# Verasys® Smart Building Hub Network and IT Guidance

## Technical Bulletin

LC-SBH100-x, LC-SBH200-x

**Code No. LIT-12012324**
**Issued July 2018**

Refer to the QuickLIT website for the most up-to-date version of this document.

# Verasys® Smart Building Hub Network and IT Guidance Technical Bulletin

## Introduction

This document contains important information about connecting a Verasys® Smart Building Hub (SBH) to your network. From an IT perspective, a system device, such as a SBH, is simply a node on the network. However, the SBH uses communication protocols, security methods, and other technologies that you must consider carefully.

**IMPORTANT:** Engage appropriate network security professionals to ensure that the certificates are handled. Typically, the IT organization must approve configurations that expose networks to the internet. Be sure to fully read and understand IT compliance documentation for your site. Use care when performing steps on system components because restarts may be required that conflict with compliance requirements. For example, upgrading firmware or installing new SSL certificates may require the computer to be offline for a period of time.

### *Connecting for remote access*

You can connect to the internet for remote access through the following options:

**Note:** Each option has a different level of security assurance.

- **Virtual private network (VPN) device - Highest level of security assurance:** This is the most secure method for remote access to Verasys. As this method is the most complex option for remote access, it is best practice to work with the customer's IT department when you implement a VPN solution. If a customer's IT department does not provide use of a VPN device or cannot offer you assistance, contact Verasys customer service at 1-866-663-6105 for VPN routing support.
- **Simple port forwarding - Lowest level of security assurance:** This is the least secure method of remote access to Verasys. After you connect the SBH to your local subnet, use simple port forwarding to configure the system to access it from any internet connection. The router needs to port forward Port 443, which is the most secure access port for a browser. You must use an IP Address that is a WAN IP address or a public address that routes to the connected router. When you type the address in the browser, start with HTTPS:// followed by the WAN IP address. The HTTPS:// prefix ensures the browser uses Port 443. If you forward Port 80 address, the WAN IP device switches to Port 443. Most IT personnel do not consider this a secure connection. For best security practices, use strong passwords and rotate them often. It is also best practice that the only port open is 443.

**Note:** You may require assistance from IT personnel with access to the subnets router information.

- **Simple port forwarding and installed certificate - Medium level of security assurance:** It is best practice to install a certificate after the system is configured for port forwarding.

## Concepts

This section describes the use of IT concepts with the SBH.

### *Chain of trust*

Multiple users can use a chain of trust to create and use software on a system where digital certificates are verified in a chain configuration, and their keys are not stored directly in hardware. When you attempt to use the SBH without the software being digitally signed, the UI issues warnings. The signing authority only signs boot programs that enforce security, such as only running programs that are themselves signed, or allowing only signed code to have access to certain features of the machine. This process may continue for several layers.

## *Self-signed certificates and certificates signed by a public certificate authority*

A self-signed certificate is a certificate that is signed by the same entity that it certifies. This term does not refer to the identity of the person or organization that actually performed the signing procedure. A self-signed certificate is a certificate signed with its own private key, that is, the entity signing the certificate is also the entity that created the certificate.

The SBH ships with a default Verasys self-signed certificate that provides secure communication. You can only install one certificate on a SBH at a time. When you install a new certificate on a SBH, you overwrite the existing certificate. You can run a SBH on your network with a self-signed certificate.

However, if you need to expose the SBH UI on a public network and have browsers that indicate a trusted site, you must get a signed certificate matching your domain name. You can acquire a valid signed certificate from your IT department or purchase it from a Public Certificate Authority (CA) using a certificate signing request (CSR). A certificate signed by a CA is used to establish a secure connection between your browser and the SBH.

## *Public and private keys*

Public and private keys are used to verify that the entity requesting access to a system is who or what it claims to be.

