

**Wie kann ich ein eigenes SSL Zertifikat für meinen virtuellen und Root-Server erstellen und hinterlegen?**

**Wie kann ich ein eigenes SSL Zertifikat für meinen virtuellen und Root-Server erstellen und hinterlegen?**



**Wichtiger Hinweis:**

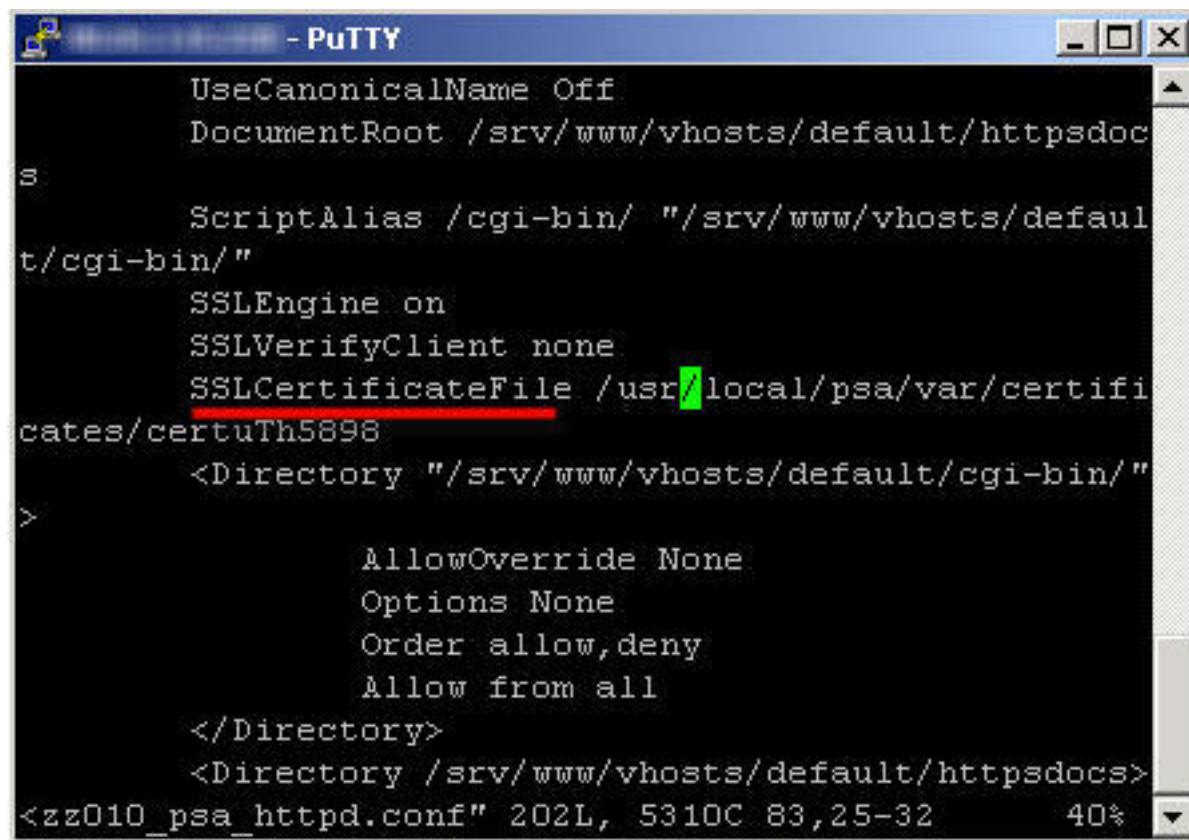
Die folgende Anleitung beschreibt die Vorgehensweise für die Referenzsysteme **Plesk 8** und **SuSE 10**.

