

Apache Webserver neues Zertifikat beantragen und mit Zertifizierungskette installieren

Version 1.4
23. August 2011

QuoVadis Trustlink Schweiz AG
Poststrasse 17 | Postfach
9001 St. Gallen

Phone +41 71 272 60 60
Fax +41 71 272 60 61
www.quovadis.ch

Einleitung

Dieses Dokument beschreibt wie im Apache mit OpenSSL ein CSR (Certificate Signin Request) für ein SSL Zertifikat angefordert wird und das Zertifikat anschliessend mit dem Zwischenstellenzertifikat im Apache eingerichtet wird. Dieses Vorgehen ist mit dem Apache 2.2.8 und OpenSSL 0.9.8g getestet worden. Es wird davon ausgegangen, dass der Apache Server und OpenSSL installiert ist.

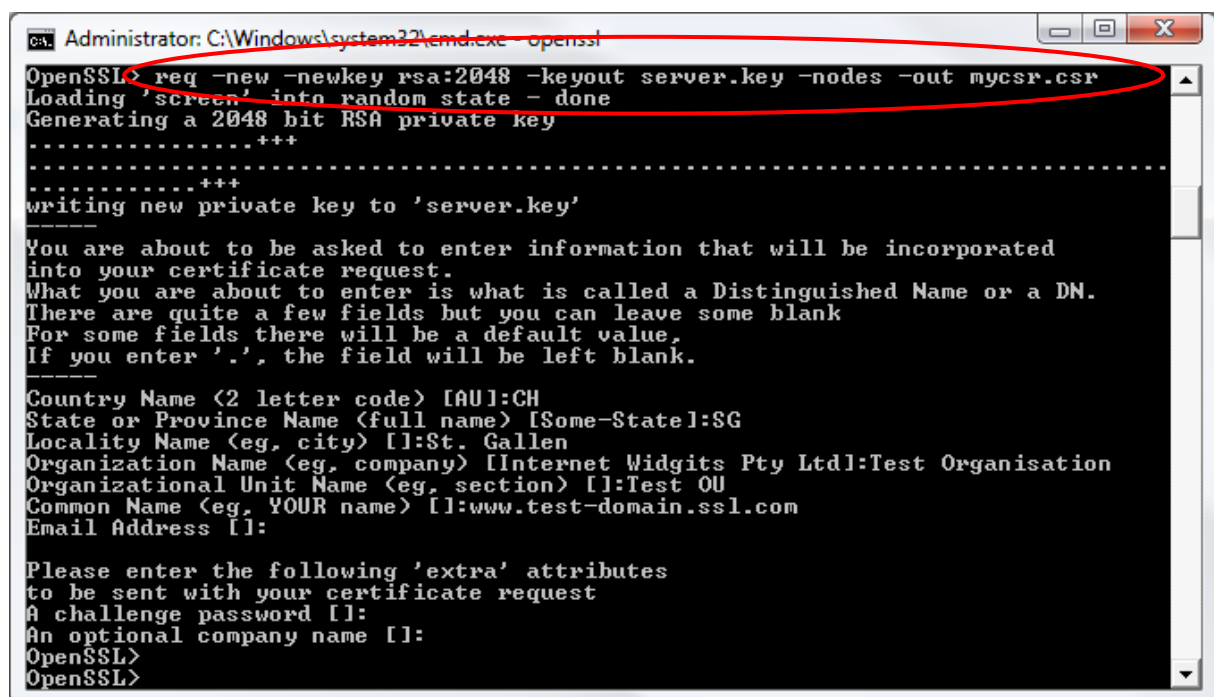
Übersicht Vorgehen

1. CSR und Key generieren mit OpenSSL
2. Stamm- und Zwischenstellenzertifikat herunterladen
3. Konfiguration des Apache (httpd.conf)
4. Überprüfung und Visualisierung