## *Man-in-the-middle attack*

This is a type of security breach where a person positions themselves between the user and the entity the user is trying to communicate with on the network. The person then has the ability to intercept and read traffic or send false information to the destination. To guard against this type of attack, use an Ethernet crossover cable to directly connect the SBH to your computer when transferring keys to the device. This configuration creates a network of two and makes a man-in-the-middle attack improbable.

## *IP addresses*

An IP address uniquely identifies devices on a TCP/IP network. You can use an IP address privately on a LAN, or publicly for use on the internet or a WAN.

## *DHCP*

Dynamic host configuration protocol (DHCP) means a network administrator can supervise and distribute IP addresses from a central point, and automatically send a new IP address when a device is plugged into a different location on the network. The network administrator can use DHCP to assign dial-up users an IP address automatically when they connect to the network. Some DHCP servers can support fixed addresses for devices that need a static IP address.

The SBH obtains its IP address and other network information using DHCP. Each device that connects to the Ethernet network needs a unique IP address. Without DHCP, enter the IP address manually for each device. Also enter a new IP address if the devices are moved to another subnet on the network. The SBH supports both dynamic and static IP address assignments.

## *DNS*

Domain name system (DNS) is the internet standard for naming host devices and mapping host domain names to IP addresses. A DNS server is a computer registered to join the Domain Name System. A domain name is a meaningful and
easy-to-remember handle for an internet address. A DNS server runs special-purpose networking software, features a public IP address, and contains a database of network names and addresses for other internet hosts to ensure that they are unique.

# Steps

## *Connecting to the SBH for the first time*

**IMPORTANT:** If you are going to use the Smart Building Hub on Ethernet, you must plug it into external power before you attach the field bus adapter.

The following instructions are based on the information in the *Quick Start Guide (Part No. 24-10737-00229)* that comes with each SBH. The default login credentials for each SBH are included in the Quick Start Guide that ships with each device.

1. Plug the Wi-Fi adapter that comes with the SBH into either of the USB ports.
2. Switch on the device. Once power is supplied to the SBH, the WiFi AP LED flashes to indicate that the device is initializing. When the **Fault** LED turns off, the WiFi AP LED flashes, and the **RUN** LED is on, connect the SBH using the built-in Wi-Fi access point.
3. Connect the SBH using the built-in Wi-Fi access point, when the **Fault** LED turns off, the Wi-Fi AP LED flashes, and the **RUN** LED is on.
4. In the Wi-Fi settings of your device or laptop, connect to the SBH Wi-Fi network using your default credentials. These credentials are included on a sticker in the *Quick Start Guide (Part No. 24-10737-00229)* that came with your device.
5. Open a web browser and navigate to www.smartbuildinghub.com to open the SBH browser interface.

   **Note:** The SBH ships with a private Smartbuildinghub.com SSL certificate installed to ensure secure communication with the Smartbuildinghub.com. However, this certificate does not indicate that it is trusted in a browser. If you wish to install your own certificate, refer to *Adding a private key and certificate to the SBH*. Use your default Admin login credentials that are also included on a sticker in the *Quick Start Guide (Part No. 24-10737-00229)* that came with your device.
6. Read and accept the SBH license agreement.
7. The first time you log in to the SBH, the **Change Password and Passphrase** web page appears. You must change the Admin password and Wi-Fi passphrase.

**IMPORTANT:** After you change the Wi-Fi passphrase or SSID, the webserver restarts and you must rejoin the SBH Wi-Fi network, using the new passphrase. On some mobile devices you must select and “forget” the original SBH Wi-Fi network before rejoining the network with the new passphrase.

**Note:** Replace the Wi-Fi Passphrase in the **New Wi-Fi Passphrase** field and click **Save**.

You can now use your SBH through the Wi-Fi connection. If you are connecting your SBH to an Ethernet network, continue to *Connecting the SBH to Ethernet*.

## *Connecting the SBH to Ethernet*

These instructions are for additional settings that are required when connecting the SBH to an Ethernet network. These settings occur after the steps in *Connecting to the SBH for the first time*.

