**HTTPS Configuration**

Domain name: **webtech2.secure.org**

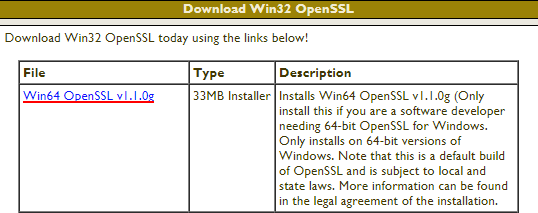
Pre-req: (This is assuming that readers are already aware of adding a website to IIS, as the following involves merely configuration.)

HTTPS is a secure version of HTTP, encrypting the connection between browsers and websites. This means that any data input cannot be read by anyone else, and is often used for online transaction such as purchases and banking. Two protocols are generally used: Secure Sockets Layer and Transport Layer Security, both using public and private keys that cannot be decrypted without the other.

In order to achieve HTTPS on a website, a SSL certificate trusted by a trusted authority should be bound to the site. The following demonstrates creating a self-signed certificate using OpenSSL, a toolkit/software library for the two protocols mentioned above.

**A. Installing OpenSSL**

1. To download the latest version, visit OpenSSL’s git repository at: https://github.com/openssl/openssl. However, this requires different installation specifications, as stated in their INSTALL note. To keep things simple, we will use Windows binaries, located at https://slproweb.com/products/Win32OpenSSL.html.
2. Scroll down and pick the binary of your choice.

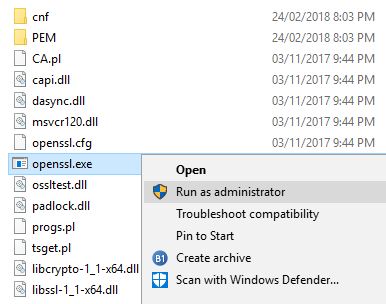


1. Execute the installer, choose the installation destination, and wait for it to finish.

Note: it is recommended to install outside of Windows system directory in **/bin**.

**B. Generating a Self-Signed Certificate Using OpenSSL**

1. Go to OpenSSL’s installation folder and find *openssl.exe* in the **bin** folder. Run the program as an administrator.

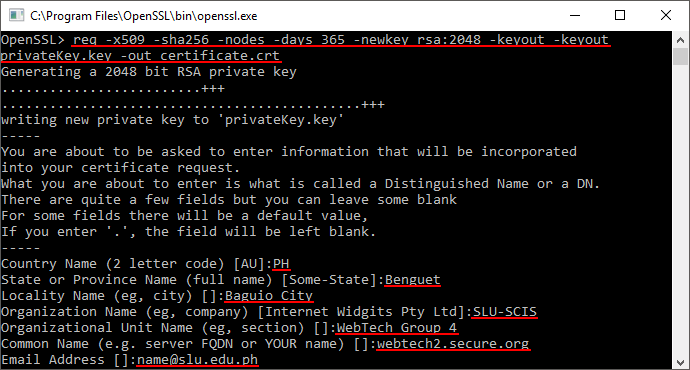
****

1. To create a self-signed certificate, use the following command:

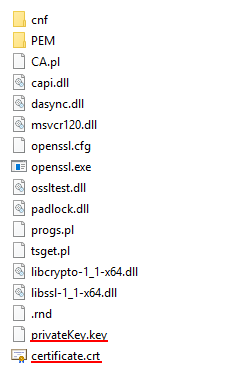
|  |
| --- |
| req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout privateKey.key -out certificate.crt |

Note: this creates a self-signed X.509 certificate with RSA-2048 encryption. **privateKey.key** specifies the name of the key; **certificate.crt**, the certificate. Both are changeable to your specifications. **-nodes** specify that no password is needed for the key.

1. Follow the onscreen instructions, and fill in the certificate details, like so:

****

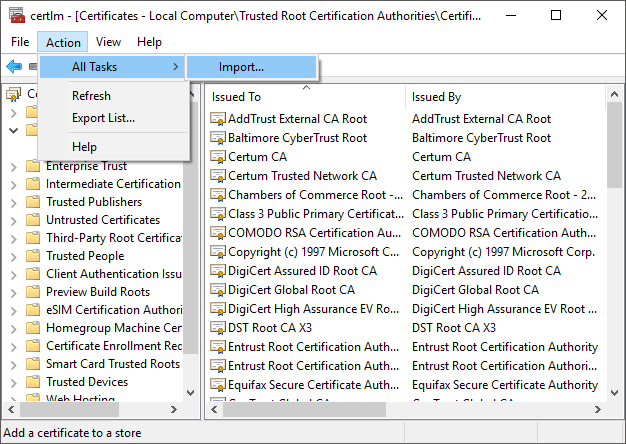
1. You will find two files in the **bin** folder, respectively named **privateKey.key** and **certificate.crt**.