1. CSR und Key generieren mit OpenSSL

Mit OpenSSL muss zuerst der CSR und der PrivateKey generiert werden. Dazu ist der folgende Befehl auszuführen:

```
req -new -newkey rsa:2048 -keyout server.key -nodes -out mycsr.csr
```



```
Administrator: C:\Windows\system32\cmd.exe - openssl
OpenSSL> req -new -newkey rsa:2048 -keyout server.key -nodes -out mycsr.csr
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'server.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.

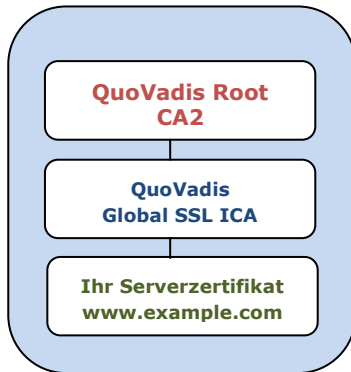
-----
Country Name (2 letter code) [AU]:CH
State or Province Name (full name) [Some-State]:SG
Locality Name (eg, city) []:St. Gallen
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Test Organisation
Organizational Unit Name (eg, section) []:Test OU
Common Name (eg, YOUR name) []:www.test-domain.ssl.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
OpenSSL>
OpenSSL>
```

Bitte senden Sie die Zertifikatsanfrage (CSR) an QuoVadis.
(register.ch@quovadisglobal.com)

2. Stamm- und Zwischenstellenzertifikat herunterladen

Um die Zertifizierungskette sicher zustellen muss das **Stamm-** und **Zwischenstellenzertifikat** (dieses beinhaltet das QuoVadis Root CA2 und Global SSL ICA) importiert werden. Diese laden Sie bitte hier herunter:



Stammzertifikat:
[Quovadis Root CA2](#)

Zwischenstellenzertifikat:
[QuoVadis Global SSL ICA](#)

Ihr Serverzertifikat: Dieses haben Sie per e-Mail erhalten

Bitte kopieren Sie den Inhalt der Textfeldes (inkl. -----BEGIN CERTIFICATE----- und -----END CERTIFICATE-----), fügen es in einen Texteditor ein und speichern es auf ihrem Webserver mit den folgenden Dateinamen im nächsten Kapitel.
([qvrca2.crt](#), [intermediate_bundle.crt](#), [server.crt](#))

3. Konfiguration des Apache

Erstellen Sie einen Unterordner „ssl“ im Apache-Konfigurationsverzeichnis und kopieren Sie die Dateien

Fügen Sie folgende Zeilen ein:

Listen 80
Listen 443

Aktivieren Sie:

```
LoadModule ssl_module modules/mod_ssl.so
```

Fügen oder ergänzen Sie folgende Zeilen ein :

```
<IfModule ssl_module>
    SSLRandomSeed startup builtin
    SSLRandomSeed connect builtin
    SSLSessionCache none
</IfModule>
```

Konfiguration virtueller Host für das Port 443

```
<VirtualHost ssl.qvtest.ch:443>
    ServerName ssl.qvtest.ch
    SSLEngine On
#QuoVadis Root CA2
    SSLCACertificateFile /etc/apache2/ssl/qvrca2.crt
#QuoVadis Global SSL ICA
    SSLCertificateChainFile /etc/apache2/ssl/intermediate_bundle.crt
#Ihr Serverzertifikat
    SSLCertificateFile /etc/apache2/ssl/server.crt
#Privater Schlüssel Ihres Servers
    SSLCertificateKeyFile /etc/apache2/ssl/server.key

</VirtualHost>
```



Hinweis

Die Zeile SSLCertificateChainFile stellt sicher, dass der Zertifizierungspfad verifiziert werden kann.

Starten Sie den Apache-Service neu.

4. Überprüfung und Visualisierung

Überprüfen Sie die abgeschlossene SSL Installation mit QuoVadis [PKI Widgets](#), den nützlichen Helfern für elektronische Zertifikate.



Das Site Seal ist ein Zeichen dafür, dass Sie Ihre Website mit einem QuoVadis SSL Zertifikat schützen. Die Besucher Ihrer Website können dies mit einem Klick auf das interaktive Siegel selbst prüfen. Installieren Sie jetzt das [QuoVadis Site Seal](#).