

Öffentlicher Schlüsselservers

<http://wwwkeys.us.gpg.net/>

Schlüsselpaar erstellen

```
gpg --gen-key
```

Öffentliche Schlüssel anzeigen

```
gpg --list-keys
```

Private Schlüssel anzeigen

```
gpg --list-secret-keys
```

Signaturen anzeigen

```
gpg --list-sigs 0x473041FA
```

Datei verschlüsseln

```
cp /etc/passwd .  
gpg --encrypt --recipient 'Ingo Wichmann' --armor passwd
```

Datei entschlüsseln

```
gpg --decrypt passwd.asc
```

Datei signieren

```
gpg --sign --armor passwd
```

1)

Datei überprüfen

```
gpg --verify --armor passwd.asc
```

Öffentlichen Schlüssel weitergeben

```
gpg --export --armor "Ingo Wichmann" > /tmp/schluessel  
# gpg --send-keys 'Ingo Wichmann' # Bitte nicht mit Testschlüsseln  
mv passwd.asc /tmp
```

Öffentlichen Schlüssel importieren

```
gpg --import --armor /tmp/schluessel  
gpg --edit-key 'Ingo Wichmann'  
trust  
5  
gpg --verify /tmp/passwd.asc  
  
gpg --search-keys 'Ingo Wichmann'  
gpg --keyserver wwwkeys.uk.pgp.net --recv-key 0x473041FA
```

Schlüssel widerrufen

```
gpg --gen-revoke 'Ingo Wichmann'
```

Dokumentation

<http://www.stierand-linuxit.de/Doku/gpg-tutorial.html>

1)

Signatur in separater Datei, z.B. für Debian Release Dateien

```
gpg --detach-sign --armor passwd
```

From:
<https://wiki.lab.linuxhotel.de/> - **Linuxhotel Wiki**

Permanent link:
<https://wiki.lab.linuxhotel.de/doku.php/lpi1:pgg?rev=1404133988>

Last update: **2014/06/30 13:13**

