



QUOVADIS SSL CERTIFICATES & SOURCE GEAR

Effective Date: March 1st, 2003
Version: 1.1



Copyright © QuoVadis 2001. All rights reserved. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by QuoVadis.

Important Note About this Document

The information contained in this document is intended for personnel charged with the implementing QuoVadis Digital Security with Source Gear suite of products. QuoVadis Ltd. takes no liability for the operation or the implementation of SSL certificates into the Source Gear suite of products. This documentation is used completely at the users own risk.

QuoVadis Ltd. is a Commercial Certificate Authority located in Bermuda catering to the digital security needs of international business. For more information or to contact QuoVadis Ltd. please visit our website at <http://www.quovadis.bm>.

Version Control

Author	Date	Version	Comments
QuoVadis Ltd.	March 1 st , 2004	1.0	Original Document.
QuoVadis Ltd.	April 12 th , 2004	1.1	Updated RNG script.

Table of Contents

1. Introduction	1
2. Generating the Certificate Signing Request.....	2
3. Installing the QuoVadis SSL Certificate.....	5
4. Important Links	6

1. Introduction

The Source Offsite Collaboration Server is an extension of Microsoft Visual SourceSafe, allowing developers to access source code, track bugs and progress through a convenient web interface. As many organizations hold much of their intellectual property in the source code that runs their mission critical applications, they realize the importance of ensuring that this source code is accessed over encrypted channels.

As a result, the default installation of Source OffSite Collaboration Server generates a self signed SSL certificate which protects the content on the web interface. By forcing this SSL connection, the sessions between developers and the SOS web interface are encrypted using 128 bit technology.

QuoVadis recommends taking this an extra step and installing a commercial SSL certificate, which ensures the identity of the server and eliminates the problems associated with self-signed certificates. This document outlines the manual steps required to install a commercial SSL certificate.

2. Generating the Certificate Signing Request

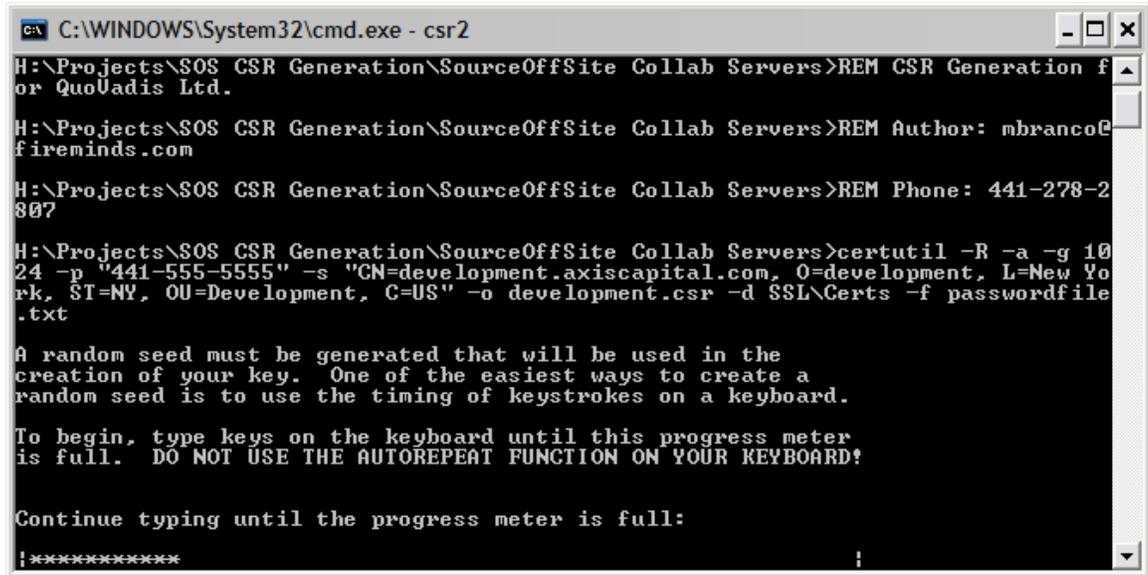
Once you have the Source OffSite Collaboration Server installed, you will need to generate a CSR which can be sent to QuoVadis for processing.

