Understanding Web Server Certificates

Please allocate a generous time for this exercise.

Learning Objectives: Upon completion of this activity, students will be able to

- Describe the process to obtain a web server certificate
- Install a web server certificate to enable HTTPS

Summary: In this exercise, you will use your Windows 7 and send a certificate request to a Windows Server 2008. The server is a local certification authority.

Delivery: Submit a lab report answering all review questions.

A.

B. Create a Certificate Request (Windows 7)

In this activity, your Windows 7 computer will be your webserver. First, the web server needs to create a certificate request. In this process, the web server also creates the public/private key pair, and the public key will be a part of that certificate request. Note that the matching private key will be locally stored in the web server.

1) In the **Control Panel** window, double-click **Administrative Tools**.
2) Double-click **Internet Services Manager**.
3) In the tree pane, expand **PC(local computer)**.
4) Under the IIS Category, double-click on **Server Certificates**.
5) On the Actions Snap-on, select **Create Certificate Request…**

A Request Certificate window will appear. Fill in the following fields.

Common name: Penn State Berks Web Server

Organization: PSU Berks

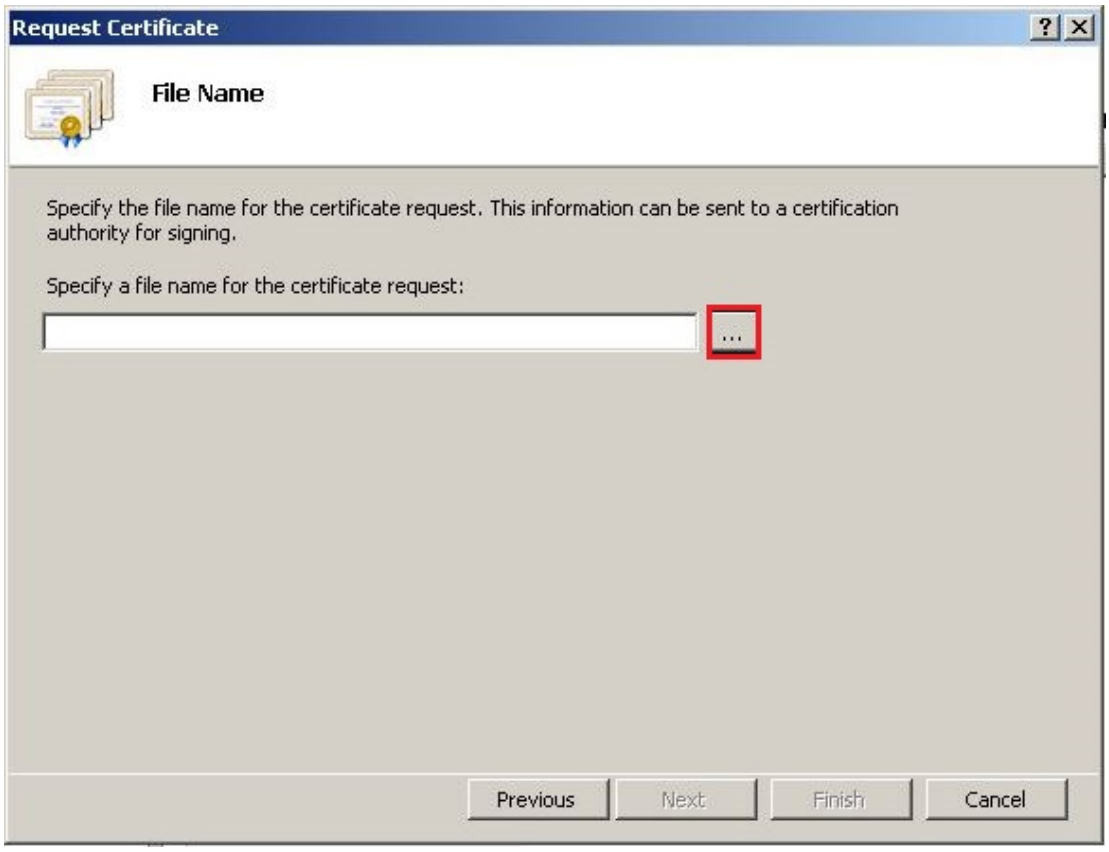
Organizational unit: IST/SRA

City/locality: USA

State/province: PA

Once the fields are filled, click **Next.**

6) Select a cryptographic service provider and bit length.
    a) Provider: Microsoft RSA SChannel Cryptographic Provider
    b) Bit Length: 1024, then click **Next.**
7) The wizard will prompt for a File Name, click on the **…** browse button.