**IMPORTANT:** When using the SBH on Ethernet, you must plug it into external power before you attach the field bus adapter.

1. In the SBH UI, navigate to **Settings** and click **Ethernet**.
2. In the Ethernet drop-down list, select **On** to activate the SBH Ethernet port.
3. Click **Save**.

   By default, the SBH is configured to dynamically receive an IP address from your network using DHCP. Take note of the address that automatically appears in the IP Address field.

4. Enter the IP address from Step 3 into your browser address bar to access the SBH over your Ethernet network.

You can use static or manual settings rather than automatic settings with your SBH. However, if you do so, you must contact your IT department for all necessary manual settings to ensure that your SBH works on your company's network.

## Using your SBH with a static IP address

Complete the following steps to configure your own static IP address parameters:

1. Navigate to **Settings** and select **Ethernet.**
2. Set **Auto DHCP Configure** to **OFF.**
3. Obtain the necessary network settings from your IT department.

## Using your SBH with a DNS

If you have a Dynamic Name Server (DNS) on your network, you can access the SBH with a unique name instead of using an IP address.

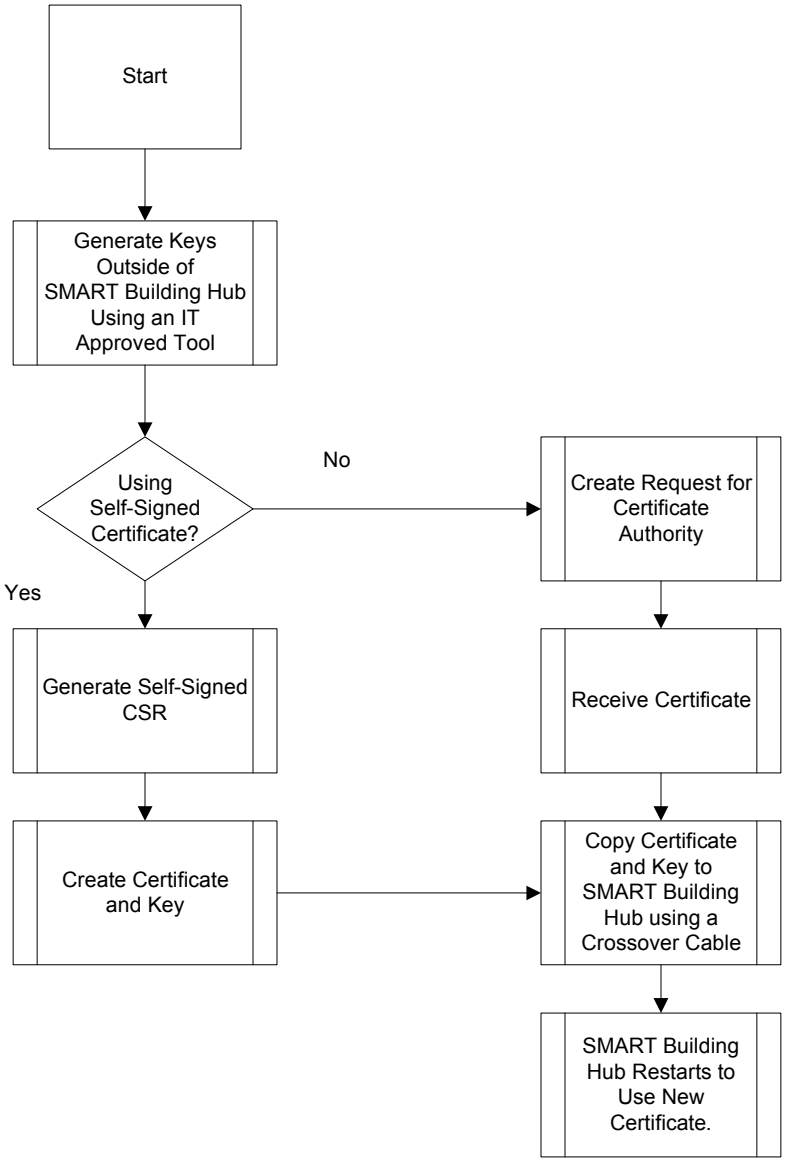
To activate a DNS, complete the following steps:

