

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

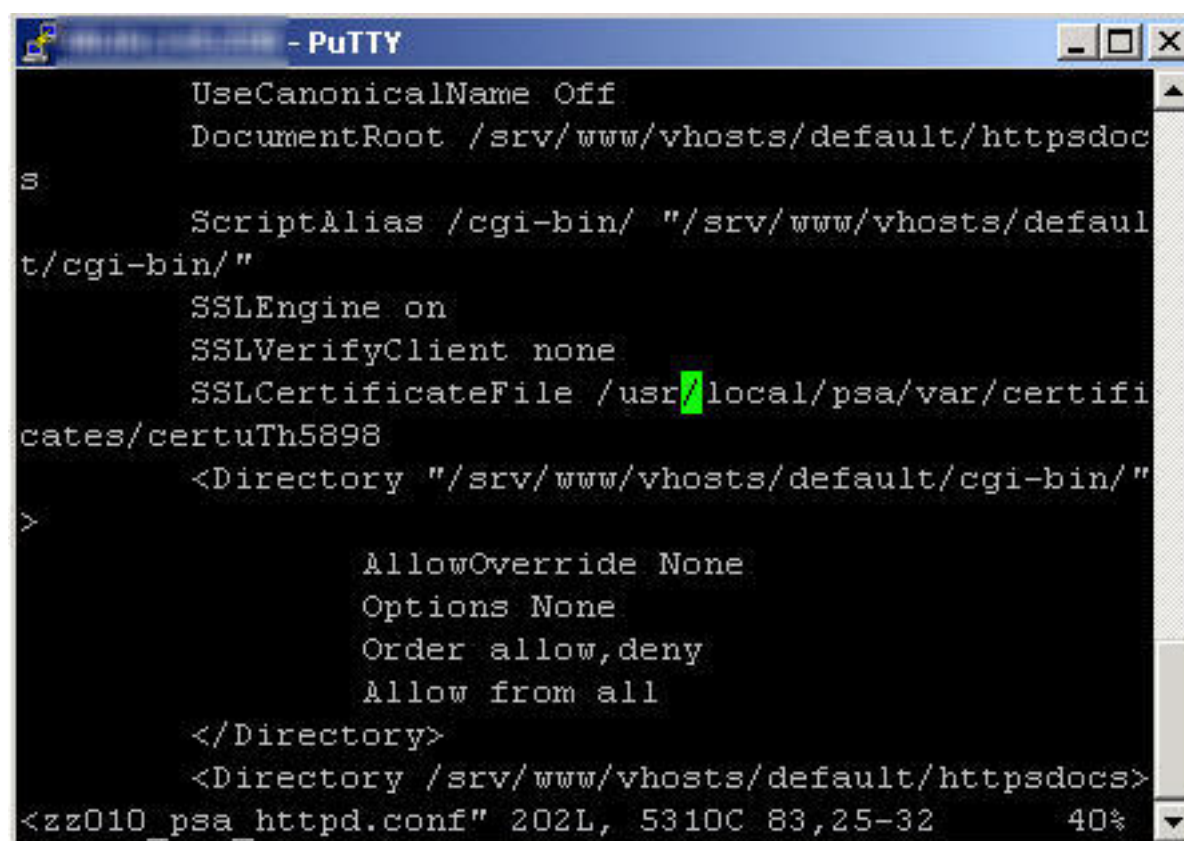
Wie kann ich ein eigenes SSL Zertifikat für meinen virtuellen und Root-Server erstellen und hinterlegen?

Wichtiger Hinweis:

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

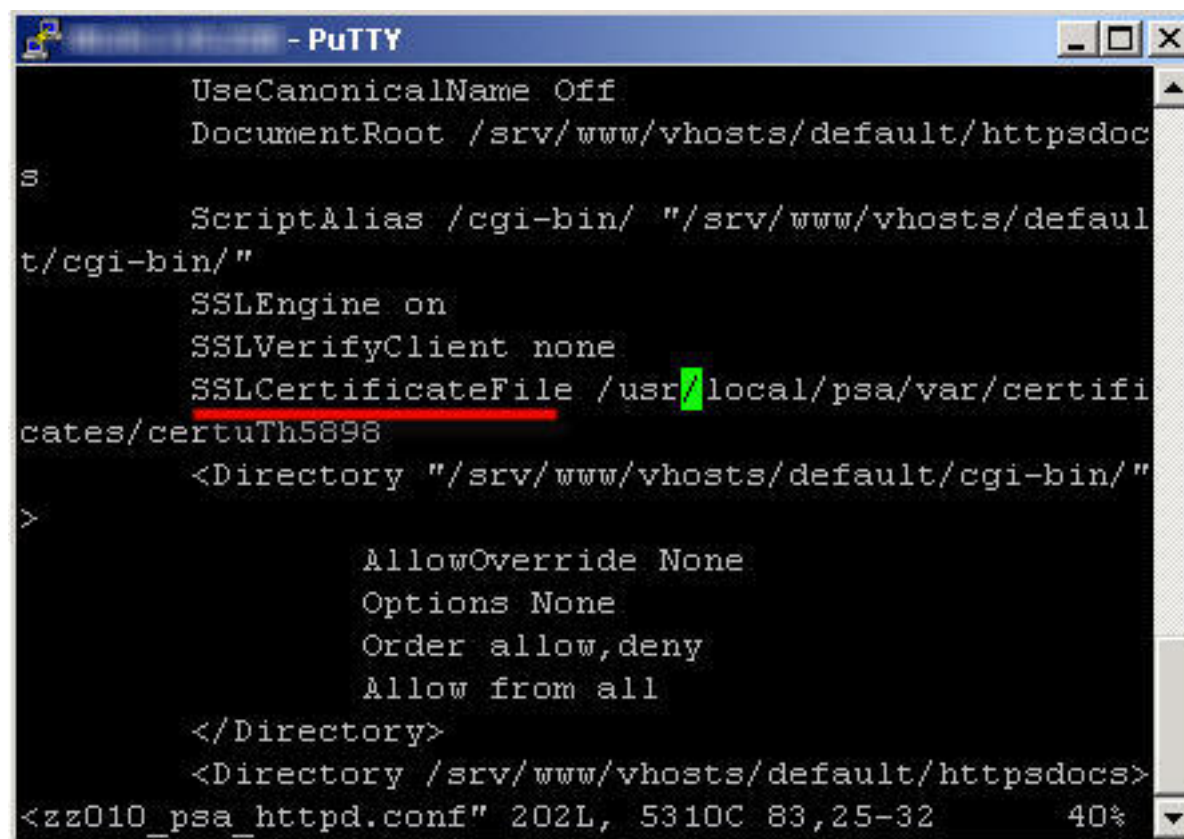
So geht's Schritt für Schritt:

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



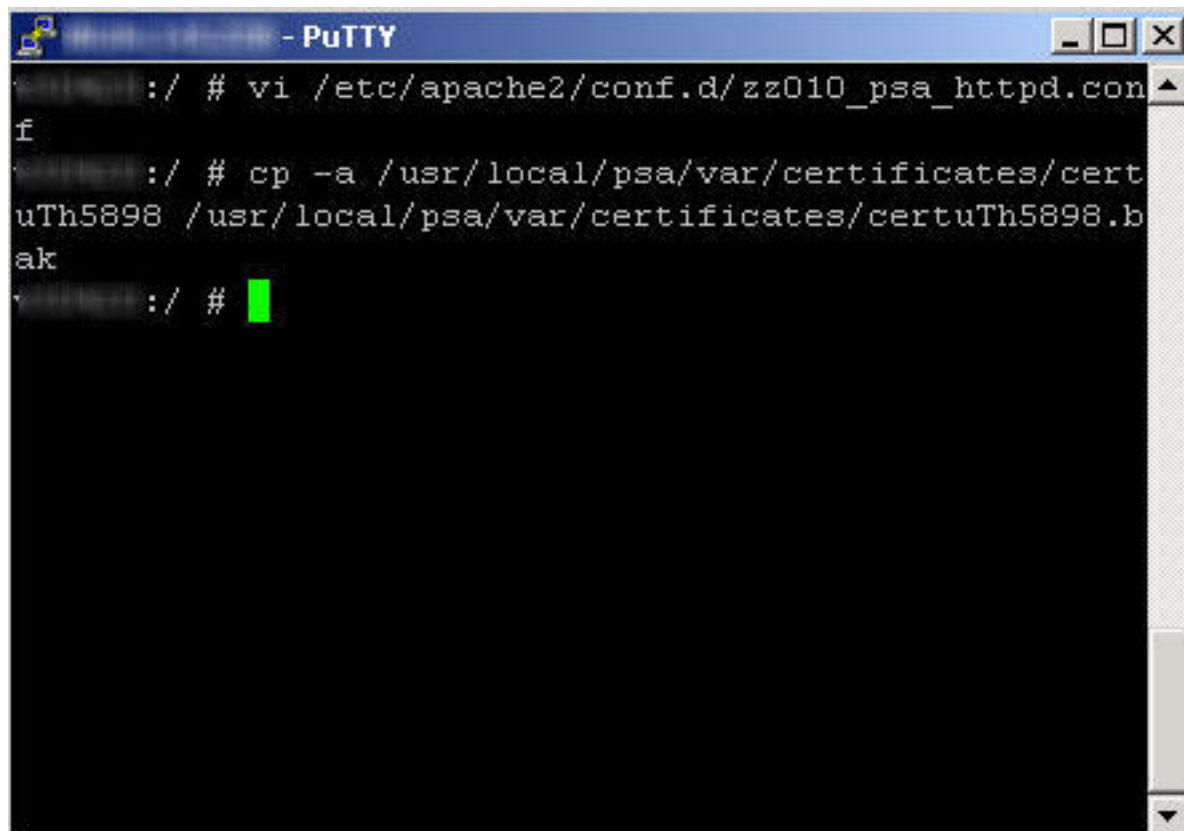
```
- PuTTY
UseCanonicalName Off
DocumentRoot /srv/www/vhosts/default/httpsdocs
ScriptAlias /cgi-bin/ "/srv/www/vhosts/default/cgi-bin/"
SSLEngine on
SSLVerifyClient none
SSLCertificateFile /usr/local/psa/var/certificates/certuTh5898
<Directory "/srv/www/vhosts/default/cgi-bin/"
>
    AllowOverride None
    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%
```

1blu-FAQ



```
- PuTTY
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%
```

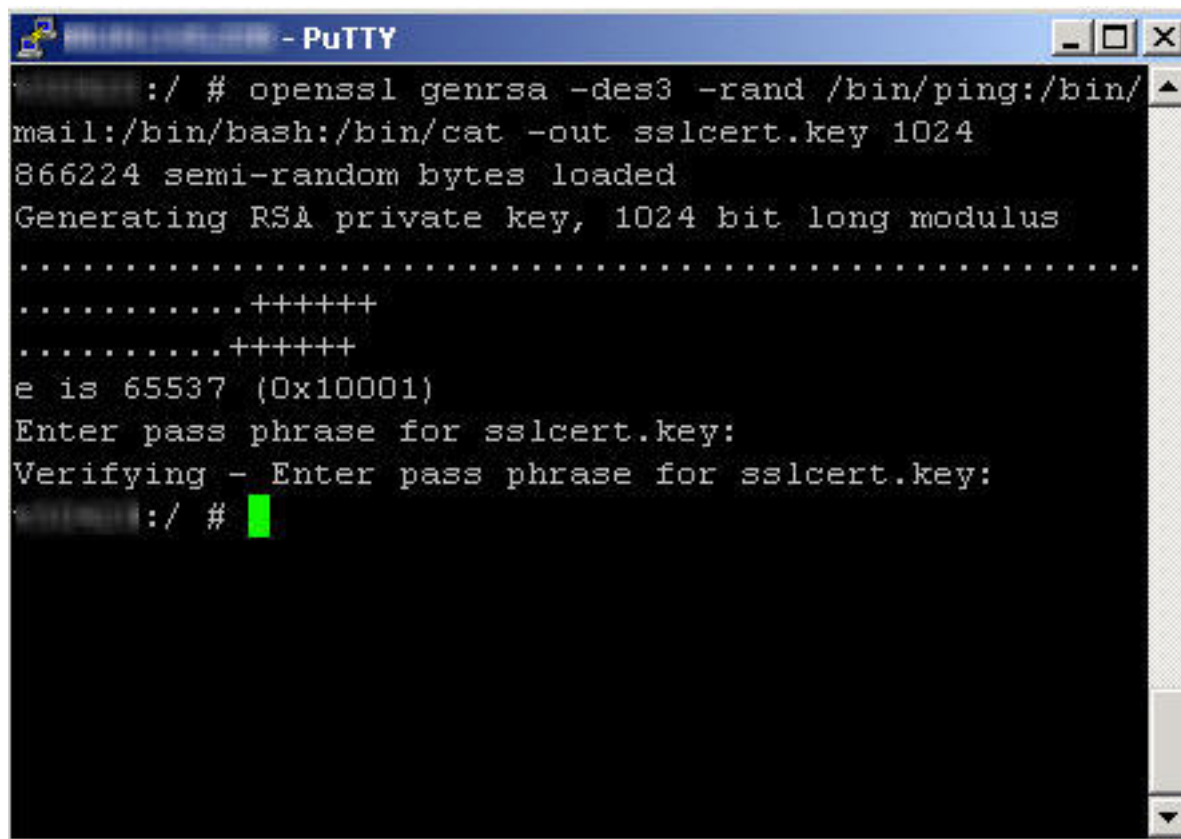
2. Sichern Sie diese Datei.



```
- PuTTY
root@localhost:~# vi /etc/apache2/conf.d/zz010_psa_httpd.conf
root@localhost:~# cp -a /usr/local/psa/var/certificates/certuTh5898 /usr/local/psa/var/certificates/certuTh5898.bak
root@localhost:~#
```