8) Navigate to the C:\ directory and name the file **certreq.txt**.

The file certreq.txt is the certificate request file that is going to be used to request a certificate from the Certification Authority. Find the file in C:\ and open this file in Notepad.

.

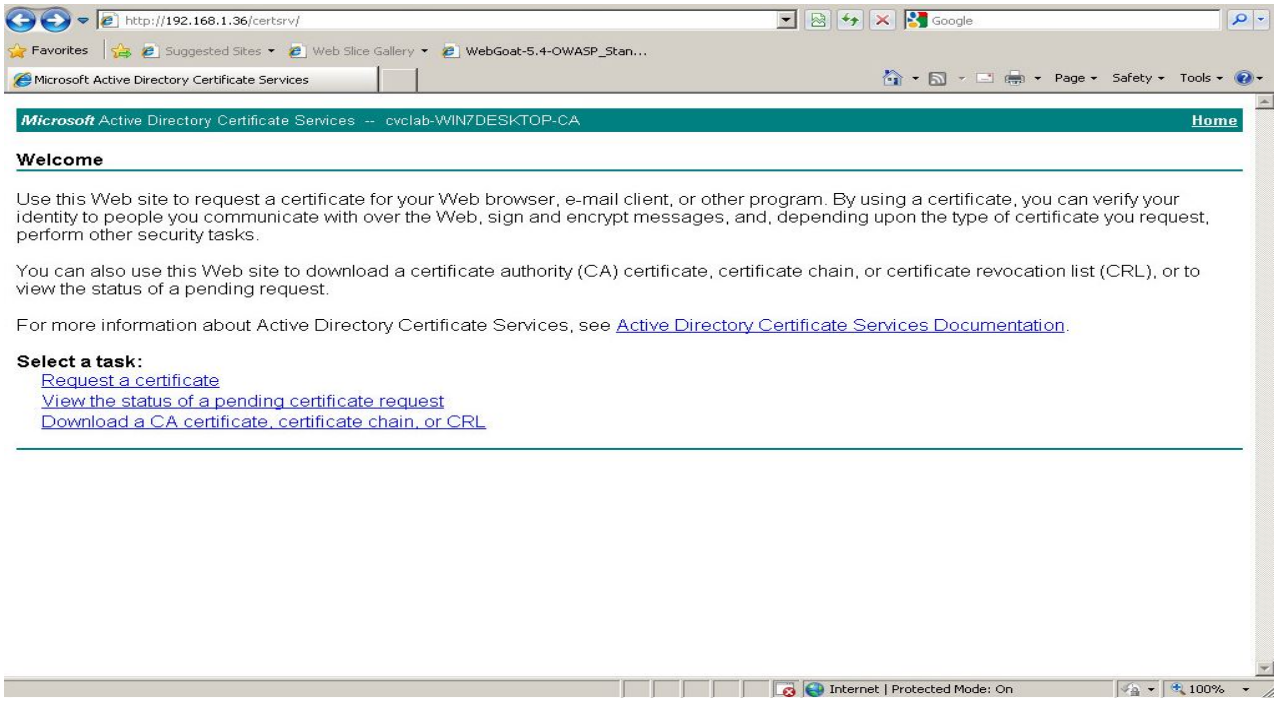
Review Questions:

- Can you understand the content of the file certreq.txt? Please include a screenshot of this certification request file.
- What type of information could be encoded in the certreq.txt? Answer this question considering the content of a digital certificate. In addition, you may want to do a web search for this.

C. Submit a Certificate Request. (192.168.1.250)

You will be submitting the certificate request from the Web server to the Certification Authority. Currently, your computer is on the same network with a Windows 2008 Server, which includes the Certification Authority service. The IP address of this server is 192.168.1.250. Ping this server before starting the following steps. If you cannot get that address to work, inform your instructor ASAP.