1. Navigate to the **Settings** tab and select **Ethernet**.
2. Set the **Auto DNS Configure** setting to **ON**.

## *Certificate workflow*

The following flowchart gives an overview of how to create and install certificates on the SBH. This process covers how to generate self-signed certificates and keys. It also covers the processes of creating a request for a certificate signed by a public certificate authority that you can install on the device. The instructions for how to install and uninstall these certificates varies depending on the browser type.

**Figure 1: Certificate workflow**



## *Generating a private key*

Before you generate a new private key, you may have to first create an encrypted database. The password for this encrypted database is used to encrypt the private key, which you need to protect. Use a key generation tool that your IT department approves. Complete the following steps to generate a new private key:

1. Open your key generating software and click **New Key**.
2. Name the new key.
3. From the drop-down lists, select a Keytype of **RSA**, and a Keysize of **2048 bit**.
4. Click **Create** and the new key appears in your list of **Private Keys**.
5. Select the private key you created and select **Export**.

**Note:** Export the private key in PEM format.

6. Click **OK** and save the file. This is the file you use when *Adding a private key and certificate to the SBH*.

## *Implementing SSL for the SBH*

The options for SSL certificates include the following:

- **Third-Party** – Coordinate with the local IT department before installing the SBH. Follow the instructions included in the *Installing a security certificate on a client that is connected to the SBH* section. If you need to create a request for a certificate signed by a public CA, see the *Creating a certificate request (CSR)*.
- **Self-Signed** – Follow the installation process that allows you to generate a self-signed certificate in the *Creating a self-signed certificate* section.

**Note:** It is best practice not to implement a self-signed SSL certificate for networks exposed directly to the internet because they do not have the protection of a firewall or VPN.

You must have Port 80 (TCP) and Port 443 (SSL) open on the computer that is connected to the SBH.

## *Creating a self-signed certificate*

The following steps demonstrate how to create a self-signed certificate. Use a certificate-generating application that is approved by your IT department. This procedure creates a file in the appropriate format for submitting the properties of your SSL certificate to the certificate authority.

1. Open your certificate creating-application and select the **Certificates** tab.
2. Click **New Certificate**.
3. Accept the defaults, unless they conflict with your IT policies.
4. Select the **Subject** tab.
5. In the **Distinguished name** properties window, complete the fields with the information shown in the following table:

| Field | Description |
|---|---|
| **Internal name** | This name is only used internally and does not appear in the certificate. |
| **organizationName** | The name of your organization |
| **countryName** | The country in which your organization is located |
| **organizationalUnitName** | The name of your department within the organization |
| **stateOrProvinceName** | The state in which your organization is located |
| **commonName** | The domain name without https://. The domain name is the site used to browse to the SBH UI. |
| **localityName** | The city in which your organization is located |

| Field | Description |
|---|---|
| **emailAddress** | This is usually the e-mail address of the administrator of your organization. |
| **Private key** | Select the private key you generated in the *Generating a private key* section. If you have not created a private key or need to generate a new one, click **Generate a new key** and follow the steps in *Generating a private key* . |

6. Select the **Extensions** tab.
7. In the **Validity** and **Time** range sections, define time limits and valid ranges for your certificate.
8. Click **OK**. The new certificate is now in your list of certificates with the internal name you assigned.
9. Select the certificate and click **Export**.
10. Choose an export format of PEM and click **OK** to save the file. This is the file you use when *Adding a private key and certificate to the SBH*.

## *Uninstalling a certificate on a client that has connected to the SBH*

If you are removing or replacing a SBH, and want to uninstall the certificate from your computer, follow the procedure that applies to the platform you are using.

