Schlüsselpaar generieren

Inhaltsverzeichnis

Der sichere Zugangsdatenspeicher benötigt ein individuelles Schlüsselpaar, welches zur Ver- und Entschlüsselung benötigt wird.

Image not found or type unknown

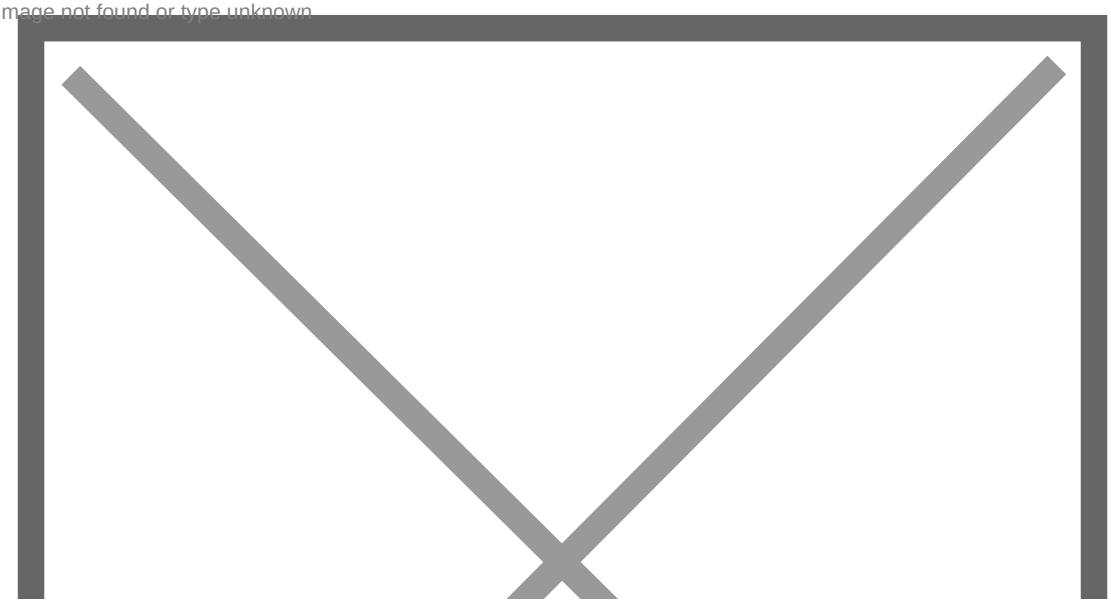


Photo by Uwe Baumann on pixabay

Alle sensiblen Daten und Kennwörter werden mit einem symmetrischen Schlüsselpaar verschlüsselt. Die Sicherheit des Zugangsdatenspeicher besteht darin, dass der private Schlüssel nicht am Server gespeichert wird. Dieser muss vor der Entschlüsselung hochgeladen werden, um die Daten zu entschlüsseln.

