# Pinewood Derby – Creating SSL Certificates

# Introduction

# Generating New CSR Request

1. Launch Putty and SSH to the server.

**NOTE:** You may already have this open.

A screen shot of a computer

Description automatically generated

1. Type the following: (replace pack442.coughlinfam.com if this ever changes)

**openssl req -new -newkey rsa:2048 -nodes -keyout pack442.coughlinfam.com.key -out pack442.coughlinfam.com.csr** and press **Enter**.



1. When prompted provide the following information pressing **Enter** for each entry.:
   1. Country Name: **US**
   2. State or Province Name: **Missouri**
   3. Locality Name: **Union**
   4. Organization Name: **Cub Scouts**
   5. Organizational Unit Name: **Pack 442**
   6. Common Name: **pack442.coughlinfam.com**
   7. Email Address: (Email of the person putting the request).
   8. A Challenge password: **doyourbest**.
   9. An optional company name: (leave blank)
2. Send pack442.coughlinfam.com.csr to be signed by a certificate authority. (Digicert, etc…)
3. When having it signed, make sure it includes all intermediate and root in the .pem file.
4. To retrieve the file from the server, go to [Get CSR from DerbyNet Server](#_Get_CSR_from).

# Applying New Certificate

1. Type **WinSCP** **>** Click **WinSCP**.

A screenshot of a computer

Description automatically generated

1. Type the ip address of the virtual machine.
2. Type the following:

Username: pack442

Password: pack442

1. Click **Login**.

A screenshot of a computer

Description automatically generated

1. Click **Yes / Accept**.

A screenshot of a computer error

Description automatically generated

1. Drag the file over to /home/pack442.

A screenshot of a computer

Description automatically generated

1. Launch Putty and SSH to the server.

**NOTE:** You may already have this open.

A screen shot of a computer

Description automatically generated

1. Type **sudo cp /etc/ssl/certs/pack442-coughlinfam-com.pem /etc/ssl/certs/pack442-coughlinfam-com.pem.bak** and press **Enter**.
2. Type **sudo cp pack442\_coughlinfam\_com.pem /etc/ssl/certs/pack442-coughlinfam-com.pem** and press **Enter**.

**NOTE:** You may be prompted for the pack442 password.

A black and white screen with a white text

Description automatically generated with medium confidence

1. Type **sudo cp /etc/ssl/private/pack442.coughlinfam.com.key /etc/ssl/private/pack442.coughlinfam.com.key.bak** and press **Enter.**
2. Type **sudo cp pack442.coughlinfam.com.key /etc/ssl/private/pack442.coughlinfam.com.key** and press **Enter**.

A computer screen with a black background

Description automatically generated

1. Type **sudo su** and press **Enter**.
2. Type **cd /etc/ssl/private/** and press **Enter**.
3. Type **chown root:ssl-cert pack442.coughlinfam.com.key** and press **Enter**.
4. Type **chmod 640 pack442.coughlinfam.com.key** and press **Enter**.

A black and white screen with white text

Description automatically generated

(Only required if changed name of .key and .pem file – Skip to Step 22)

1. Type: **cd /etc/nginx/sites-available** and press **Enter**.
2. Type: **vi default** and press **Enter**.

A black and white text

Description automatically generated

1. Press INS button on keyboard.
2. Change these lines in red.

*# SSL configuration*

*#include snippets/snakeoil.conf;*

*ssl\_certificate /etc/ssl/certs/pack442-coughlinfam-com.pem;*

*ssl\_certificate\_key /etc/ssl/private/pack442.coughlinfam.com.key;*

A screenshot of a computer program

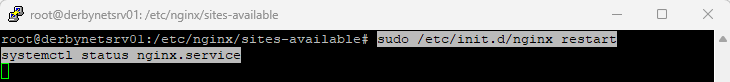
Description automatically generated

1. Press **ESC**
2. Type**:wq!** (including “:”) and press Enter.

A screenshot of a computer program

Description automatically generated

1. Type: **exit** and press **Enter**.
2. Type: **sudo /etc/init.d/nginx restart** and press **Enter**.
3. Type: **systemctl status nginx.service** and press **Enter**.



A screenshot of a computer screen

Description automatically generated

1. Press **q**.

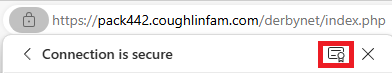
# Verify Certificate is Applied

1. Navigate to <https://pack442.coughlinfam.com/derbynet>.
2. Click **Connection is secure**.

A screenshot of a computer

Description automatically generated

1. Click on the **certificate icon**.



1. Review the new certificate to make sure the date is correct.

A screenshot of a certificate

Description automatically generated

# Replace Existing Certificate Information

1. Replace the existing. pem and .key files in the github repository. [Pack442PineWoodDerby-main-main/Configuration/etc/ssl at main · majora15/Pack442PineWoodDerby-main-main (github.com)](https://github.com/majora15/Pack442PineWoodDerby-main-main/tree/main/Configuration/etc/ssl)
2. Ask for assistance with this step.

# Get CSR from DerbyNet Server

1. Type **WinSCP** **>** Click **WinSCP**.

A screenshot of a computer

Description automatically generated

1. Type the ip address of the virtual machine.
2. Type the following:

Username: pack442

Password: pack442

1. Click **Login**.

A screenshot of a computer

Description automatically generated

1. Click **Yes / Accept**.

A screenshot of a computer error

Description automatically generated

1. Drag the pack442.coughlinfam.com.csr to your download folder.