**Note:** You do not need to uninstall the certificate from the SBH because new certificates overwrite existing certificates.

### Uninstalling the security certificate on iOS® platforms

To remove the SBH security certificate on an iOS platform, complete the following steps:

1. Navigate to the **Settings** tab and select **General.**
2. Tap **Profiles.**
3. Select the Smartbuildinghub.com certificate.
4. Tap **Remove** twice.

### Uninstalling the security certificate in windows® internet explorer® web browser

1. Open the internet explorer web browser.
2. Navigate to the **Tools** menu and click **Internet options**.
3. In the **Internet Options** dialog box, click the **Content** tab.
4. Click **Certificates**.
5. In the **Certificates** dialog box, click the **Trusted Root Certification Authorities** tab.
6. Select the **Smart Building Hub authority**.
7. Click **Remove**.
8. In the **Certificates warning** dialog box, click **Yes**.
9. In the **Root Certificate Store warning** dialog box, click **Yes**.
10. In the **Certificates** dialog box, click **Close.**
11. Click **OK**.

### Uninstalling a certificate in Google Chrome

1. Open the Google Chrome web browser.
2. In the top right hand corner, click the **Customize and control Google Chrome** button.

3. Select **Settings**.
4. Scroll down to the bottom of the panel and click **Advanced**.
5. Navigate to **Manage certificates** and click it.
6. Select the **Trusted Root Certification Authorities** tab.
7. Select the Smart Building Hub authority, and then click **Remove**. A certificates warning appears.
8. Click **Yes**. The certificate is removed immediately.

## *Adding a private key and certificate to the SBH*

Complete the following steps to add the private key and certificate to your SBH.

1. Connect to the SBH through an Ethernet crossover cable. The Ethernet crossover cable prevents the possibility of a *Man-in-the-middle attack*.

   **Notes:**

   - To Log in to your SBH UI, open your web browser and enter www.smartbuildinghub.com. You must log in as an administrator to perform these tasks.
   - If your computer does not connect to the SBH UI, disconnect any other network connections, LAN or wireless, and try again. If your computer is connected to another network, it might not redirect to the SBH UI when you enter www.smartbuildinghub.com.
2. Click **Settings** and select **SSL**.
3. Navigate to the location of the private key file (***.pem) that you created for your site, and right-click the private key file.
4. Select **Open with,** and click **Notepad**.
5. Highlight the text and copy the entire file.
6. Paste this file as a plain text file in the **Private Key box** of your SBH SSL settings **Private Key box.**
7. Navigate to the location of the security certificate (***.crt) that you created for your site and, right-click the file.
8. Select **Open with,** and click **Notepad**.
9. Highlight the text and copy the entire file.
10. Paste this file as a plain text file in the **New Certificate box** of your SBH SSL settings **Private Key box**.
11. Click **Save**. A reset warning screen appears.
12. To apply the new certificate and private key, restart the SBH web server. Click **OK**. The fault light flashes for five seconds, then turns off. The rest of the lights continue to function normally. The SBH goes offline while restarting and displays the device resetting screen.

**Note:** When a SSL key or certificate is corrupted, the SSL page detects it and alerts you to the corrupted key or certificate. However, if the corruption is minor, for example an extra space copied while installing the certificate or a missed character, the UI does not detect the problem and allows the corrupted key or certificate to save. The server detects the error and returns the **Error Saving SSL Settings** message. This prevents the use of the bad key or certificate, but it does not inform you what the source of the problem is. In this case, you need to recopy and reinstall the SSL Key or Certificate.

13. When the connection reestablishes, log in to the SBH and use normally.

## *Installing a security certificate on a client that is connected to the SBH*

Until you add the security certificate for the SBH as a trusted certificate, you receive a security alert every time you visit the www.smartbuildinghub.com website. How you install the certificate differs based on the web browser and device platform.