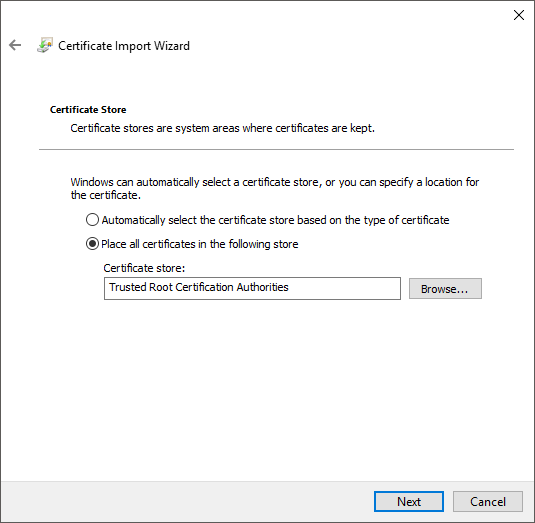
**C. Installing the Certificate**

By default, a **certificate.crt** will state that it isn’t trusted, and will require the user to install the certificate.

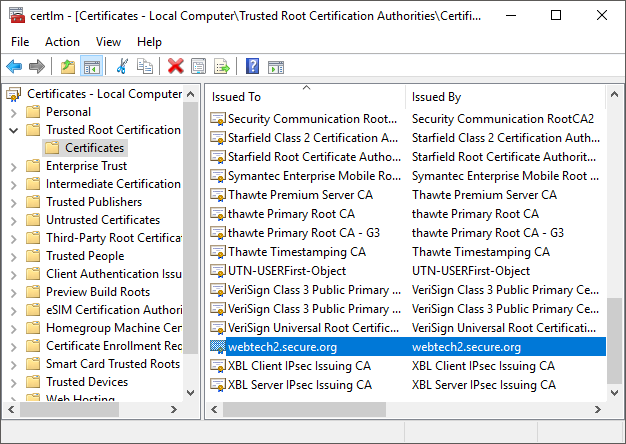
1. Open *Microsoft Management Console* either through Control Panel (typing ‘Manage Computer Certificates’) or by directly searching it through Start.
2. Import the certificate: **Action > All Tasks > Import**.



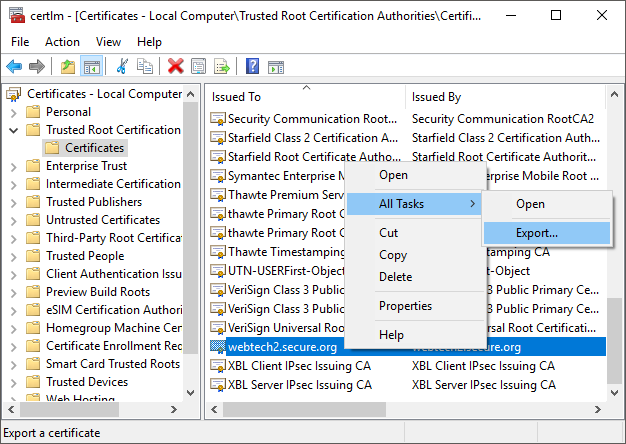
1. A new window should pop up. Follow the instructions, and fill out the appropriate data in the fields. Specify the certificate name and location, and ensure that the certificate is placed in the store: **Trusted Root Certification Authorities**.