**So geht's Schritt für Schritt:**

1. Suchen Sie den Standart **SSL Vhost** und dort nach Wert **SSLCertificateFile**.

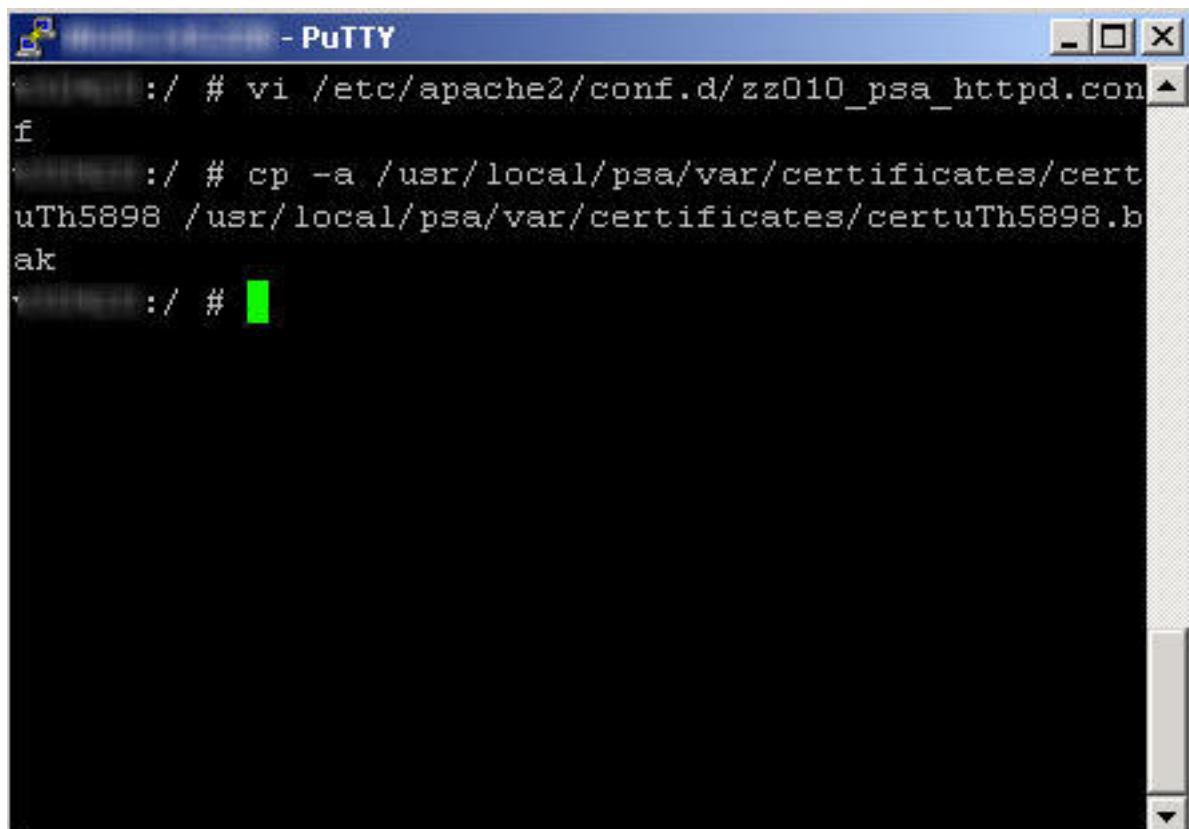
The screenshot shows a PuTTY terminal window with the title '- PuTTY'. The window displays an Apache configuration file (httpd.conf) with the following content:

```
UseCanonicalName Off
DocumentRoot /srv/www/vhosts/default/httpsdocs
ScriptAlias /cgi-bin/ "/srv/www/vhosts/default/cgi-bin/"
SSLEngine on
SSLVerifyClient none
SSLCertificateFile /usr/local/psa/var/certificates/certuTh5898
<Directory "/srv/www/vhosts/default/cgi-bin/">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
<Directory /srv/www/vhosts/default/httpsdocs>
<zz010_psa_httpd.conf" 202L, 5310C 83,25-32 40%
```



```
UseCanonicalName Off
DocumentRoot /srv/www/vhosts/default/httpsdocs
s
    ScriptAlias /cgi-bin/ "/srv/www/vhosts/default/cgi-bin/"
    SSLEngine on
    SSLVerifyClient none
    SSLCertificateFile /usr/local/psa/var/certificates/certuTh5898
<Directory "/srv/www/vhosts/default/cgi-bin/"
>
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
<Directory /srv/www/vhosts/default/httpsdocs>
<zz010_psa_httpd.conf" 202L, 5310C 83,25-32      40%
```

## 2. Sichern Sie diese Datei.



```
:/ # vi /etc/apache2/conf.d/zz010_psa_httpd.conf
f
:/ # cp -a /usr/local/psa/var/certificates/certuTh5898 /usr/local/psa/var/certificates/certuTh5898.b
ak
:/ #
```