1) Double-click on the **Internet Explorer** icon on the desktop.
2) In the **Address** bar, type http://192.168.1.250/certsrv/ and press **ENTER**. (be patient the following steps may take a minute or so)
3) You will be prompted with a login screen. Use the credentials for the Windows Server 2008 machine by clicking **Other**.
    a) **User:** Administrator
    b) **Password:** Cvclab14@
4) On the **Microsoft Certificate Services Welcome** page, click **Request a Certificate**.



5) (BE CAREFUL in this step) click **Advanced certificate request.**

6) On the **Advance Certificate Request** page, select **Submit a certificate request using a base64 encoded CMC or PKCS #10 file**...and.

7) You will copy all content of the certreq.txt file to the **Save Request** textbox as shown in the picture below.

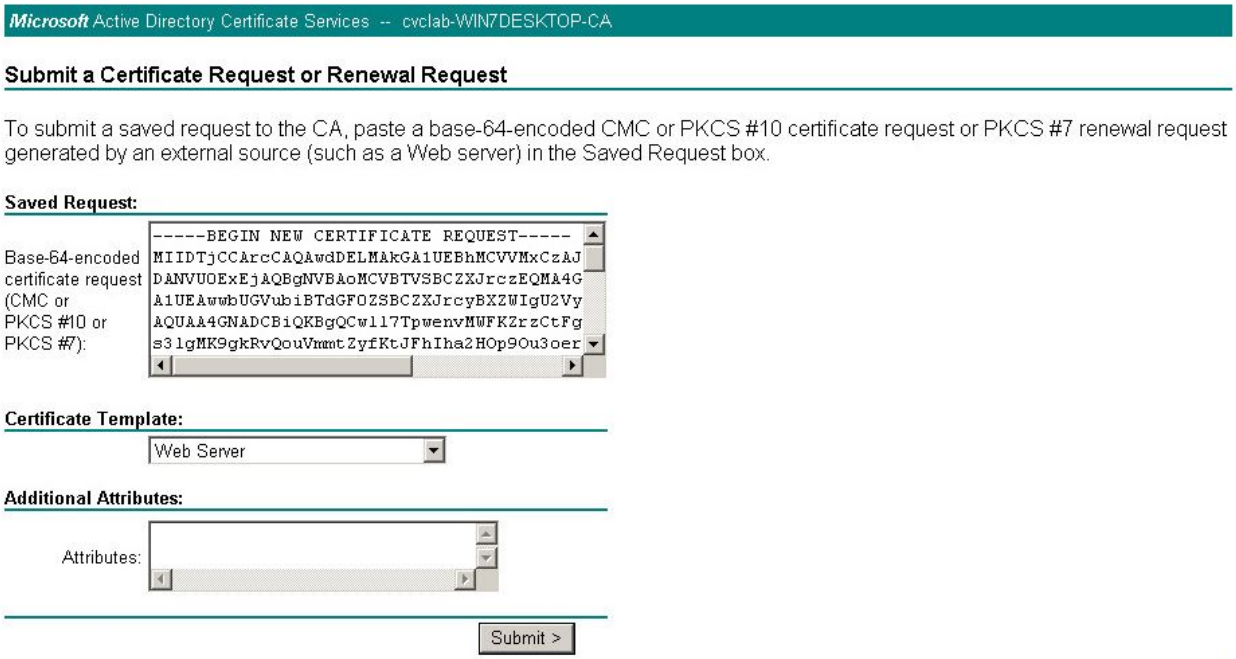
8) Navigate to C:\certreq.txt and click Open.

9) In **Notepad** click Edit, **Select All**.

10) Click **Edit** and **Copy**. Close Notepad.

11) Go back to to the Internet Explorer, on the **Submit a Saved Request** page, in the **Saved Request** text box, right-click and select Paste.

12) For Certificate Template: Select Web Server



13) Click **Submit**.

C. Configure the Web Site to Use the SSL with the Certificate

The Certificate was issued from the web server.