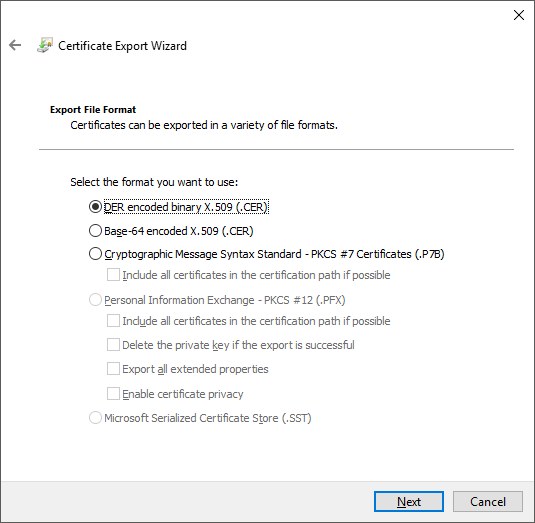
1. Once imported, the certificate should be properly installed or added. To check, go to *Trusted Root Certification Authorities*, and click on **Certificates**. Your recently-added certificate should be located in the list.



1. In order to use the certificate in IIS, you require a **.cer** file to complete the certificate request. Simply right-click your certificate, and click **All Tasks >** **Export**.



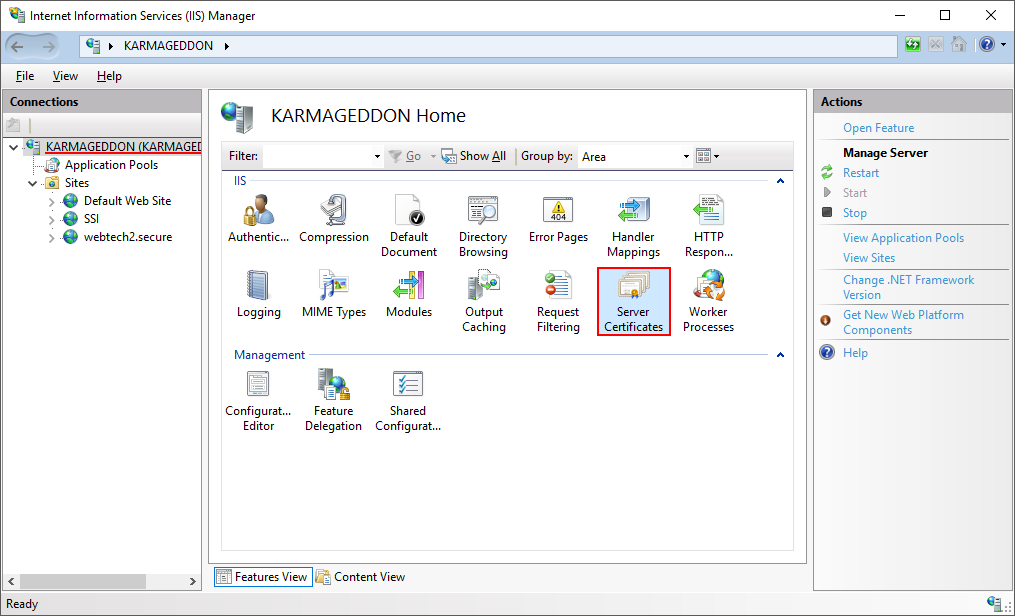
1. A new window should pop up. Follow the instructions, and fill out the appropriate data in the fields. The format to be used should be **DER encoded binary X.509**, and specify the file name and location.



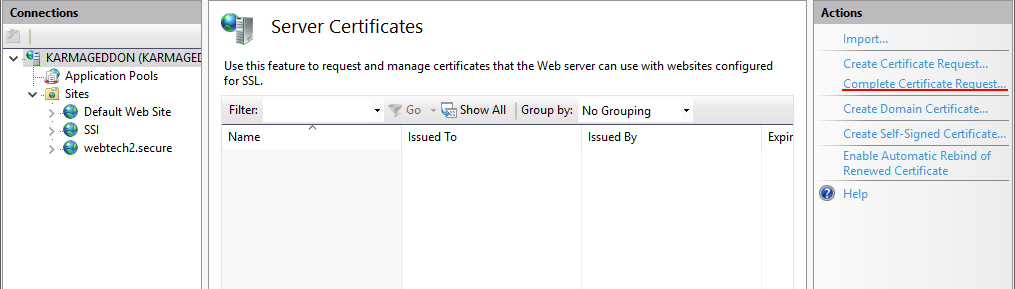
1. The **.cer** file should now appear in wherever you had saved it.

