

Creating and Installing a Self Signed Certificate for PEAP Authentication

A server side X.509 digital certificate is required for PEAP authentication. This certificate can be purchased from a third-party Certificate Authority such as VeriSign, or it can be issued from an organization's internal Certificate Authority. But these options may be costly for test environments.

Creation of Self Signed Certificate

TekCERT

You can use TekCERT to generate self signed certificates for test environments. TekCERT is a standalone executable program which requires Microsoft .NET Framework 2.0. You can download TekCERT from TekRADIUS Support site.

When you run TekCERT you will see following form to create a certificate:

The screenshot shows the 'TekCERT - Certificate Generator' application window. It has two tabs: 'Certificate Generation' (selected) and 'Browse Certificates'. The 'Certificate Generation' tab contains the following fields and options:

- Issued to:**
 - Name: Test
 - Organization: Test Org.
 - City: Istanbul
 - State: (empty)
 - Country: TR
- Options:**
 - Key Length: 1024
 - Valid for [Day(s)]: 30
 - Serial #: 2652daa4f489c11f
- Operation:**
 - Reset Form
 - Generate Certificate

At the bottom of the window, there is a status bar that says 'TekCERT is ready' and buttons for 'About' and 'Exit'.

Figure 1. - TekCERT certificate parameters

Click “Generate Certificate” button to create the certificate after filling necessary fields. You need to enter at least a valid “Name” for the certificate.

The screenshot shows the 'TekCERT - Certificate Generator' application window with the 'Browse Certificates' tab selected. It displays a table of generated certificates:

Issuer	Issued to	Not Before	Not After	Key Length
Test	Test	12.05.2008	11.06.2008	1024
USER	USER	03.01.2008	02.01.2009	1024

Below the table, there are buttons for 'Delete' and 'Export'. At the bottom of the window, the status bar says 'Certificate created.' and there are buttons for 'About' and 'Exit'.

Figure 2. - Browse certificates

You can export public key in .cer (*DER encoded X.509*) format after creating the certificate for client deployment. Click “Browse Certificates” tab, select the generated certificate and click “Export” button.

SelfSSL

There are a couple of tools can be used for generating a self signed certificate. You can use OpenSSL or SelfSSL comes with Internet Information Services (IIS) 6.0 Resource Kit. You can download Internet Information Services (IIS) 6.0 Resource Kit from:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&displaylang=en>.

After downloading resource kit, double click to installation file (iis60rkt.exe) and follow the instructions.

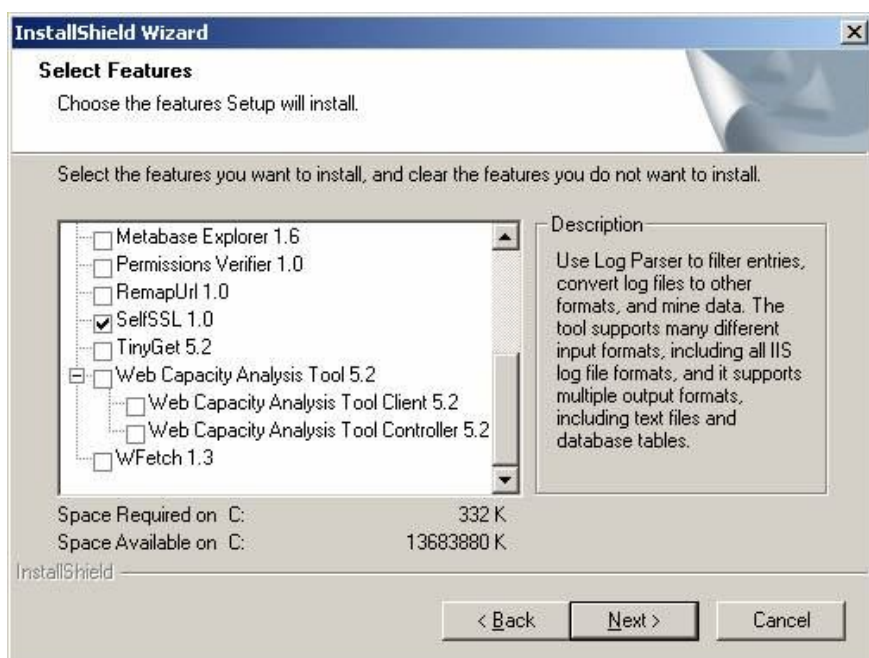


Figure 3. - Select Features dialog

You can select just SelfSSL 1.0 component as it is the only component required. Although it is built to generate test certificates for IIS, these certificates can be used by RADIUS servers as they are standard X.509 type certificates.

