Managing The Lifecycle of a Certificate

(CompTIA Security + SY – 601)

Objectives:

- To explore the properties of digital certificates
- To use Windows in requesting, issuing and revoking certificates
- To Implement Public Key Infrastructure (PKI)

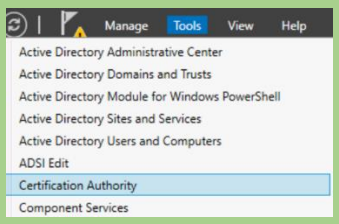
Resources:

- Windows Virtual Machine
- Kali Virtual Machine
- 515support-CA
- Internet Information Services (IIS) Manager

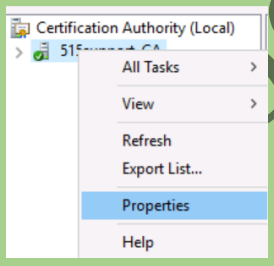
Instructions:

Browse Certificate Server Properties

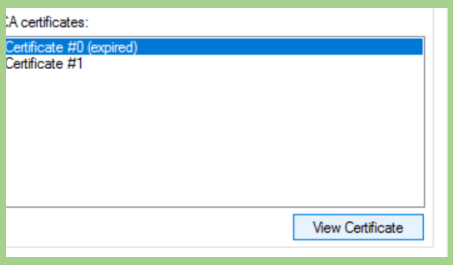
- Sign-in to DC1 VM
- In the Server Manager, Select **Tools > Certificate Authority**



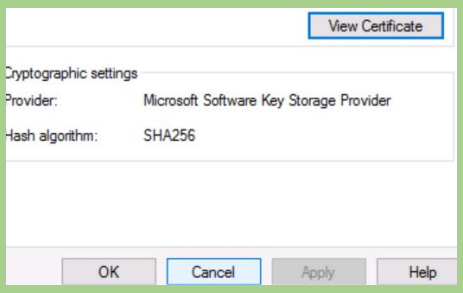
- Right-Click the Server **(515support-CA)** and select properties



- On the General Tab, note the root **(Certificate #0)**
- Select the **View Certificate** button

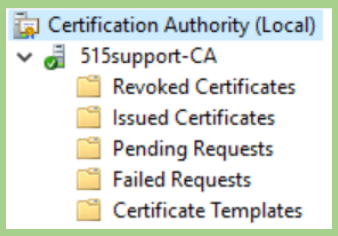


- Close the certificate window and then select Cancel to close the **515 support-CA properties Window**

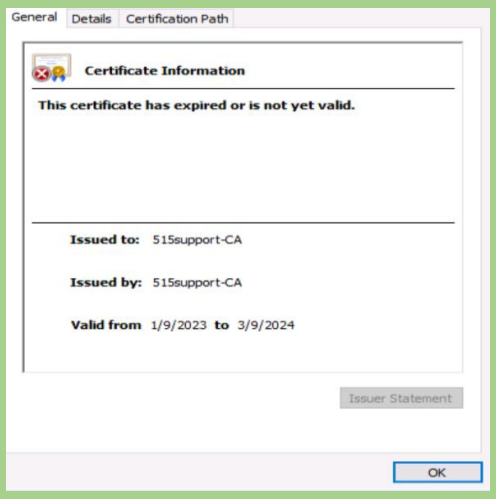


Browse Certificate Services components

- In the Certification Authority console, expand **server 515support – CA** to view the subfolders



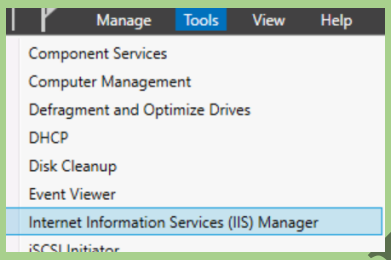
- Select Issued Certificates. The domain controller certificates issued to the host are displayed
- If there is more than one certificate, select the one with the most current **Certificate Effective Date**, and then Right-Click this certificate and select **open**
- Select **Ok** to close the certificate dialog box



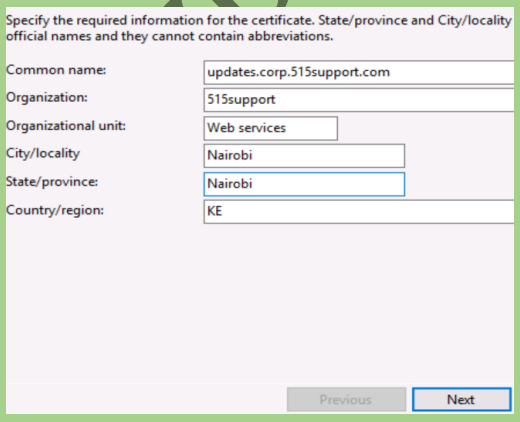
- Select the Certificate Template

Request a Server Certificate

- Switch to MS1 VM
- In the Server Manager select the MS1 server select **Tools > Internet Information Service (IIS) Manager.**