**D. Enabling SSL on IIS Using Self-Signed Certificates**

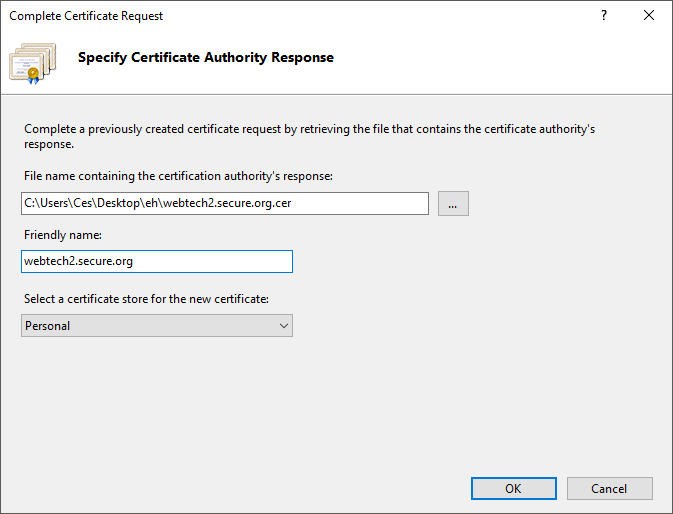
1. Open *Internet Information Services* (IIS) and click on **Server Certificates** on the root host.



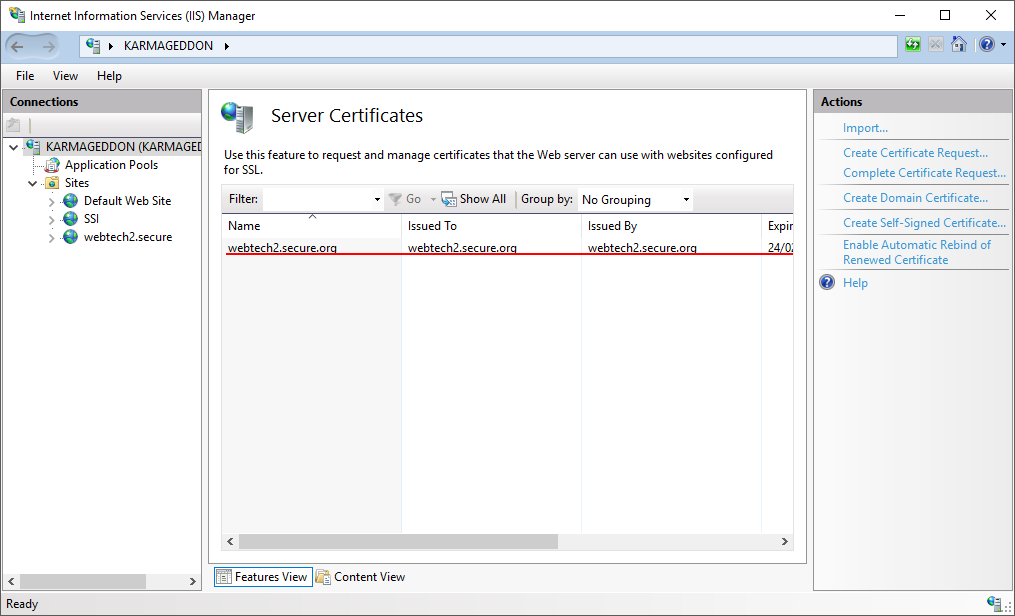
1. Click on **Complete Certificate Request** in the *Action* pane.



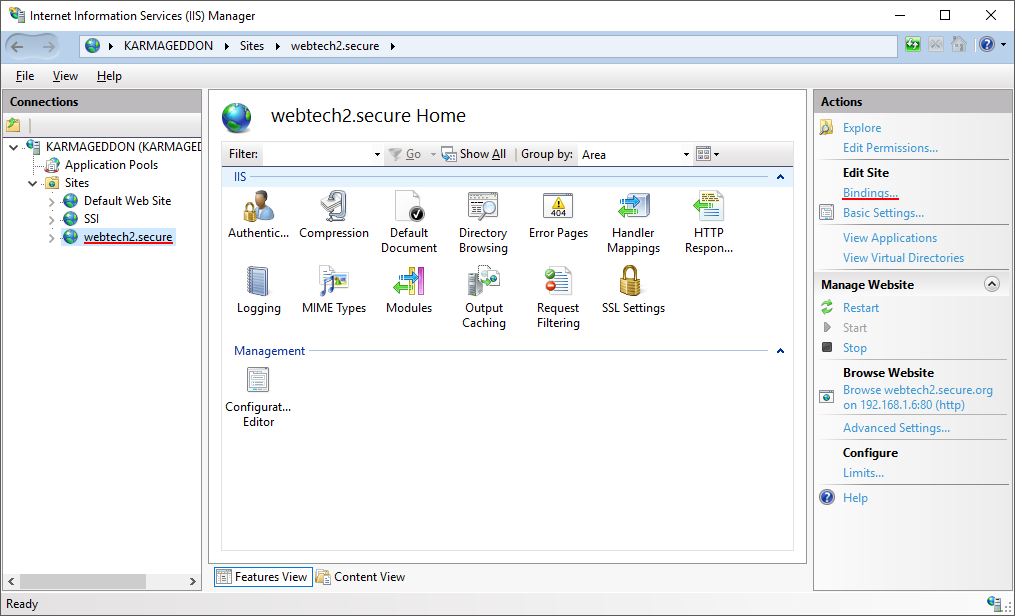
1. Fill out the appropriate data in the fields. Link to the exported certificate, and provide a friendly name it will have in the list of Server Certificates.