### 3. Erstellen Sie den **SSL Key** mit einer **1024 Bit Verschlüsselung**:

**4. Entfernen Sie das Passwort des Keys**, da es beim Apache Neustart abgefragt wird und den Startprozess des Apaches unterbricht:

## 5. Erstellen Sie **SSL CSR Datei** ( Certificate Signing Request):

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

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

**Organization Name (eg, company) [Internet Widgits Pty Ltd]: 1blu GmbH**

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

**Common Name (eg, YOUR name) []: www.web-technik.de**

** Wichtiger Hinweis:**

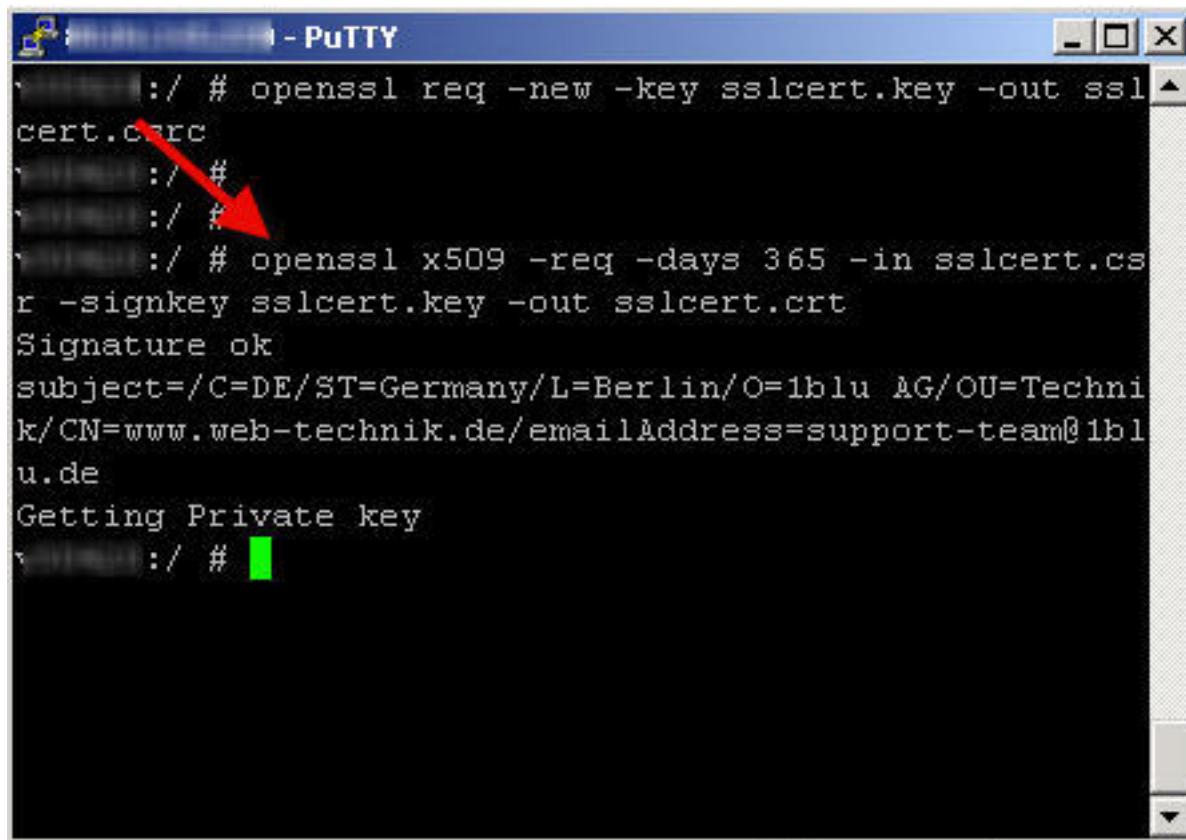
Common Name ist der Name der URL, mit der das SSL Zertifikat registriert wird!