On the RADIUS Server, open up a command prompt and go to the directory where you installed it (*C:\Program Files\IIS Resources\SelfSSL is default*). Type the following command to generate the certificate:

```
selfssl /N:CN=Servername /K:1024 /V:365 /S:1 /P:443
  /N : CN is the identifier for your certificate and can be the name of the server.
  /K : is size of the RSA key in bits. Set to 1024.
  /V : is the number of days before the certificate expires. Set to 365 for one year.
  /S : is the site number in IIS.
  /P : is the TCP port number. 443 is the standard SSL port.
```

/S and /P parameters are not important as you do not have an IIS installed on the server. If you don't have IIS installed, executing the SelfSSL command will return an error message; "Error opening metabase: 0x80040154". This error is occurred when an IIS site was not found so just ignore it.

Creation of Root Certificate and Client Deployment

You do not need to deploy a root certificate on clients as long as you require server's certificate verified by the clients. But if you require client verification of server certificate, you need to export root certificate and deploy it on the clients.

Click Start/Run and type "mmc" (*Without quotes*) and click OK. Select "Add/Remove Snap-in" on File menu. Click "Add" button on "Add/Remove Snap-in" dialog. Select clicking on "Certificates" entry on "Add Standalone Snap-in" dialog and click "Add" button.

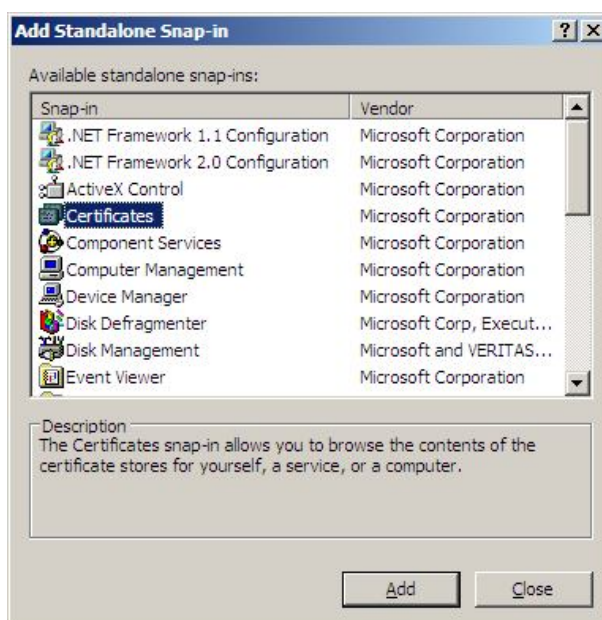


Figure 4. – Add Standalone Snap-in dialog

Select "Computer account" on "Certificates snap-in" dialog and click "Next". Select "Local computer" on "Select Computer" dialog and click "Finish". Close "Add Standalone Snap-in" dialog clicking "Close Button".

On "Console Root" tree expand Certificates/Personal/Certificates key. You must see the certificate you've recently created. Right click on your certificate's entry and select All Tasks/Export. Click "Next" on Certificate Export Wizard" dialog. Select "No, do not export the private key" and click "Next". Select "DER encoded binary X.509 (.CER)" and click "Next". Specify a file name for the root certificate and click "Next". Click "Finish" on the last dialog displayed.

Now you have the root certificate can be deployed on the clients.