### Installing the security certificate in internet explorer

1. Navigate to www.smartbuildinghub.com/downloadtlsprofile
2. Download the rootCA.pem file.
3. On the **Tools** menu, click **Internet options**.
4. In the **Internet Options** dialog box, select the **Content** tab.
5. Click **Certificates.**
6. Select the **Trusted Root Certification Authorities** tab.
7. Click **Import**.
8. In the **Certificate Import Wizard** dialog box, click **Next**.
9. Browse to the rootCA.pem security certificate file and select it.
10. Click **Open**, and then click **Next**.

    **Note:** Install the **rootCA.pem** file, not the www.smartbuildinghub.com file that the browser prompts you to install. The rootCA.pem file certifies your device for any SBH you use. If you install the www.smartbuildinghub.com file that the browser prompts you to install instead, you need to add a new certificate for each new SBH device that you use.
11. On the **Certificate Store** page of the Wizard, select **Place all certificates in the following store**.
12. Verify that the certificate store listed is **Trusted Root Certification Authorities**, and then click **Next**.
13. Click **Finish**.
14. In the **Security Warning** dialog box, click **Yes**.
15. A success message appears, click **OK.**

### Installing the security certificate in Google Chrome

1. Navigate to www.smartbuildinghub.com/downloadtlsprofile, and then download the rootCA.pem file.
2. On the **Customize and control Google Chrome** menu, click **Settings**.
3. At the bottom of the settings page, click **Advanced**.
4. Click **Manage certificates**.
5. In the **Certificates** dialog box, click the **Trusted Root Certification Authorities** tab.
6. Click **Import**.
7. In the **Certificate Import Wizard** dialog box, click **Next**.
8. Browse to the rootCA.pem security certificate file and select it.
9. Click **Open**
10. Click **Next**.

    **Note:** Install the rootCA.pem file and not the www.smartbuildinghub.com file that the browser prompts you to install. The rootCA.pem file certifies your device for any SBH you use. If you install the www.smartbuildinghub.com file that the browser prompts you to install instead, you need to add a new certificate for each new SBH device that you use.
11. On the **Certificate Store** page of the Wizard, select **Place all certificates in the following store**.

12. Verify that the certificate store listed is **Trusted Root Certification Authorities.**
13. Click **Next**.
14. Click **Finish**.
15. In the **Security Warning** dialog box, click **Yes**.
16. Click **OK** on the success message to close the wizard.

## *Importing a certificate signed by a public CA*

If you have a certificate from a public CA, import it using the following procedure:

1. In the **Certificates** dialog box, click the **Trusted Root Certification Authorities** tab.
2. Click **Import**.
3. In the **Certificate Import Wizard** dialog box, click **Next**.
4. Browse to the rootCA.pem security certificate file and select it.
5. Click **Open.**
6. Click **Next**.

   **Note:** Install the rootCA.pem file and not the www.smartbuildinghub.com file that the browser prompts you to install. The rootCA.pem file certifies your device for any SBH you use. If you install the www.smartbuildinghub.com file that the browser prompts you to install instead, you need to add a new certificate for each new SBH device that you use.
7. On the **Certificate Store** page of the Wizard, select **Place all certificates in the following store**.
8. Verify that the certificate store listed is **Trusted Root Certification Authorities**.
9. Click **Next**.
10. The **Completing the Certificate Import Wizard** appears, Click **Finish**.
11. In the **Security Warning** dialog box, click **Yes**.
12. Click **OK** to close the Wizard.

## *Creating a certificate request*

This section describes how to create a certificate signing request and how to purchase an SSL certificate from a Public Certificate Authority. Coordinate with your IT department and only use an approved Public Certificate Authority for your location.

- The steps to purchase a domain name and a security certificate vary according to the registrar. Use the instructions in this document as an example. You may choose a different registrar to purchase a domain name and security certificate.
- The domain name and security certificate costs are not included as part of the purchase cost of the SBH.
- Domain names and third-party security certificates expire. Best practice is to register domain names and third-party certificates for the longest duration available, typically three years. Plan to renew domain names and security certificates before they expire.