**Email Address []: support-team@1blu.de**

**A challenge password []:**

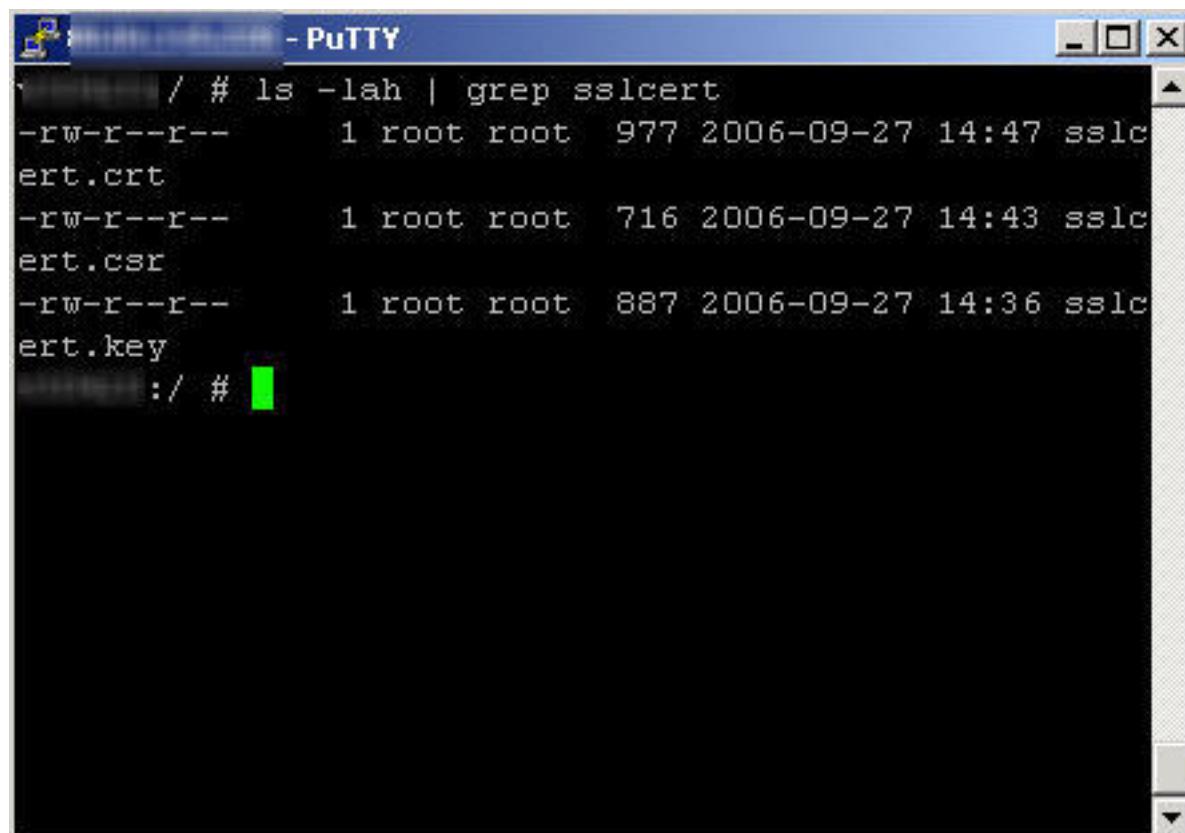
**An optional company name []:**

**6. Erstellen Sie das **selbstsignierte SSL Zertifikat**:**



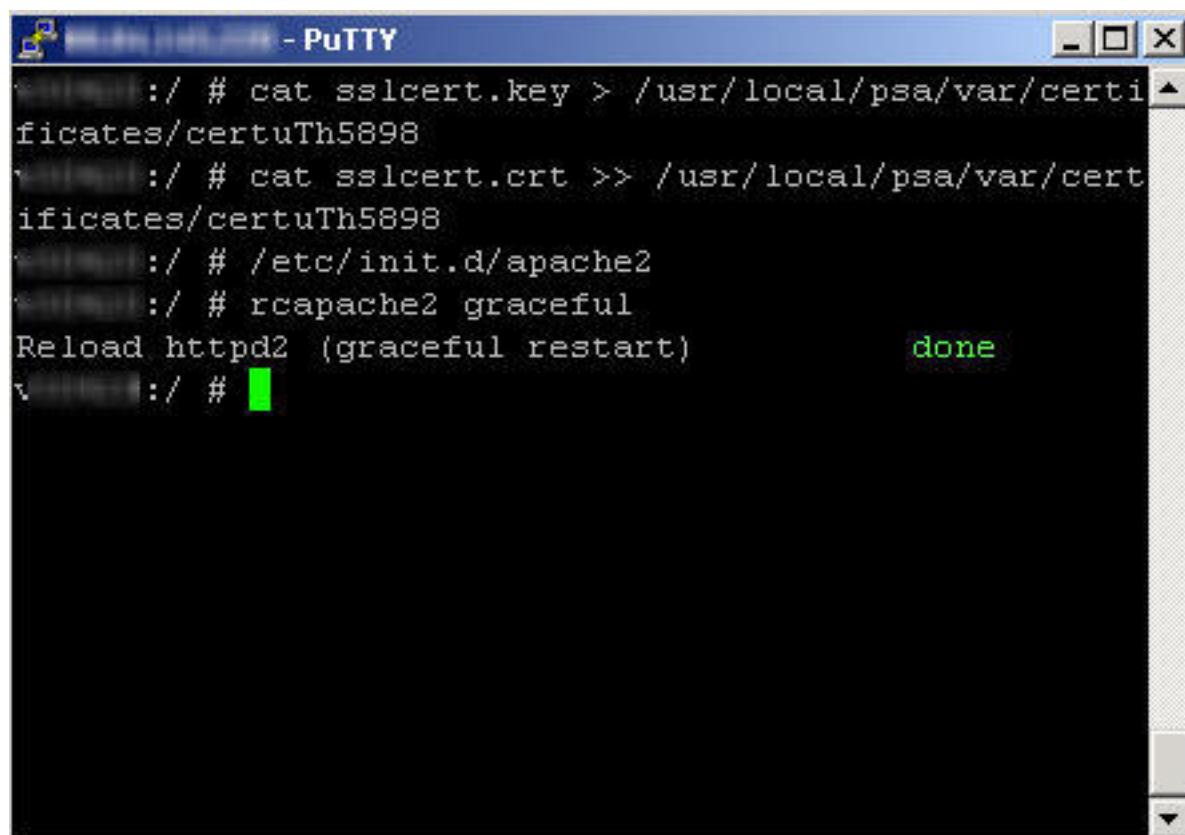
```
... :/ # openssl req -new -key sslcert.key -out sslcert.csr
... :/ #
... :/ #
... :/ # openssl x509 -req -days 365 -in sslcert.csr -signkey sslcert.key -out sslcert.crt
Signature ok
subject=/C=DE/ST=Germany/L=Berlin/O=1blu AG/OU=Technik/CN=www.web-technik.de/emailAddress=support-team@1blu.de
Getting Private key
... :/ #
```

**7. Es sollten im Working Directory **.key, .csr und .crt File** vorliegen:**



```
/ # ls -lah | grep sslcert
-rw-r--r-- 1 root root 977 2006-09-27 14:47 sslcert.crt
-rw-r--r-- 1 root root 716 2006-09-27 14:43 sslcert.csr
-rw-r--r-- 1 root root 887 2006-09-27 14:36 sslcert.key
:/ #
```

8. Fügen Sie nun .key und .crt File ins SSLCertificateFile ein und **starten** den Webserver **neu**:



```
:/ # cat sslcert.key > /usr/local/psa/var/certificates/certuTh5898
