Application Note – AN1502

Generate SSL Certificates

Rev. 1

2015/08/21

Content

Overview

In order to ensure secure transactions between the PPBE web service and browsers, users can upload their own digital certificates. Users can sign their own digital certificates, which are called self-signed certificates, or provide the certificates that are issued by the certificate authority or certification authority (CA), which is a trusted third-party. As users trust the certificate, therefore they also trust the owner who signs this certificate. All data between the PPBE web service and browsers will be encrypted.

Obtain a SSL Certificate in KeyStore Instance

Follow the below steps to generate a SSL certificate. Please make sure that the **OpenSSL** toolkit is installed on your system. If your system is not installed the **OpenSSL** toolkit, refer to **Prepare OpenSSL Toolkit** section.

1. Switch to ***<OpenSSL_Installation_Directory>>.***

cd <OpenSSL_Installation_Directory>

<OpenSSL_Installation_Directory> is the absolutely path of the installation directory of **OpenSSL** toolkit. All generated files mentioned in the following steps will be placed here in the *<OpenSSL_Installation_Directory>* directory.

2. **Generate a private key.**

openssl genrsa -des3 -out server.key 2048

```
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
....+++
.....................................+++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

3. **Generate a CSR (Abbreviation for Certificate Signing Request)**

openssl req -new -key server.key -out server.csr

Generate a certificate signing request once the private key is generated. The CSR can be self-signed which demonstrates in next step or can be delivered to the certificate authority. Users will be prompted to provide the further information of the certificate during generating a CSR.

To users which would like generate a self-signed SSL certificate, go to step 4; to users which would like apply for SSL certificate to the trusted 3rd party certificate authority, go to step 5.

```
Enter pass phrase for server.key:
Loading 'screen' into random state - done
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]:US
State or Province Name (full name) [Some-State]:Minisota
Locality Name (eg, city) []:Shakopee
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CyberPower Systems (USA), Inc.
Organizational Unit Name (eg, section) []:Tech Support
Common Name (e.g. server FQDN or YOUR name) []:cyberpowersystems.com
Email Address []:sales@cpsww.com

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

***Note**: "Common Name" should be filled in with 127.0.0.1, fully qualified domain name of server to be protected or the host IP that PPBE has been installed.*

4. Generate a self-signed certificate.

openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

During the generation a self-signed certificate, a pass phrase mentioned in step 2 is required.

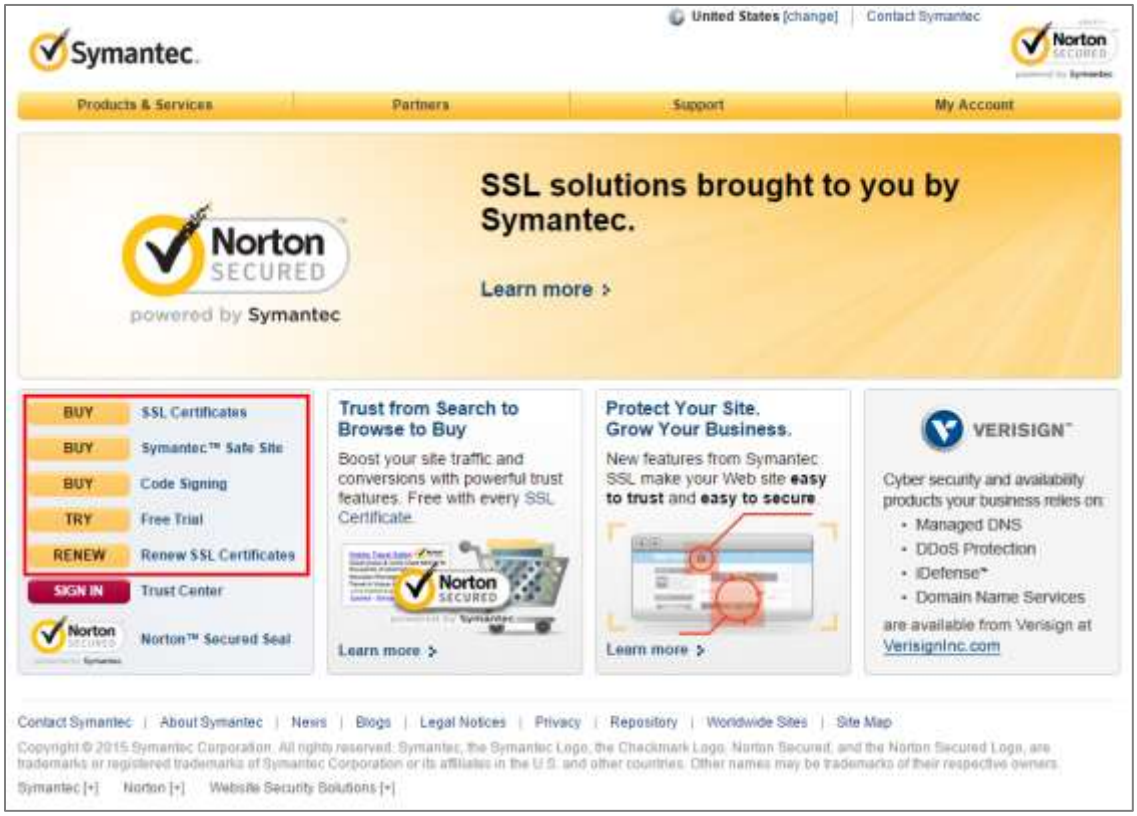
```
Loading 'screen' into random state - done
Signature ok
subject=/C=US/ST=Minisota/L=Shakopee/O=CyberPower Systems (USA), Inc./OU=Tech Support/CN=cyberpowers
ystems.com/emailAddress=sales@cpsww.com
Getting Private key
Enter pass phrase for server.key:
```