### Creating a certificate request (CSR)

You must use a certificate request generating application that your IT department approves. The procedure creates a file in the appropriate format required for submitting the properties of your SSL certificate to the certificate authority.

Your IT department must also approve the Public Certificate Authority to which you submit your request.

1. Open your certificate request creating application, select the **Certificate signing request** tab.

2. Click **New Request**.
3. In the **Create Certificate signing request** dialogue box, navigate to **Signing request.**
4. Enter **unstructuredName** and **challengePassword**. The certificate signing authority uses the unstructured name and you can set it to your organization name.
5. Select the **Subject** tab.
6. In the **Distinguished name** properties window, complete the fields with the information shown in the following table:

| Field | Description |
|---|---|
| **Internal name** | This name is only used internally and does not appear in the certificate. |
| **organizationName** | The name of your organization |
| **countryName** | The country in which your organization is located |
| **organizationalUnitName** | The name of your department within the organization |
| **stateOrProvinceName** | The state in which your organization is located |
| **commonName** | The domain name without https://. The domain name is the site used to browse to the Smart Building Hub UI. |
| **localityName** | The city in which your organization is located |
| **emailAddress** | This is usually the e-mail address of the administrator of your organization. |
| **Private key** | Select the private key you generated in the *Generating a private key* section. If you have not created a private key or need to generate a new one, click **Generate a new key** and follow the steps in *Generating a private key*. |

7. Select the **Extensions** tab. The new certificate signing request is now in your list of certificates with the internal name you assigned.
8. Select the certificate and click **Export**.
9. Click the **Browse** button and choose a location for the new CSR file
10. Click **OK**. This file is used to purchase a certificate request from a Public Certificate Authority.

## *Purchasing an SSL certificate from a public authority*

You can obtain an SSL certificate from any public certificate authority. The SBH requires a basic Class 1 SSL certificate, also called a domain verified certificate. This section includes instructions using the following vendor: https://www.namecheap.com/

This vendor is a popular reseller of SSL certificates from several of the largest certificate authorities, including GeoTrust, Inc. The RapidSSL product from GeoTrust, Inc. is used as an example in this document. You can use any public certificate authority to purchase an SSL certificate. The steps to purchase a security certificate vary according to the registrar.

1. In a web browser, browse to https://www.namecheap.com/.
2. Navigate to the SSL certificate products.
3. Choose the RapidSSL option used in these instructions and select the longest duration available for the certificate.
4. Click **Add to Cart**.
5. The **Order Confirmation** page appears. Click **Confirm Order**.
6. You are prompted to create an account with https://www.namecheap.com/. If you already have an account, log in. If you do not have an account, enter your account information and click **Create Account** and **Continue**.
7. On the **Order Review** page, review your order and select your payment option.
8. Complete your purchase.
9. To view your purchased certificate, click **Manage My Account.**
10. On your **Manage My Account** page, a message appears alerting you to activate your SSL certificate. Click the **SSL Certificates** page.
11. In the **Status** column, click **Activate Now**.
12. From the **Select** web server drop-down list on the **Digital Certificate Order Form** page, select **Apache + ApacheSSL.**
13. On your computer, navigate to the location where you stored the certificate request in *Creating a certificate request (CSR)*.
14. Select all of the text from the.txt file and paste the text into the **Enter CSR** field on the Digital Certificate Order Form page.
15. Click **Next**.
16. Select the approver email address to verify ownership of the domain name. You must have access to the mailbox of the email address selected.
17. An email containing a validation code is sent to this email address. Click **Next**.
18. A confirmation page appears. Confirm the administrator contact information is correct.
19. Click **Submit Order.**
20. The **Digital Certificate Order Process Summary** appears. Wait for the email to approve the certificate. See *Importing a certificate signed by a public CA* to complete the process.

**Building Technologies & Solutions**
507 E. Michigan Street, Milwaukee, WI 53202