:/ # cat sslcert.crt >> /usr/local/psa/var/certificates/certuTh5898
:/ # /etc/init.d/apache2
:/ # rcaapache2 graceful
Reload httpd2 (graceful restart) done
:/ #
```

9. Sie können das selbst signierte SSL Zertifikat jetzt unter ➔ <https://ihre-ip> untersuchen. Dort  
Seite 6 / 7

sollten jetzt Ihre Werte stehen.

**10.** Wünschen Sie ein geprüftes Zertifikat, liefern Sie Ihren Key sowie Ihr .csr File bei [Thawte](#) oder [VeriSign](#) ein.

 **Wichtiger Hinweis:**

Beachten Sie bitte, dass dies kostenpflichtig ist!

**11.** Um eigene Inhalte für das SSL Zertifikat zu hinterlegen, müssten Sie die Daten als SSH Rootbenutzer **in das DocumentRoot dieses Vhostes hochladen**.

In unserem Beispiel, geprüft anhand der Datei

**/etc/apache2/conf.d/zz010\_psa\_httpd.conf**

war das Document Root des SSL Vhosts

**/srv/www/vhosts/default/httpsdoc**

In dieses müssten Sie beispielsweise via WinSCP die Daten veröffentlichen.

Eindeutige ID: #1155

Verfasser: n/a

Letzte Änderung: 2025-09-27 19:32