden, das Verzeichnis ~/.ssh:

```
mkdir ~/.ssh
```

Jetzt kann das Schlüsselpaar erstellt werden:

```
ssh-keygen -t rsa -f ~/.ssh/id_rsa
```

Verbinden Sie sich vorab per SSH mit Ihrem Speicherplatz und erstellen Sie, wie bereits weiter oben beschrieben, den Ordner ~/.ssh auf Ihrem Speicherplatz:

```
mkdir ~/.ssh
chmod 700 ~/.ssh
```

Ihr öffentlicher Schlüssel kann nun von Ihrem lokalen PC aus mit dem folgenden Befehl auf den Speicherplatz übertragen werden:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub ftpbenutzer@ihredomain.de
```

Sofern Sie keine Fehlermeldung erhalten, können Sie sich nun mit Ihrem Schlüssel am Server authentifizieren:

```
ssh -i ~/.ssh/id_rsa ftpbenutzer@ihredomain.de
```