****

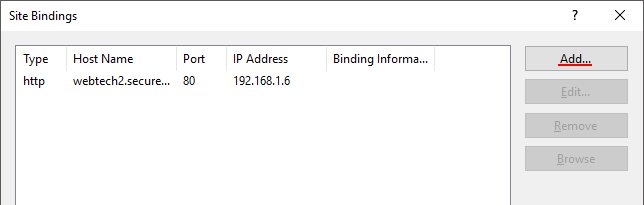
1. The certificate should now appear on the list.



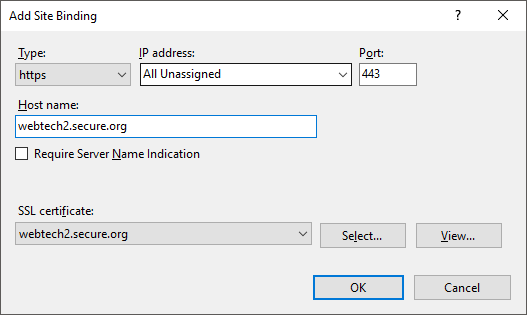
1. Next, to bind the certificate, go to the website and click **Bindings** in the *Action* pane.



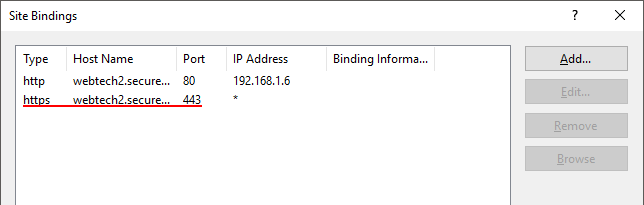
1. A new window should pop up, displaying all Site Bindings. Click **Add**.



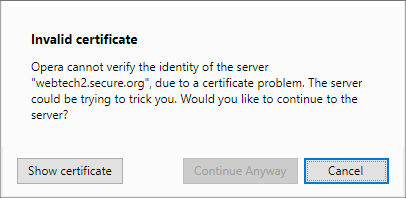
1. Fill out the appropriate data in the fields. Change the type to **https**, and select the **SSL certificate** you had just added.



1. After clicking **OK**, you should now see it in the list.

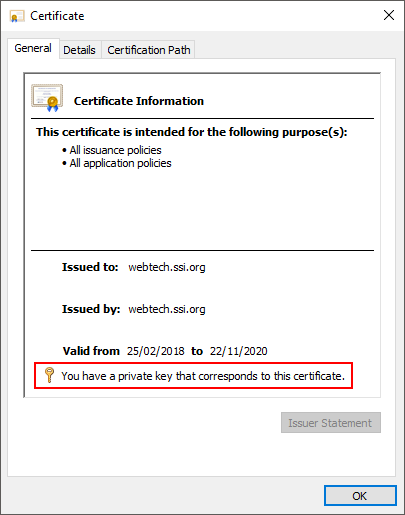


1. Try to access the website using **https://**. At first, a window about invalid certificates will pop-up. (Note: this only happens as we are using a self-signed certificate, and not an officially trusted one.) Feel free to ignore this, and continue anyway.