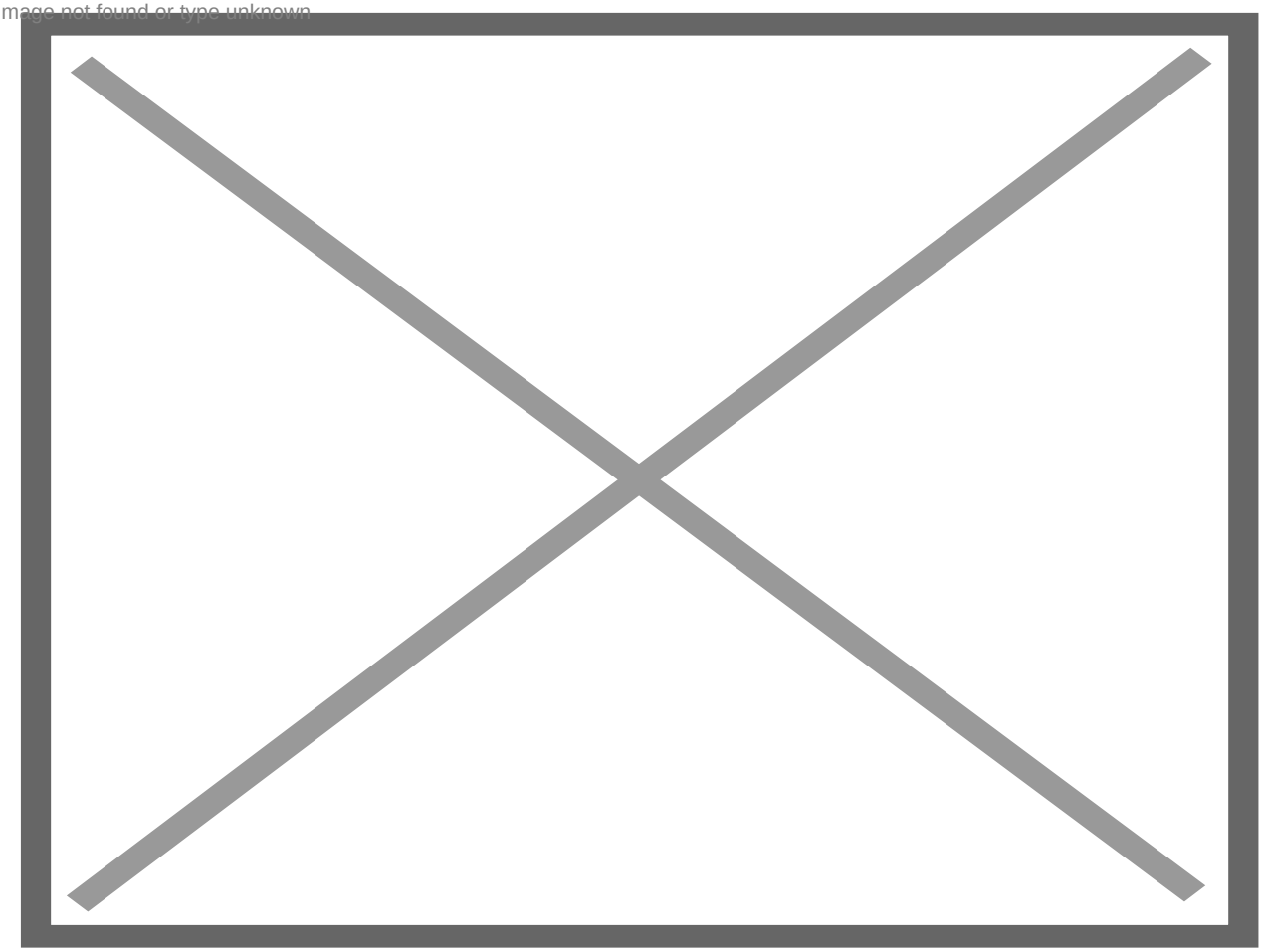
1 Schlüsselgenerierung

Dieses Schlüsselpaar muss nach der Installation erstellt werden. Es gibt dafür mehrere Möglichkeiten. Es wird ein RSA Schlüssel im PEM-Format (base64-kodiert) mit einer empfohlenen Schlüssellänge von 4096 bit benötigt.

1.1 Online Service

Der einfachste (wenn auch nicht sicherste Weg) ist die Generierung über einen kostenlosen Online-Service wie JSCrypt. Wählen Sie hier eine `Key Size` von `4096 bit` aus und klicken anschließen auf `Generate New Keys`.