After the self-singed certificate is generated, go to step 6.

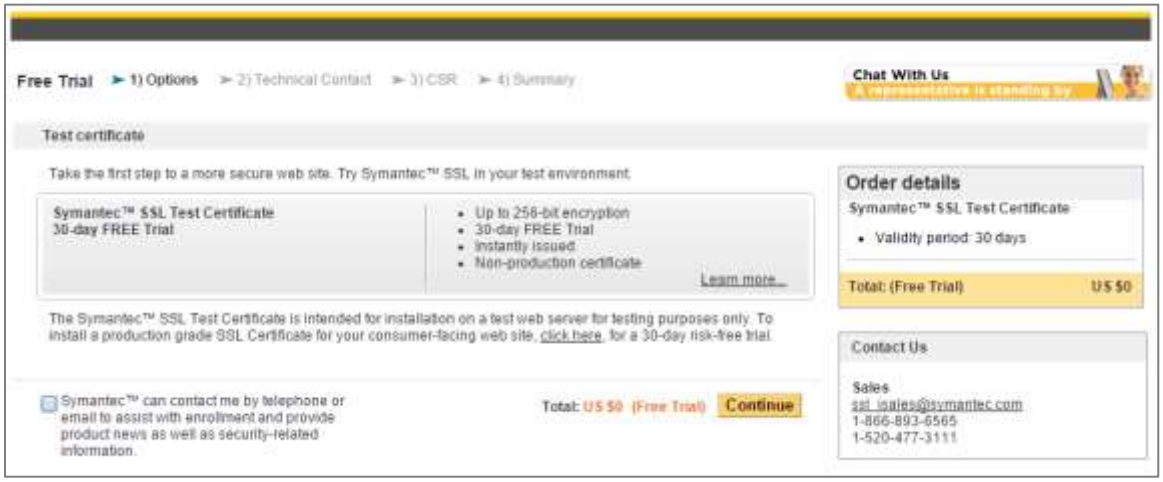
5. Deliver CSR to Certificate Authority

After the generation of certificate signing request, CSR can be delivered to the certificate authority (CA) to verify the identity and issue a signed certificate. Following steps demonstrates how to deliver a CSR to Symantec trust center and get a signed certificate.