1) Click on **Download Certificate Chain** and **save** it to the Desktop.

Name the file:**certnew.p7b**

It may take a few moments to open the file. Internet Explorer Security may show a warning for the certificate, click **Allow**.

2) A certificate window will appear saying who the certificate is issued to as well as who issued it. Click **Install Certificate**.

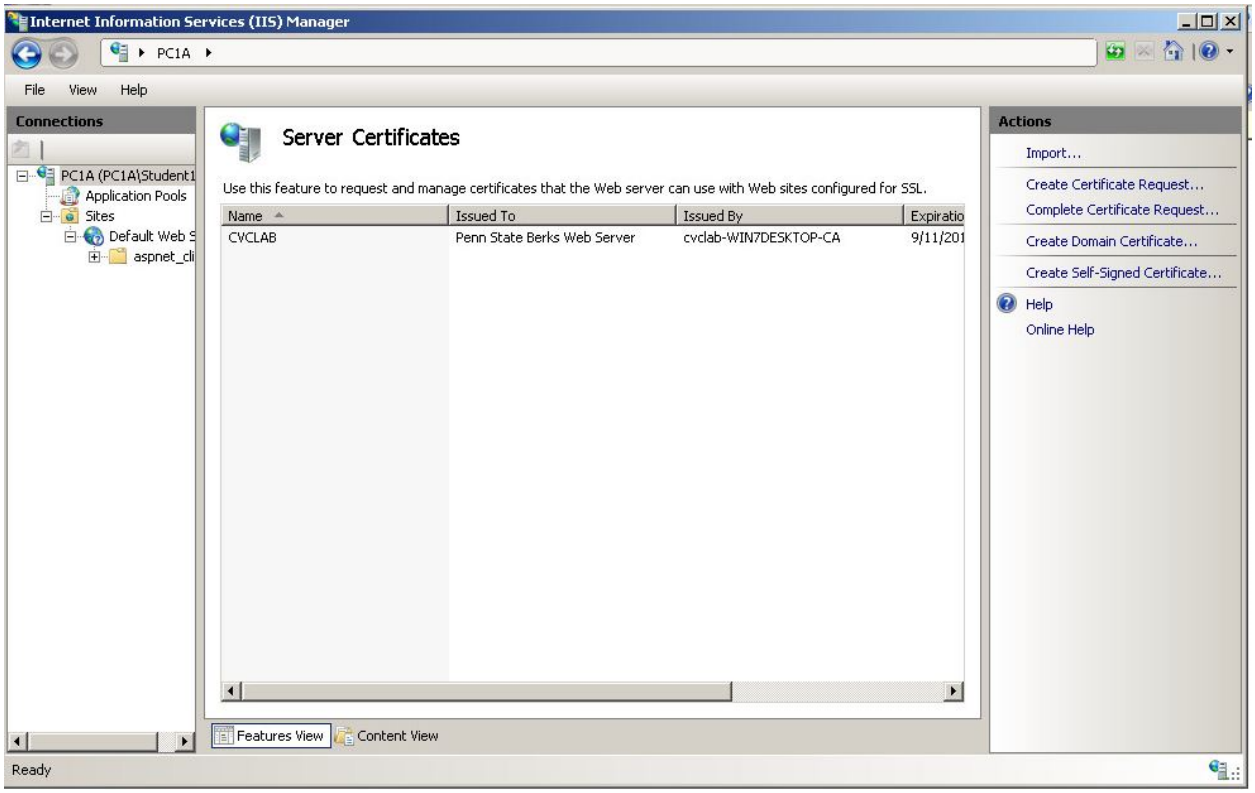
3) A certificate import wizard will then pop up. On the Process a pending request screen, in the **Path and File name** box, browse to the Desktop and select certnew.cer and click **Next**. Finally, Click **Next** then **Finish**.

4) Now open the **Internet Information Services Manager (IIS)** as you have done in the beginning of this activity and click on PC1A.

5) Double-click on **Server Certificates.**

6) On the Actions Snap-on, click **Complete Certificate Request…**.

7) Browse for **certnew.p7b** on the Desktop and **Open it**. For the Friendly Name, enter CVCLAB.