**E. Issues With Certificates**

There may be some issues with self-signed certificates not being added to IIS’s Server Certificates, and may require additional fiddling. In some cases, despite importing the certificate to *Windows Management Console*, it doesn’t come with the key automatically. A way to check if your certificate comes with its private key is to double-click on the certificate, and look for this section:



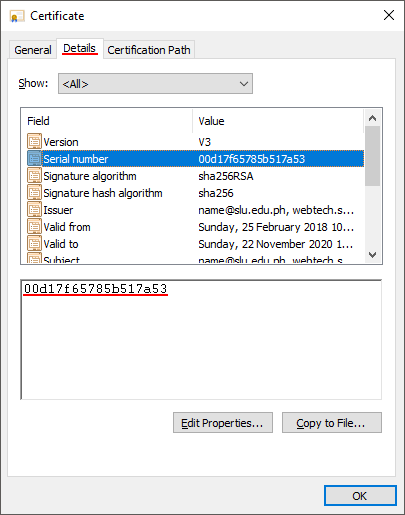
Note: if the specified section is blank, then it means that the certificate cannot locate its private key.

In that case, feel free to use any of the alternate methods below:

1. **Recover the Private Key of the SSL Certificate**

There are several ways to recover a certificate’s private key, but a simple way is using the certificate’s serial number and Window’s own *command prompt*.

1. The certificate’s serial number can be located by double-clicking the **.cer** file, and going to its **Details** tab. Click on **Serial Number**, and copy its value.

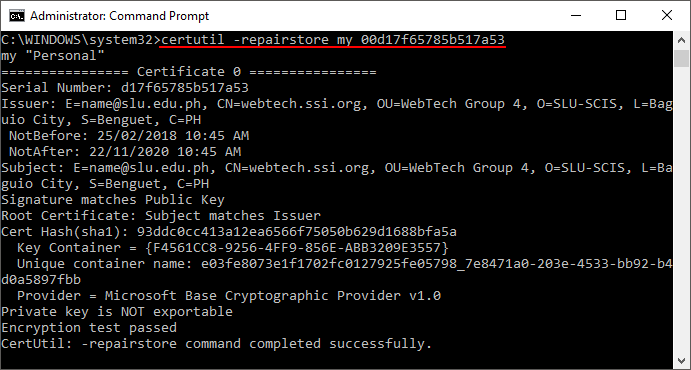


1. Open the *command prompt*, and run as administrator. One way to do this is by typing “CMD” into Windows Start, right-clicking **Command Prompt**, and **Run as Administrator**.
2. Use the following command:

|  |
| --- |
| certutil -repairstore my [serial number] |

Note: Replace **[serial number]** with your certificate’s actual number.

End result:



1. Follow the same steps starting from Step C.
2. **Merge the key and certificate**.

Instead of importing the **.cer** file in *Windows Management Console*, you can merge the certificate and the key to create a **.pfx** file using OpenSSL.

1. After creating the certificate and key on OpenSSL, execute the following command after:

|  |
| --- |
| pkcs12 -export -in certificate.cer -inkey privateKey.key -out certificateMerged.pfx |

Note: **certificate.cer** is the name of the certificate, **privateKey.key** is the name of the key, while **certificateMerged.pfx** is the name of the merged certificate and key. Feel free to change the names.

1. Open *Windows Management Console*, and perform Steps 1 to 3 of Part C. The only difference is that instead of importing your **.cer** file, import the **.pfx** file instead.



1. Follow the same steps afterward.

**References**

Microsoft. Retrieved from:

https://msdn.microsoft.com/en-us/library/ms525185(v=vs.90).aspx

Malachi, G. (2001). Retrieved from:

http://th.atguy.com/techCorner/Server-Side\_Includes.shtml

Shannon, R. (2012, August) Retrieved from:

http://www.yourhtmlsource.com/sitemanagement/includes.html

Parkansky, K. Retrieved from:

http://www.parkansky.com/tutorials/bdlogxbh.htm

*SSL Certificate*. Retrieved from:

https://www.instantssl.com/ssl-certificate.html

(2017, March). Retrieved from:

http://www.entrust.net/knowledge-base/technote.cfm?tn=7905

(2017, June). Retrieved from:

https://www.cloudinsidr.com/content/how-to-install-the-most-recent-version-of-openssl-on-windows-10-in-64-bit/

No-author sites:

https://specopssoft.com/support-docs/specops-password-reset/reference-material/installing-the-self-signed-ssl-certificate-into-the-trusted-root-certificate-authorities-store/

https://www.digicert.com/csr-creation-ssl-installation-iis-10.htm#ssl\_certificate\_install