1blu-FAQ

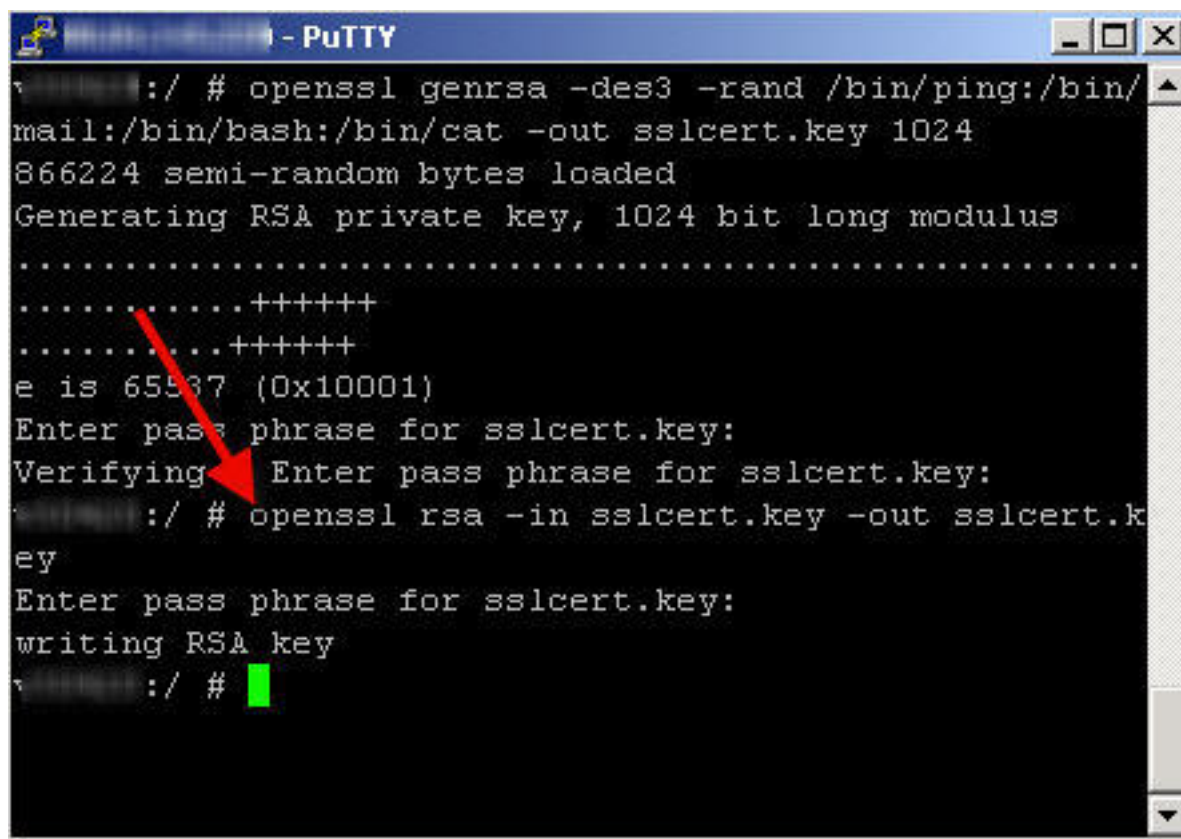
3. Erstellen Sie den **SSL Key** mit einer **1024 Bit Verschlüsselung**:

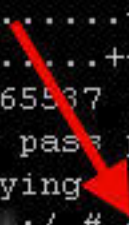


```
:/ # openssl genrsa -des3 -rand /bin/ping:/bin/mail:/bin/bash:/bin/cat -out sslcert.key 1024
866224 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....
.....++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for sslcert.key:
Verifying - Enter pass phrase for sslcert.key:
:/ #
```

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

1blu-FAQ



```
root@1blu:/ # openssl genrsa -des3 -rand /bin/ping:/bin/
mail:/bin/bash:/bin/cat -out sslcert.key 1024
866224 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....
.....++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for sslcert.key:
Verifying  Enter pass phrase for sslcert.key:
root@1blu:/ # openssl rsa -in sslcert.key -out sslcert.k
ey
Enter pass phrase for sslcert.key:
writing RSA key
root@1blu:/ # 
```

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



```
root@1blu:/ # openssl req -new -key sslcert.key -out ssl
cert.csr 
```

1blu-FAQ

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 AG

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!

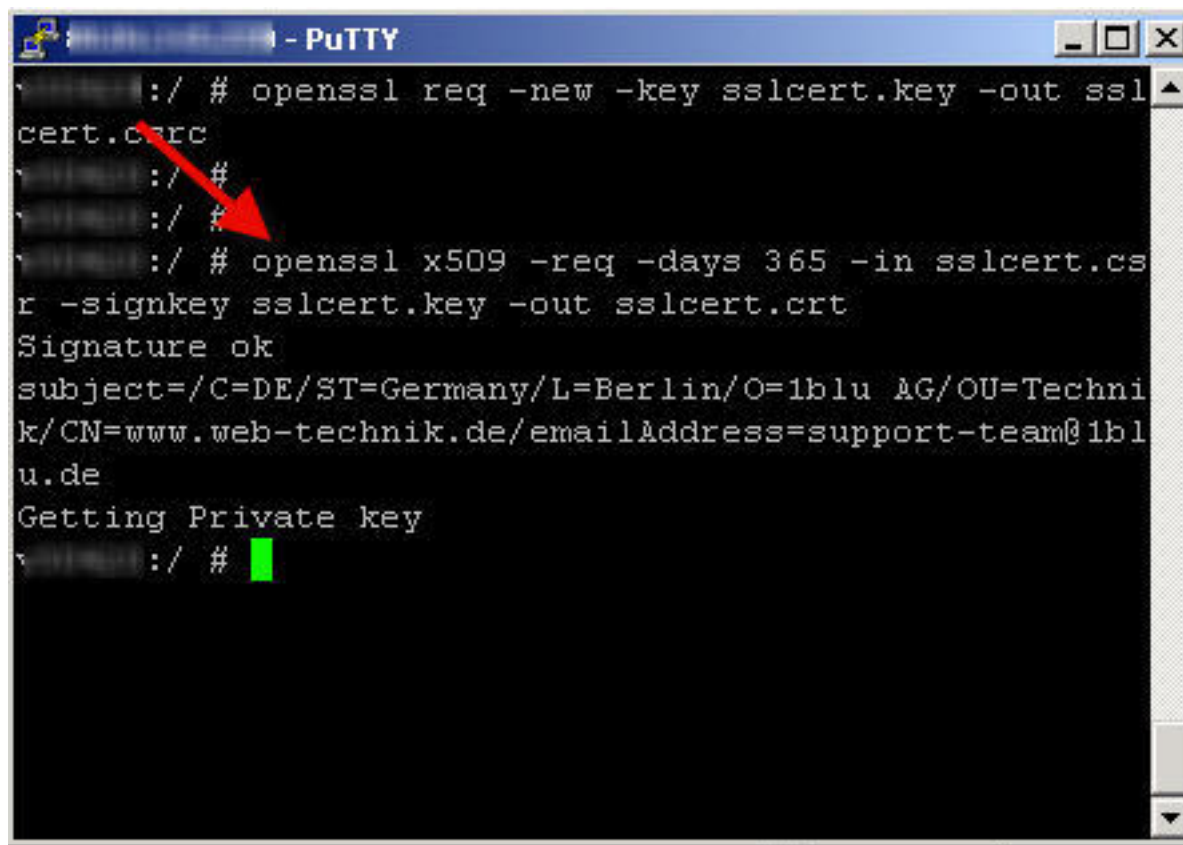
Email Address []: support-team@1blu.de

A challenge password []:

An optional company name []:

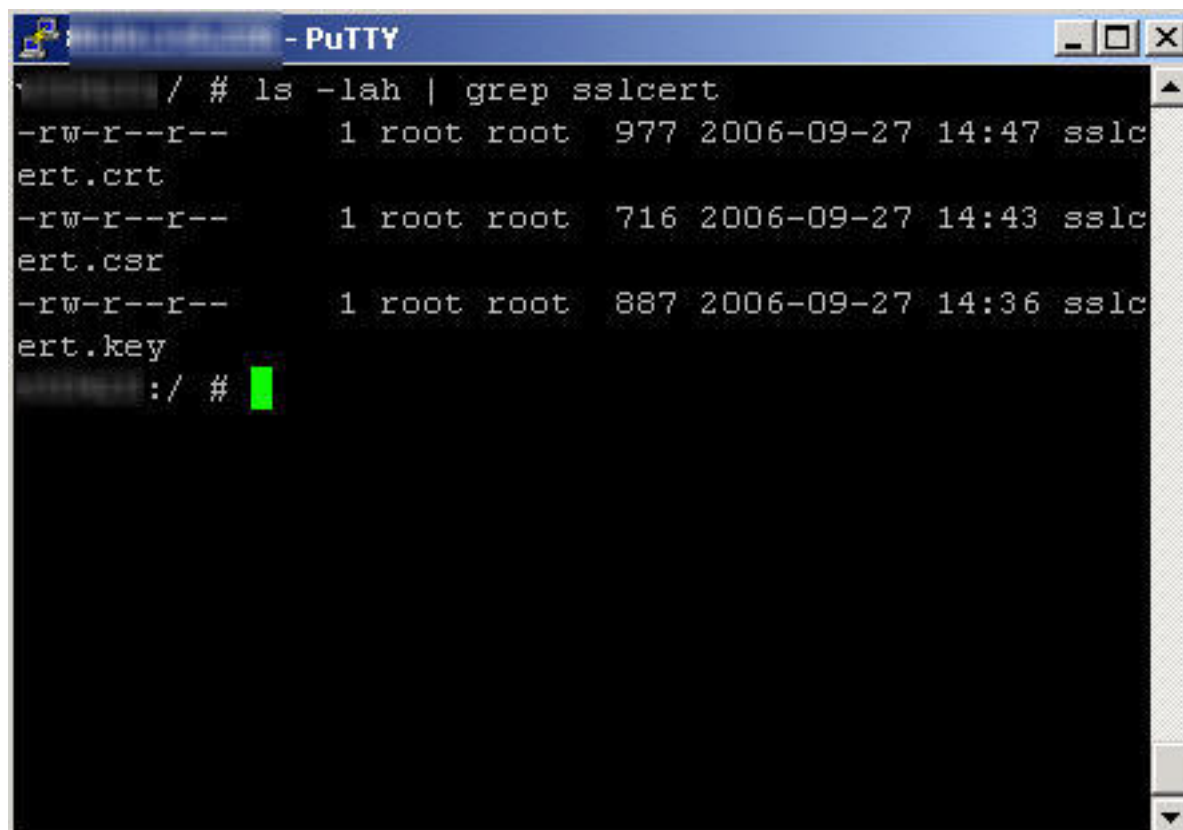
6. Erstellen Sie das selbstsignierte SSL Zertifikat:

1blu-FAQ



```
root@:/ # openssl req -new -key sslcert.key -out sslcert.csr
root@:/ #
root@:/ #
root@:/ # 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
root@:/ #
```

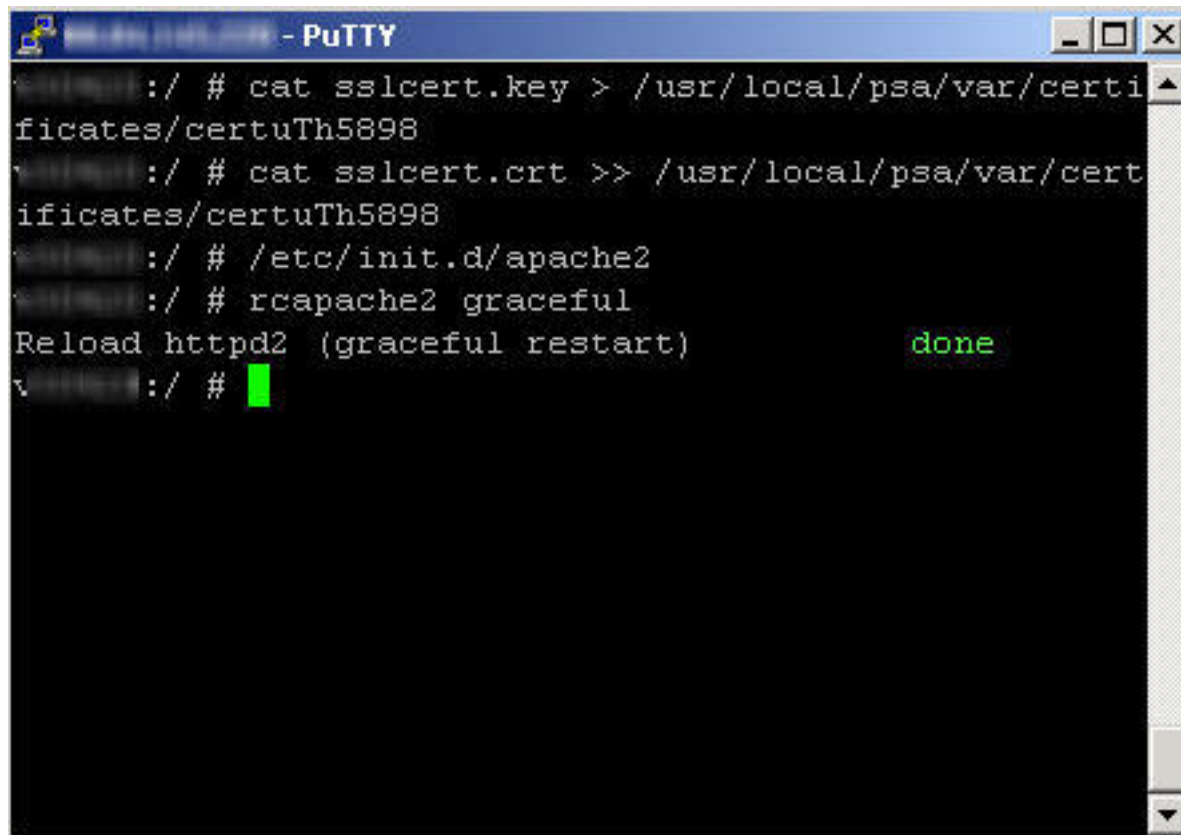
7. Es sollten im Working Directory **.key**, **.csr** und **.crt File** vorliegen:



```
root@/ # 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
root@:/ #
```


1blu-FAQ

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



```
root@psa:/usr/local/psa/var/certificates# cat sslcert.key > /usr/local/psa/var/certificates/certuTh5898
root@psa:/usr/local/psa/var/certificates# cat sslcert.crt >> /usr/local/psa/var/certificates/certuTh5898
root@psa:/usr/local/psa/var/certificates# /etc/init.d/apache2
root@psa:/usr/local/psa/var/certificates# rcapache2 graceful
Reload httpd2 (graceful restart) done
root@psa:/usr/local/psa/var/certificates#
```

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

1blu-FAQ

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: 2021-10-20 13:58