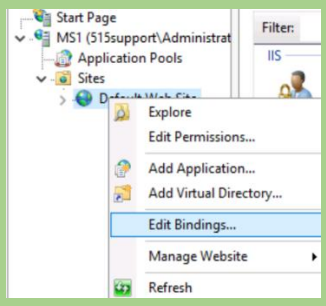
- In the connections pane, select the MS1 server icon. In the **MS1 Home pane**, open the server certificate applet
- In the Actions Pane, select **Create Domain Certificate**. Complete the create certificate wizard
- Select Next



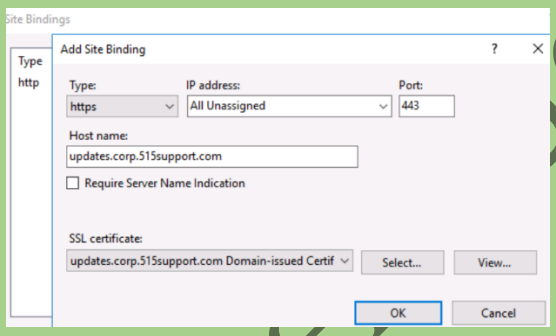
- On the Online Certificate Authority page **select** button, then select **515support-CA** and select OK

Bind Certificate to HTTPS port

- In the IIS Manager, expand the server, then Sites to show the Default Web Site node. Right-Click Default Web Sites and then Select Edit Bindings



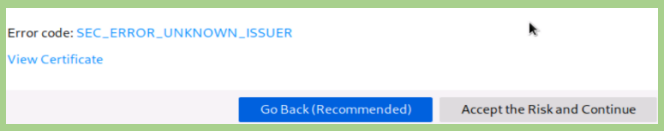
- Select the Add buttons
- In the Add Site Binding dialog box, from the Type box select https
- In the Host name box type: updates.corp515support.com
- From the SSL certificate box select **updates.corp 515support.com Domain -issued certificate**
- Select **OK**



- In the **Site Bindings** dialog box, select the http entry, then select **Remove**. Confirm by selecting **Yes**, select the Close button
- Switch to the DC1 VM and then observe new certificate in the **Issued Certificate** folder

Test Secure Web Services

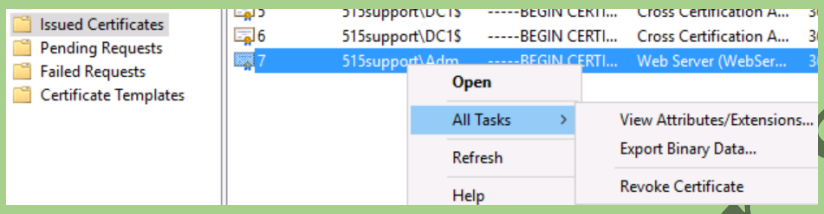
- Switch to PT1-Kali VM
- Use the firefox web browser to connect to https://updates.corp.515support.com
- Navigate through the Interface to accept the risk of connecting to a site with a root of untrusted root certificate



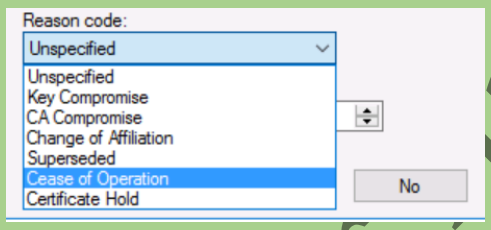
- To the left of the https://updates.corp.515support.com URL, select the padlock icon to display the certificate information. Expand the message for more information on the certificate

Revoke Certificate

- Switch to the DC1 VM. If necessary, the web server certificate in the **Issued Certificate** folder



- Right click the certificate and then select **All Tasks > Revoke Certificate**
- From the reason code box, Select Cease of Operation. Leave the date and time to set to the current time and select Yes to confirm



- Close the **certsrv** console

Observations:

Certificate Server Properties

- Accessed root certificate properties on 515support-CA.
- Confirmed root certificate details and navigated the Certification Authority console.

Browse Certificate Services Components

- Viewed and identified the most current issued certificate for the domain controller.

Request a Server Certificate

- Created and requested a domain certificate using IIS Manager on MS1 VM.
- Bound the certificate to the HTTPS port.

Test Secure Web Services

- Connected to the secure web service on PT1-Kali VM.
- Reviewed and confirmed the certificate information in the browser.

Revoke Certificate

- Revoked the web server certificate on DC1 VM, selecting "Cease of Operation."

Results:

- Root certificate details were confirmed.
- Successfully reviewed issued certificate details.
- Domain certificate created and bound to HTTPS port.
- Secure connection established and certificate information verified.
- Certificate successfully revoked and removed from the issued certificates list.

Conclusion:

The lab effectively demonstrated managing the lifecycle of digital certificates, including creation, issuance, and revocation, using Windows tools and PKI implementation. Secure communications were verified through HTTPS configuration and testing.

Future Work:

- Automate certificate management processes.
- Explore advanced PKI configurations and policies.
- Test cross-platform compatibility of issued certificates.
- Integrate certificate management with security monitoring tools.