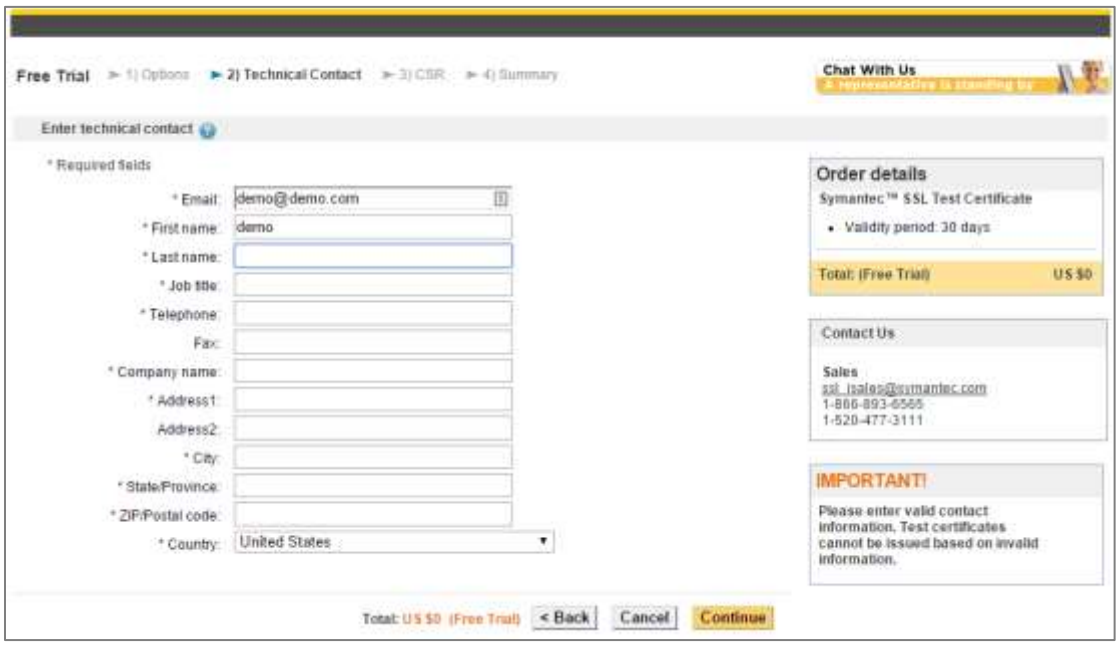
a. Access the Verisign website (Symantec Authentication Services provider). In this step, click **TRY** as a sample step to apply for a signed certificate.



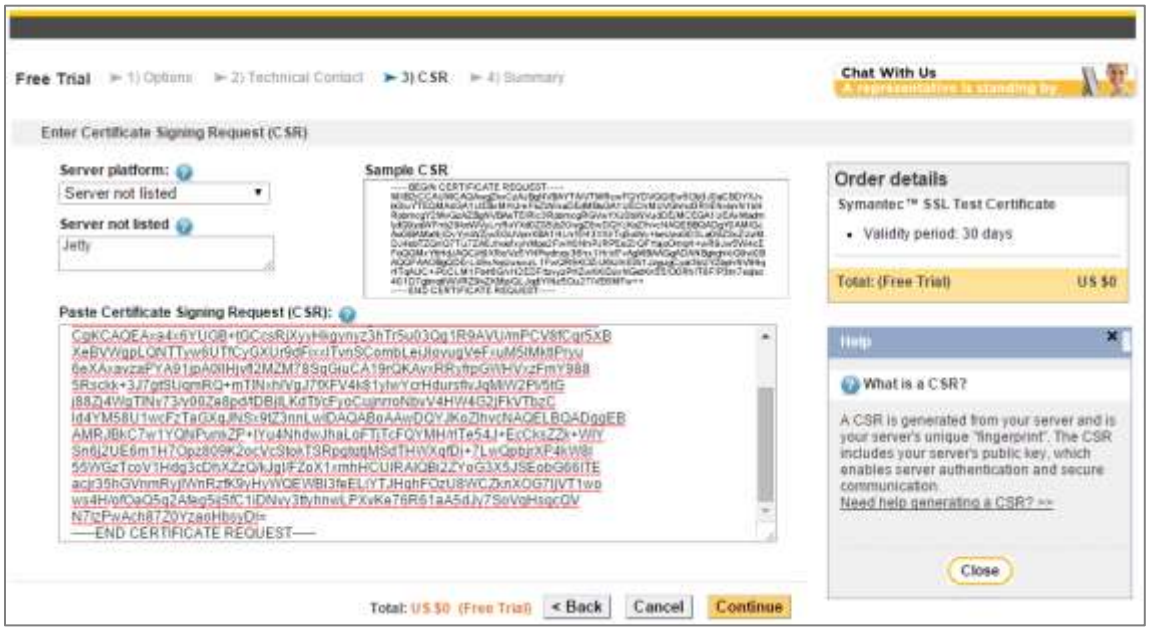
b. Click **Continue** to the next step.



