HANDS-ON: CERTIFICATE BASED AUTHENTICATION TO MICROSOFT VPN

PREREQUISITES:

1. Windows 2008 R2 Enterprise domain server with the following setup:
   - Active Directory (domain level 2008)
   - Network Policy and Access Services (NPS)
   - Microsoft Certificate Services (Enterprise CA)
2. The following certificate templates enabled on the CA:
   - Enrollment agent
   - Smartcard user

   Set user rights to read and enroll over the templates.
3. SafeNet Authentication Client (SAC) 8.0 installed on the server.
4. Test user in Active Directory.
5. Windows XP Client with SAC 8.0 installed – Optional.
6. PKI services Class session

DURATION:

30 minutes

THE AIM OF THIS HANDS-ON SESSION:

At the end of this hands-on session you will know how to:

1. Configure your domain server for Routing and Remote Access Services (RRAS) for certificate based VPN authentication.
2. Configure the client machine for certificate based authentication to MS-VPN
3. Enroll a smartcard user certificate on behalf of the domain user for VPN authentication and use it with dial-in for authentication

Step 1: Configure the domain server for Routing and Remote Access

1. Verify having a server certificate (by default the server certificate should be installed on the on the computer)
    a. Start MMC console.
    b. Click **File > Add/Remove Snap in**.
    c. Click **Certificates** and then click **Add**.
    d. Choose **Computer account** and click **Next**. Select **Local computer** and click **Finish**.
    e. Click **OK** to close the snap-in selection window.
    f. Expand the **Certificate** console and click **Personal → Certificates**.
    g. View the listed certificates and verify your server has certificate by the name of your domain, issued by the **Domain Controller** certificate template.

Step 2 - Add Routing and Remote Access service to your server for VPN access:

1. From Windows *Start* menu, open **Programs > Administrative Tools > Server Manager**.
2. Expand the **Roles** tree item.
3. Right click *Network Policies and Access Services*, select **Add Role Services.**
    a. Add **Routing and Remote Access Services**. Click **Next** and **Install**.
4. From the *Roles* tree, expand **Network policy and access services** and right click **Routing and Remote Access**.
5. Select **Configure and Enable Routing and Remote Access**.
6. The *Routing and Remote Access Server Setup* wizard opens. Click **Next**.
7. Select **Custom Configuration** and click **Next**.
8. Select **VPN Access** and click **Next**.
9. Click **Finish**. A pop up message indicates creating a default connection request policy. Click **OK**. Click **Start service…**to start the service.

Step 3 - Configure Routing and Remote Access to accept EAP authentication

1. Add EAP protocol
    a. From the Roles tree Right click *Routing and Remote Access* and click **Properties**.
    b. Open the **Security** tab. Click the **Authentication Methods** button.
    c. Make sure the option **Extensible Authentication Protocol (EAP)** is selected. If not select it.
    d. Select all Authentication methods. Click **OK** twice. (A pop up offers you to view help topics – click **No** to close it). Click **OK** twice.

2. Enable EAP in Remote Access Policies
    a. From Windows Administrative tools, select **Network Policy Server** (**NPS).** Set its *Standard Configuration* (right pane) to **RADIUS Server for Dial-Up or VPN Connections**.
    b. Expand **NPS → Policies** tree item.
    c. Select **Connection Request Policies**.
    d. In the right pane, right click the policy **Microsoft Routing and Remote Access service Policy**. Open its properties.
    e. The type of “network access server” field is **Remote Access Server (VPN-Dial up)**.

f. Open the *Setting* tab. Select **Authentication Methods**. In the right pane select **Override network policy authentication settings**.
g. Under EAP types click the **Add** button. Add **Microsoft: Smart card or other certificate**.
h. Click **OK**.

3. Allow Dial in connection for the user accounts
   a. Open *Active Directory Users and Computers* snap-in
   b. In the properties of your test user account open the **Dial-in** tab
   c. Under ***Network access permission***, select **Allow Access** and apply the change.

Step 4 - Enroll Smartcard user certificate for VPN authentication:

At this point you should have a Smart card user certificate enrolled from setting up Microsoft Smart card logon. If not, follow these steps:

Connect token

1. Install SafeNet Authentication Client on the server or workstation on which you intend to enroll.
2. Insert the user's token to the USB port.
3. Start MMC, from the *File* menu, open **Add\remove snap-in.** Open the *Certificates* snap-in. Select the snap-in for "My user account". Click **Finish** and **OK**.
4. In the content tree, under **Personal>Certificates**, right click **Certificates** and select **All Tasks > Advanced Operations > Enroll on behalf of…**
5. Click **Next**.
6. Click next again
7. Select the *Enrollment Agent certificate*: Browse and select **Administrator** certificate you have enrolled in the previous step. Click **Next**.
8. The Certificate Enrollment page opens, and you can select the type of certificate to enroll.
9. Select **Smartcard logon** certificate. Click the Details scroll down menu button to view further options.
10. Click the **Properties** button. In the *Private Key* tab, open the **Cryptographic Service Provider** scroll down menu.
11. Select **eToken Base Cryptographic Provider** and uncheck *Microsoft strong cryptographic provider*. Click **OK**. Click **Next** to proceed with the enrollment.
12. Click **Browse** and select a domain user. Click **Enroll**. (You may need to re-insert the token)
13. The token's password prompt window appears - type in the token's password.
14. After enrollment succeeds, view the new enrolled certificate details. Close the enrollment window.

Step 5: Configure the client for certificate based VPN authentication (XP or 2008)

1. Choose **one** of the below two options:
   a. Create a new dialer connection on the client machine (XP)
      i. From Windows *Start* menu, open **Settings→Network Connections**.
      ii. Double click **Create a new connection** (may appear as **New Connection wizard**). When the wizard opens, click **Next**.
      iii. Under *Network Connection Types*, select **Connect to the network at my workplace**. Click **Next**.

iv. Select **Virtual Private Network connection** and click **Next**.
v. Name the connection and click **Next**.
vi. Type in the IP address of the VPN server and click **Next.**
vii. Select Anyone's use and finish the setting up the connection.

b. Alternatively, Create a new dialer connection on Windows 2008
i. Right click the Network icon on your Desktop and open **Properties**.
ii. Select the task **Setup a new connection or network**
iii. Select **connect to a workplace**. Click **Next**.
iv. Select **Use my Internet Connection (VPN)**
v. When you are asked to setup your Internet connection, type in the **IP address** of your authenticating server and provide a name for the new connection.
vi. At the check boxes below, select **use a smart card** and allow also other people to use this connection.
vii. Click **Connect**. You will be now asked to insert the smartcard. Insert the token. Provide the PIN for authentication.

Step 6 - Authenticate to the VPN using the Token:

1. Logon as the domain user to whom you enrolled the certificate on the Token.
2. Insert the token if you have not logged on using smart card logon.
3. Right click the new VPN connection created and select **Connect**.
4. Enter the Token's password when you are prompted for the smartcard PIN. Click **OK**.
5. Accept the connection (first time).
6. Connection window should appear. Click **OK**.