

Schlüsselpaar generieren

Inhaltsverzeichnis

- [1 Schlüsselgenerierung](#)
 - [1.1 Online Service](#)
 - [1.2 Lokale Generierung](#)
- [2 Umgang mit Schlüsseln](#)

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



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.

Online RSA Key Generator

The screenshot shows a web-based RSA key generator. At the top, there's a dropdown menu for 'Key Size' set to '4096 bit'. Below it is a blue button labeled 'Generate New Keys'. To the right, a message says 'Generated in 15354 ms'. There are two sections: 'Private Key' and 'Public Key', each containing a large block of encoded RSA key data.

Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIJwIBAAKCAgBfIFLO0/PZPtNcCCS4yYchZXaQvX3597l0Npm0/6fmMvG
gMO
SfdlgoluDovLMifMpC8dm25ICjEprCacUK0GCC5SofyWkMhINPZ5nWAUw8i
djm
xYNa+AoOvJMI8WmDmWwlBskmNPix2K0a3VPHF3zAa3OT02L6oOgYPnEFkf
B8Vtkg
I6OPCNx/8jCeZntElnqGoktH/BjGBt7m6TQzkVkgvUT3hvcGfkTj0+FVjeA67kRm
66/pBQX/b5ERh8r4ITxkt1KfPl0mRJTob9RjEjmWMEmuV0MdQlDE5BXsvKEHj
Vn
t1AZkutcrJxRrPEWm0yyL031lgABt6V7uFuJf5d9HleMC6lYJ80gLqvJQcJPurJi
68LRicaJAq/Bao2yEFrXdFoLzJtBc92W16Y8gVX09/N1RP3AddxGLBseNp2YD
Zp
xde/ayNN7yw6ajxXcuP/M53D0cT700oFSsUDMS2oJSFzL96xl+ansH9Z53Tm
nEvA
```

Public Key

```
-----BEGIN PUBLIC KEY-----
MIICITANBgkqhkiG9w0BAQEFAOCAg4AMICCQKCAGBfIFLO0/PZPtNcCCS4
yYch
ZxaQvX3597l0Npm0/6fmMvGgMOSfdlgoluDovLMifMpC8dm25ICjEprCac
UK0
GCC5SofyWkMhINPZ5nWAUw8idjMxYNa+AoOvJMI8WmDmWwlBskmNPix2
K0a3VPH
F3zAa3OT02L6oOgYPnEFkfB8VtkgI6OPCNx/8jCeZntElnqGoktH/BjGBt7m6TQ
z
KVkgvUT3hvcGfkTj0+FVjeA67kRm66/pBQX/b5ERh8r4ITxkt1KfPl0mRJTob9Rj
EjmWMEmuV0MdQlDE5BXsvKEHjVn1AZkutcrJxRrPEWm0yyL031gA8t6V7
uFjJ
f5d9HleMC6lYJ80gLqvJQcJPurJi68LRicaJAq/Bao2yEFrXdFoLzJtBc92W16Y
8gVX09/N1RP3AddxGLBseNp2YDZpxde/ayNN7yw6ajxXcuP/M53D0cT700oF
SsUD
```

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
```

```
Mac-902b34da4a68:key earlyhost$ openssl genrsa -out private.pem 4096
Generating RSA private key, 4096 bit long modulus
.
.
.
e is 65537 (0x10001)
Mac-902b34da4a68:key earlyhost$ openssl rsa -in private.pem -pubout > public.pem
writing RSA key
[Mac-902b34da4a68:key earlyhost$ ls
private.pem    public.pem
Mac-902b34da4a68:key earlyhost$ ]
```

Die Datei `private.pem` beinhaltet Ihren privaten Schlüsseln. 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.

The screenshot shows the WolfLab Suite administration interface. The left sidebar has a dark blue background with white icons and text. The main area has a light blue header with the title "Öffentlichen Schlüssel hinzufügen". The main content area is titled "Allgemeine Daten" and contains fields for "Name", "Öffentlicher Schlüssel" (with a note about PEM encoding), and "Eigentümer". A blue "ABSENDEN" button is at the bottom right. The footer says "Community-Software: WolfLab Suite™ 5.2.4".

Administrationoberfläche - WLSuite

localhost:php7/2019/acp/index.php?credentials-public-key-add/

Deutsch AD

ÖFFENTLICHE SCHLÜSSEL AUFLISTEN

Öffentlichen Schlüssel hinzufügen

Allgemeine Daten

Name

Öffentlicher Schlüssel

Der öffentliche Schlüssel muss im PEM (base64 encodiert) angegeben werden. Es wird empfohlen einen RSA-Schlüssel mit einer Bit-Länge von mindestens 4096 bit zu erstellen.

Eigentümer

ABSENDEN

Community-Software: WolfLab Suite™ 5.2.4