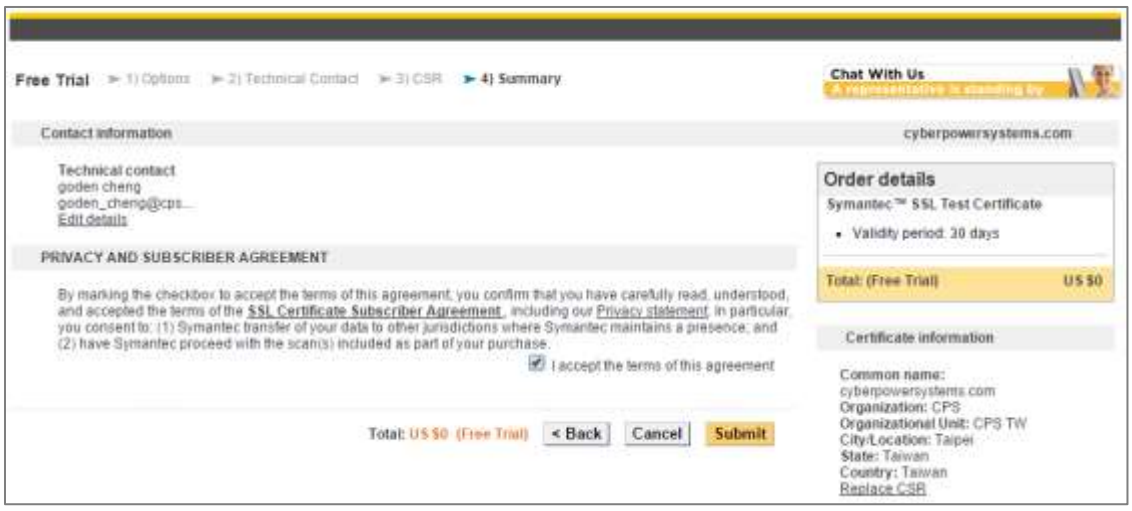
c. Fill in with all required data. Click **Continue** to the next step.



d. Open the **server.csr** in the notepad. Copy the entire content and past the **Paste Certificate Signing Request (CSR)** field. Click **Continue** to the next step.



e. Click **I accept the terms of this agreement** to accept the agreement**.** Click **Submit** to apply for a signed certificate.



f. After Symantec verifies and approves the application, an e-mail including the signed certificate will be sent. Copy the signed certificate and save as **server.crt** file in the <*OpenSSL_Installation_Directory*> folder.

ORDER NUMBER: 788812180
COMMON NAME: LOCALHOST

Dear goden cheng,

Congratulations! Symantec has approved your request for a Trial SSL Certificate, and is included at the end of this email.

In order for your Trial SSL Certificate to function properly, perform all the 3 steps below:

Step 1. Download and install the Test Root CA Certificate.

Open the link below and follow the steps to install the Root certificate in your internet browser:
https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=SO10670

Step 2. Download the Trial SSL Intermediate CA Certificate.

To download the Trial Intermediate CA on each Web server you are testing with, go to:
https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR1737

Note: Microsoft Internet Information Services (IIS) 5.0 and above automatically installs the Intermediate CA Certificate when you install the SSL Certificate and does not require separate installation and can skip this step. All

other Web servers require you to install the Intermediate CA separately.

***Note**: Each certificate from the commercial Certificate Authority (CA) may be subject to the certificate authority fee.*

***Note:** The workflow to apply for a SSL certificate will varies by the 3rd party Certificate Authority. Please contact the Certificate Authority for further information.*

6. **Combine the certificate (server.crt) and site key (server.key) and export it in pkcs12 format (server.pkcs12).**

   openssl pkcs12 -inkey server.key -in server.crt -export -out server.pkcs12

```
Loading 'screen' into random state - done
Enter pass phrase for server.key:
Enter Export Password:
Verifying - Enter Export Password:
```

7. **Import the certificate into the keystore (keystore).**

   *For **Linux**, run the keytool -importkeystore -srckeystore server.pkcs12 -srcstoretype PKCS12 -destkeystore keystore command.*

   *For **Windows**, run the "<PPBE_Installation_Directory>\jre\bin\keytool.exe" -importkeystore -srckeystore server.pkcs12 -srcstoretype PKCS12 –destkeystore command.*

   <PPBE_Installation_Directory> is the absolute path of PowerPanel Business Edition installation directory.

```
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias 1 successfully imported.
```

Import SSL Certificates

The **Security/Network** page allows users to import your own SSL certificate. The generated keystore file is placed in the *<OpenSSL_Installation_Directory>* directory. Users can import the certificates as following steps:

- Click the **Settings** button to switch the *SSL Certificates Wizard*.
- Click the **Import** button to upload the SSL certificate file.
- Enter the *Key Passphrase* field and the *Keystore Password* field. Click the **Continue** button to import the SSL certificates. *Key Passphrase* is the pass phrase to access the private key mentioned in step 2 and *Keystore Password* is the password for keystore mentioned in step7 in the **Obtain a SSL Certificate in Keystore Instance** section.