Image not found or type unknown

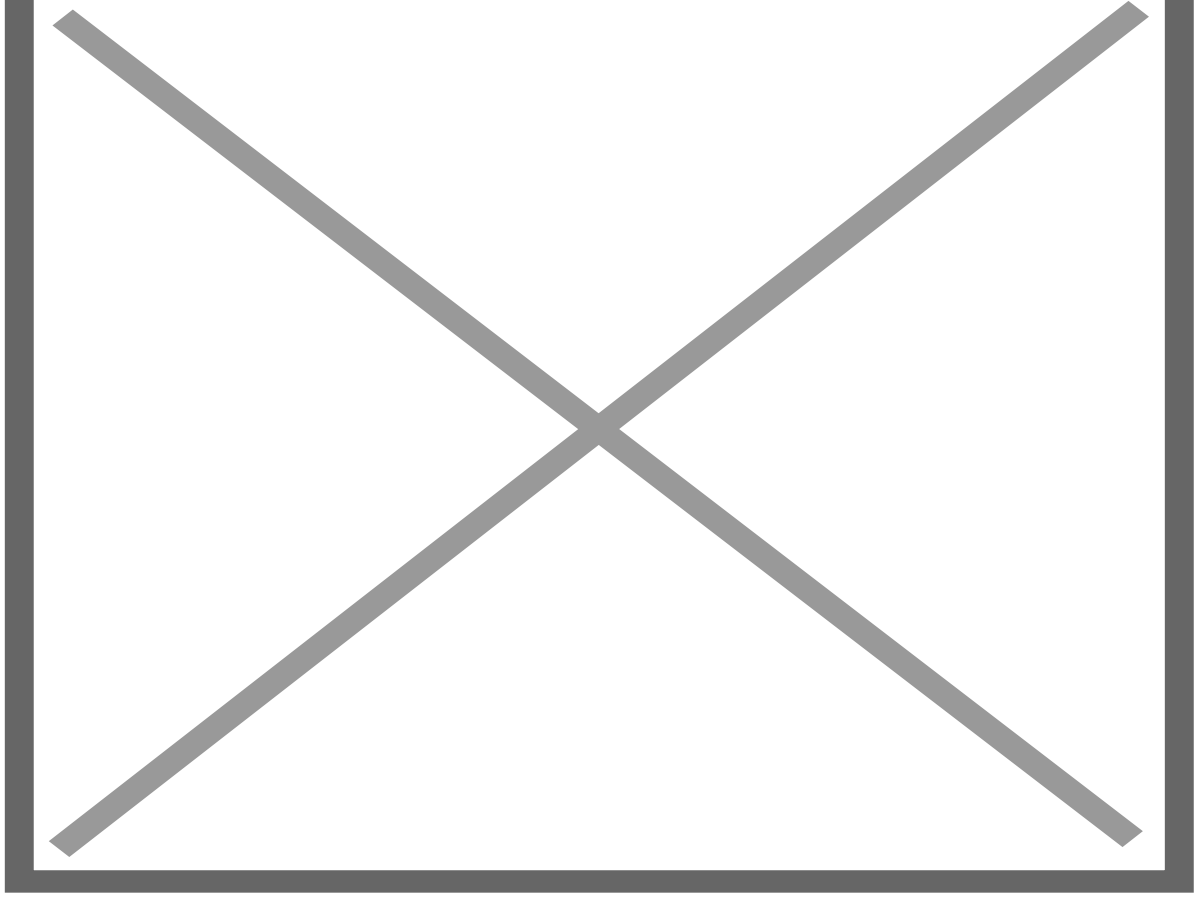


1.2 Lokale Generierung

Der sicherste Weg ist das Schlüsselpaar lokal zu generieren, da der private Schlüssel potentiell mit keiner fremden Webseite geteilt wird. Es gibt dafür unterschiedliche Tools wie `openssl`, welches auf den meisten Linux und MacOS Systemen bereits vorinstalliert ist. Führen Sie folgende Befehle aus.

Code

```
openssl genrsa -out private.pem 4096
openssl rsa -in private.pem -pubout > public.pem
```



Die Datei `private.pem` beinhaltet Ihren privaten Schlüssen. Die Datei `public.pem` den dazugehörigen öffentlichen Schlüssel.

2 Umgang mit Schlüsseln

Der öffentliche Schlüssel muss im ACP unter `Inhalte > Zugangsdaten-Speicher > Öffentliche Schlüssel` hinterlegt werden. Die Zugangsdaten werden ab sofort mit dem öffentlichen Schlüssel verschlüsselt und können nur mit dem privaten Schlüssel entschlüsselt werden. Speichern Sie diesen Schlüssel sicher ab. Wenn Sie ihn verlieren können Sie nicht auf die verschlüsselten Zugangsdaten zugreifen. Zugangsdaten, welche vor dem Hinzufügen des öffentlichen Schlüssels erstellt wurden, können nicht entschlüsselt werden.

Image not found or type unknown