## Wie kann ich ein eigenes SSL Zertifikat für meinen virtuellen und Root-Server erstellen und hinterlegen? <u>Wie kann ich ein eigenes SSL Zertifikat für meinen virtuellen und Root-</u> <u>Server erstellen und hinterlegen?</u>

## **O**<u>Wichtiger Hinweis:</u>

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.

d'	- PuTTY	×
	UseCanonicalName Off	
	DocumentRoot /srv/www/vhosts/default/http	psdoc
s		
	ScriptAlias /cgi-bin/ "/srv/www/vhosts/de	efaul
t/cgi	i-bin/"	
	SSLEngine on	
	SSLVerifyClient none	
	SSLCertificateFile /usr <mark>/</mark> local/psa/var/ce	ctifi
cates	s/certuTh5898	
	<directory "="" cgi-}<="" default="" srv="" td="" vhosts="" www=""><td>oin/"</td></directory>	oin/"
>		
	AllowOverride None	
	Options None	
	Order allow, deny	
	Allow from all	
	<directory default="" https:<="" srv="" td="" vhosts="" www=""><td>docs&gt;</td></directory>	docs>
<zz01< td=""><td>10_psa_httpd.conf" 202L, 5310C 83,25-32</td><td>40% 🔽</td></zz01<>	10_psa_httpd.conf" 202L, 5310C 83,25-32	40% 🔽

# 1blu-FAQ



SSL

2. Sichern Sie diese Datei.



Seite 2 / 7 © 2025 1blu AG <info@1blu.de> |

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:

<u> </u>	- PuTTY	- O ×
n :/ # mail:/bin/k 866224 sem: Generating	openssl genrsa -des3 -rand /bin/ping bash:/bin/cat -out sslcert.key 1024 i-random bytes loaded RS) private key 1024 bit long modul	:/bin/ 🔺
e is 65387	<pre></pre>	
Enter pase Verifying · :/ # ev	phrase for sslcert.key: Enter pass phrase for sslcert.key: openssl rsa -in sslcert.key -out ssl	cert.k
Enter pass writing RSJ v :/ #	phrase for sslcert.key: A key	
		•

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



Seite 4 / 7 © 2025 1blu AG <info@1blu.de> |

# **1blu-FAQ**

SSL

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:



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

Seite 5 / 7

#### © 2025 1blu AG <info@1blu.de> |



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



Seite 6 / 7 © 2025 1blu AG <info@1blu.de> |

**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 <u>Thawte</u> oder <u>VeriSign</u> ein.

## **O**<u>Wichtiger Hinweis:</u>

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: 2021-10-20 13:58