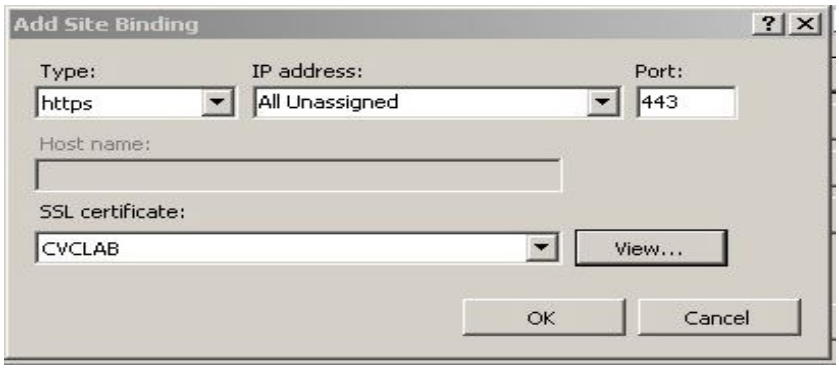


Now that the certification has been imported and completed. We must now enable the SSL protocol.

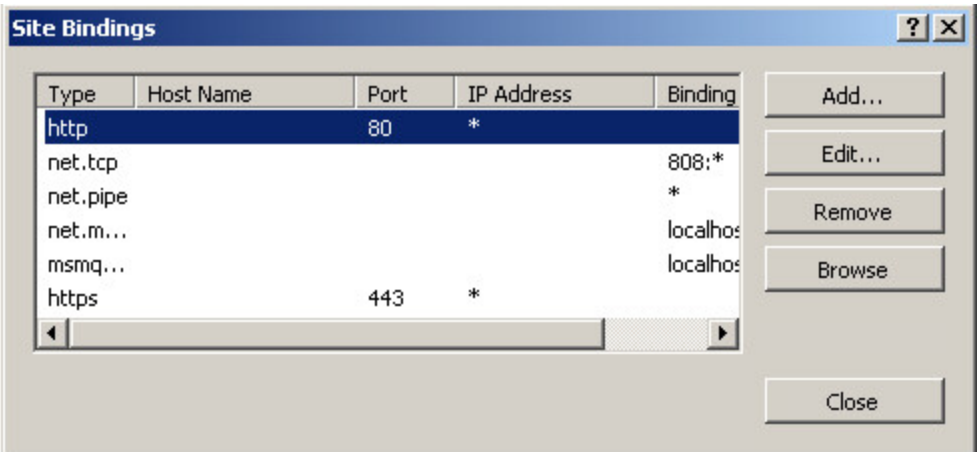
8) Under the **IIS manager**, within the Connections snap-on **Expand** Sites and right-click on Default Web Sites. Select **Edit Bindings…**.

9) A window will appear called Site Bindings, click **Add.**

10) Change the type of the protocol to **https**. Select the Certificate from the SSL certificate drop down menu. Then click **Ok**.



11) Under the **IIS manager**, within the Connections snap-on **Expand** Sites and right-click on Default Web Sites. Select **Edit Bindings…**. Select http (port 80) and Click Remove to remove the HTTP service. Only HTTPS service should work as a result.



D. Testing (Results to be submitted)

1) Start Internet Explorer.

2) In the address bar, type http://localhost and press ENTER. What is the error message? Include a screen capture.

3) Type https://localhost. What happens? Why do you get a certificate warning although you installed the certificate yourself? **Select Trust** the connection and confirm security exception. Include a screen capture.

Review Questions:

- Open the certificate that you just downloaded. You will get an Unknown publisher warning. What is the reason that you are getting this warning?

- Why do you think the issuer of this certificate cannot be verified?

- Find and list the information about the publisher of the certificate.

- What is the first three octet of your public key (in hexadecimal numbers). Include a

screenshot of the certificate.

- Can you use the certificate that you created in the Internet to provide **data confidentiality** and **integrity** between your web server and other client computer? Why or Why not?

- Can you use the certificate that you created in the Internet to **authenticate** your web server to client computer? Why or Why not? What do you need to do so?