



## Kurzanleitung: Domino Schlüsselring erstellen

Im Zweifel nachsehen, ob eine neue OpenSSL-Version (light) verfügbar ist, diese installieren.

OpenSSL-Win64 ist das Installationsverzeichnis von OpenSSL. Konfiguration OpenSSL:

```
C:\OpenSSL-Win64\bin>set OPENSSL_CONF=c:\OpenSSL-Win64\bin\openssl.cfg
```

```
C:\OpenSSL-Win64\bin>set RANDFILE=.rnd
```

Schlüsselpaar generieren (server.key):

```
C:\OpenSSL-Win64\bin>openssl genrsa -out server.key 4096
```

Schlüsselpaar ansehen.

```
C:\OpenSSL-Win64\bin>type server.key
```

CSR (server.csr) erzeugen, Zertifikatsinformationen eingeben.

```
C:\OpenSSL-Win64\bin>openssl req -new -sha256 -key server.key -out server.csr
```

Country Name (2 letter code) [AU]:**DE**

State or Province Name (full name) [Some-State]:**Hamburg**

Locality Name (eg, city) []:**Hamburg**

Organization Name (eg, company) [Internet Widgits Pty Ltd]:**ITEE**

Organizational Unit Name (eg, section) []:**Headquarter**

Common Name (e.g. server FQDN or YOUR name) []:**server.itee.zz**

Email Address []:**juergen.kunert@itee.de**

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:**geheim**

An optional company name []:**OptionalCompanyName**

CSR ansehen.

```
C:\OpenSSL-Win64\bin>type server.csr
```

**Variante 1: server.csr von Zertifizierungsstelle signieren lassen. Zurück kommt dann eine server.pem.**

**Variante 2: Zertifikat selbst signieren.**

```
C:\OpenSSL-Win64\bin>openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.pem
```

Zertifikat (server.pem) ansehen.

```
C:\OpenSSL-Win64\bin>type server.pem
```

Hinweis: Statt einer .pem-Datei kann es auch eine .crt-Datei zurückgeben. Die folgenden Befehle gelten genauso für .pem-Dateien.

Zertifikate (server.key und server.pem) zusammenfügen (server.txt).

```
C:\OpenSSL-Win64\bin>COPY C:\OpenSSL-Win64\bin\server.key+C:\OpenSSL-Win64\bin\server.pem  
server.txt
```

Reihenfolge: privater Schlüssel, von der Zertifizierungsstelle erhaltenes Zertifikat, Intermediate-Zertifikat(e) der Zertifizierungsstelle, Root-Zertifikat der Zertifizierungsstelle

Zwischenergebnis ansehen.

```
C:\OpenSSL-Win64\bin>type server.txt
```

In das Notes-**Programmverzeichnis** wechseln.

Zu Domino-Version passende Version (Version, 32/64Bit) von kyrtool.exe in das Notes oder Domino-Programmverzeichnis kopieren.

Für die Aufrufe von kyrtool ist der „-“Parameter dann nötig, wenn die notes.ini nicht im Pfad liegt:  
="C:\Program Files (x86)\IBM\Notes\notes.ini"

server.txt verifizieren:

```
C:\Program Files (x86)\IBM\Notes>kyrtool verify "C:\OpenSSL-Win64\bin\server.txt"
```

Schlüsselring erzeugen.

```
kyrtool create -k c:\notes\data\keyring.kyr -p auch-geheim
```

Variante A: Zertifikat in einem Schritt in den Schlüsselring importieren, wenn möglich.

```
kyrtool import all -i C:\OpenSSL-Win64\bin\server.txt -k c:\notes\data\keyring.kyr
```

Variante B: Zertifikat mit Intermediate-Zertifikaten schrittweise in den Schlüsselring importieren, beginnend mit dem Key.

```
Kyrtool import keys -i C:\OpenSSL-Win64\bin\server.key -k c:\notes\data\keyring.kyr
```

```
Kyrtool import certs -i C:\OpenSSL-Win64\bin\server.pem -k c:\notes\data\keyring.kyr
```

```
kyrtool import roots -i C:\OpenSSL-Win64\bin\intermediate1.pem -k c:\notes\data\keyring.kyr
```

```
kyrtool import roots -i C:\OpenSSL-Win64\bin\intermediate2.pem -k c:\notes\data\keyring.kyr
```

```
Kyrtool import roots -i C:\OpenSSL-Win64\bin\serverroot.pem -k c:\notes\data\keyring.kyr
```

Schlüssel anzeigen.

```
kyrtool show keys -k c:\notes\data\keyring.kyr
```

Zertifikate anzeigen.

```
kyrtool show certs -k c:\notes\data\keyring.kyr
```

Links:

<https://www.openssl.org/docs/>

<http://slproweb.com/products/Win32OpenSSL.html> (OpenSSL Download)

[https://hclpnpsupport.hcltech.com/csm?id=kb\\_view2](https://hclpnpsupport.hcltech.com/csm?id=kb_view2), dann KB0073172 (kyrtool Download)

[Generating a keyring file with a self-signed SHA-2 cert using OpenSSL and kyrtool](#)

[Generating a keyring file with a third party CA SHA-2 cert using OpenSSL and KYRTool on a Windows workstation](#)

[How to create a .pfx file from a server certificate in a Domino keyring](#)