***Note:** When importing a SSL certificate, you should notice below:*

- *If the keystore file is not generated from the pkcs12 format file, enter the key passphrase of private key to the Key Passphrase field and the keystore password to the Keystore Password field.*
- *If the keystore file is generated from the pkcs12 format file:*
  - *The private key has been assigned a key passphrase. The key passphrase should be matched with the keystore password.*
  - *The private key has been not assigned. Enter the keystore password as the key passphrase to the Key Passphrase field.*

Prepare OpenSSL Toolkit

Install the **OpenSSL** toolkit first before you generate a SSL certificate. You should install the latest stable version from the **OpenSSL** website:

For **Linux** users:

- http://www.openssl.org/source/

For **Windows** users, download the latest installer.
(32-bit installer format is **Win32 OpenSSL vX.X.X**; 64-bit installer format is **Win64 OpenSSL vX.X.X**. **X.X.X** is the version number.):

- http://slproweb.com/products/Win32OpenSSL.html

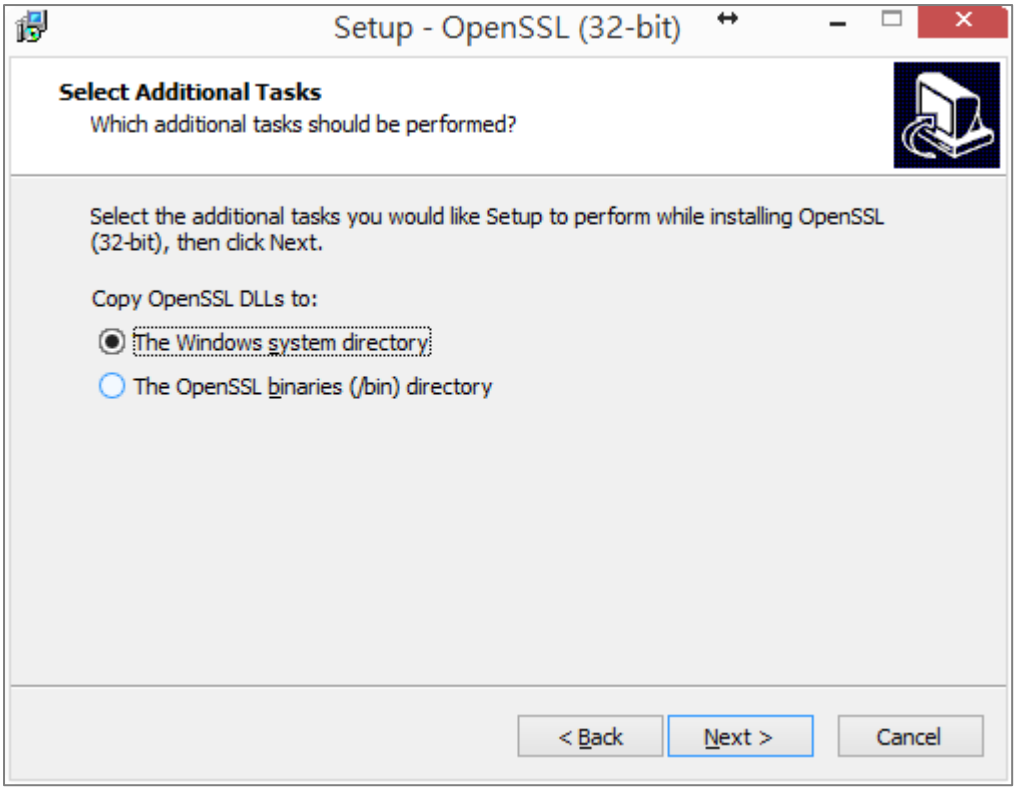
For other operating systems, please refer to **OpenSSL** website for further details.

- http://www.openssl.org/about/binaries.html

You should install the appropriate version for your operating system. In most Linux distributions, the toolkit is usually placed at */usr/local/ssl/bin* directory. You can run the below command to find the directory.

```
find / -name openssl -print
```

In the Windows platforms, you should select the **The Windows system directory** option of the **Select Additional Tasks** screen during installation.



You can use below command to make sure that that version is not affected by *Heartbleed* bug. If your version is affected by *Heartbleed* bug, please upgrade to the fixed version.

openssl version

The versions which are affected by *Heartbleed* bug: **1.0.1** – **1.0.1f** / **1.0.2-beta – 1.0.2-beta1**.

The versions whose *Heartbleed* bug has been fixed: **1.0.1g** / **1.0.2-beta2 ~ 1.0.2.**