You must generate a CSR directly from the SourceOffsite Collab Server. This is done using the Netscape certutil tool. You cannot generate the CSR from another tool such as Microsoft certutil or IIS. The instructions below assume that you have the SOS Collab Server installed in the default location (C:\Program Files\SourceOffSite Collab Servers).

1. STOP all SourceOffSite services. If you don't it will corrupt your Certificate DB files. This is done by right mouse clicking on the SOS Server Administrator in the System Tray and stopping both the Primary & Web Server services.
2. Extract ZIP file to a temporary directory. You should copy the following files into C:\Program Files\SourceOffSite Collab Servers.
 - csr.bat
 - passwordfile.txt
3. Update "passwordfile.txt" with your SourceOffsite SSL Certificates password, which can be found by accessing the SOS Server Administrator and clicking on the SSL tab.
4. Update the csr.bat file with your company specific parameters. The following sample file has the values that you must customize.

```
-----  
REM CSR Generation for QuoVadis Ltd.  
REM Author: mbranco@fireminds.com  
REM Phone: 441-278-2807
```

```
certutil -R -a -g 1024 -p "441-555-5555" -s "CN=development.axiscapital.com,  
O=development, L=New York, ST=NY, OU=Development, C=US" -o development.csr -d  
SSL\Certs -f passwordfile.txt  
-----
```



```
C:\WINDOWS\System32\cmd.exe - csr2
H:\Projects\SOS CSR Generation\SourceOffSite Collab Servers>REM CSR Generation for QuoVadis Ltd.
H:\Projects\SOS CSR Generation\SourceOffSite Collab Servers>REM Author: mbranco@fireminds.com
H:\Projects\SOS CSR Generation\SourceOffSite Collab Servers>REM Phone: 441-278-2807
H:\Projects\SOS CSR Generation\SourceOffSite Collab Servers>certutil -R -a -g 1024 -p "441-555-5555" -s "CN=development.axiscapital.com, O=development, L=New York, ST=NY, OU=Development, C=US" -o development.csr -d SSL\Certs -f passwordfile.txt
A random seed must be generated that will be used in the
creation of your key. One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.
To begin, type keys on the keyboard until this progress meter
is full. DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!
Continue typing until the progress meter is full:
|*****|
```

* Note you will be prompted to enter random text which will be used to seed the certificate.

- Phone Number (-p): List your contact number, this number is not included in the certificate but is used if there is a problem in generating your new SSL certificate.
 - Common Name (CN): This is the external address of your server which is used to access it. Ensure that you input the correct address.
 - Organization (O): This is your organization name that will appear on the SSL certificate.
 - Locale (L): This is the locality that will appear on your SSL certificate, this value usually matches the city of the organization.
 - State (ST): This is the state, region, province or parish of the organization. This value is typically abbreviated to two characters.
 - Organizational Unit (OU): This is the department or division of the organization which will appear on the SSL certificate.
 - Country (C): This is the country of the organization which will appear on the SSL certificate.
5. Run csr.bat at a command line
 6. Email QuoVadis your CSR file (i.e. development.csr).

QuoVadis will process your CSR once it has received completed paperwork as required on <http://www.quovadis.bm/identity/buyssl.asp>. QuoVadis will email you the certificate response within 1 business day of completed SSL requests.

3. Installing the QuoVadis SSL Certificate

Once you receive the SSL certificate from QuoVadis you can follow the manual steps listed below to install the certificate. Once you receive a response file from QuoVadis (i.e. development.crt), you will need to install the certificate.

1. STOP all SourceOffSite services. If you don't it will corrupt your Certificate DB files
2. At the command line go to the SourceOffsite application directory (i.e. C:\Program Files\SourceOffSite Collab Servers)
3. Copy the certificate response file (i.e. development.crt) to this directory
4. Run the following command:

```
certutil -A -n development.quovadis.bm -t "u,u,u" -i development.crt -d SSL\Certs
```
5. You may check your install by typing the following command:

```
certutil -L -d SSL\Certs
```
6. Start both the Primary Server & Web Server.
7. Go to the website address and check that the certificate is now loading under HTTPS.

4. Important Links

QuoVadis Ltd: www.quovadis.bm

Source Gear: www.sourcegear.com