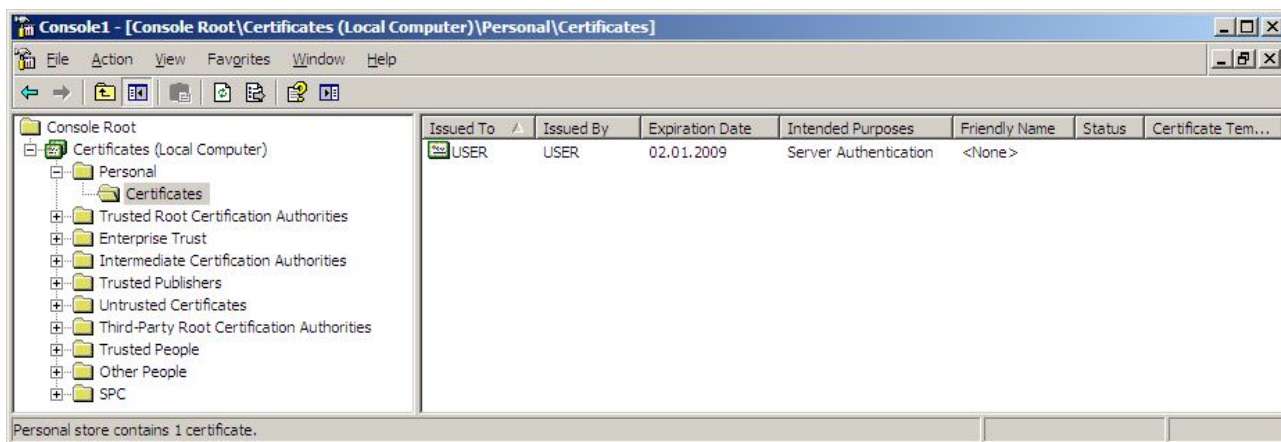


Figure 5. - MMC Console

Client Deployment

Copy the file contains root certificate to client computer. Locate the certificate file on the client computer; right click on it than select "Install Certificate". Click "Next" on "Certificate Import Wizard" dialog. Select "Place all certificates in the following store" than click "Browse". Click "Show physical stores" and then select "Trusted Root Certification Authorities/Local Computer", click OK to close "Select Certificate Store" dialog.



Figure 6. - Select Certificate Store dialog

Click "Next" after selecting certificate place on "Certificate Import Wizard" dialog and then click "Finish" to complete manual deployment of server root certificate.

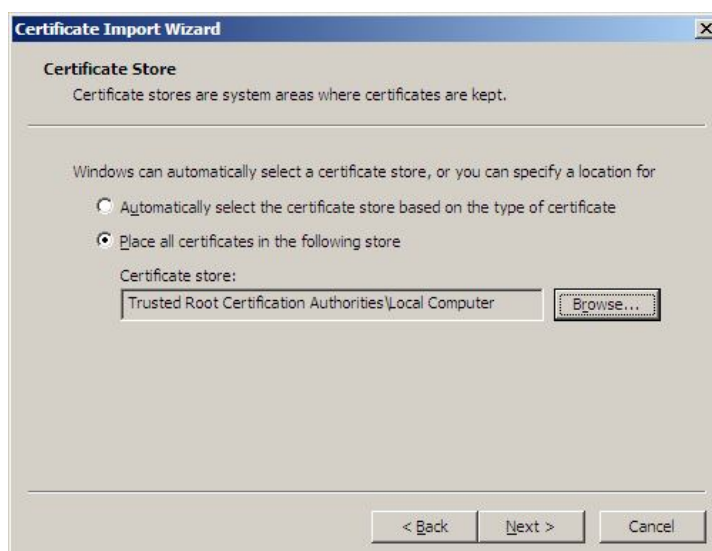


Figure 7. - Certificate Import Wizard dialog



Figure 8. - Certificate Import Wizard dialog

Client PEAP Configuration

Although there are commercially and freely available PEAP supported 802.1X supplicant alternatives for Windows, Windows XP and Vista has a built-in supplicant. In order to configure PEAP (PEAPv0-EAP-MS-CHAP v2) Authentication for a Wireless Network Connection, open Network Connections (Start/Settings/Network Connections), right click on particular wireless connection and select properties.

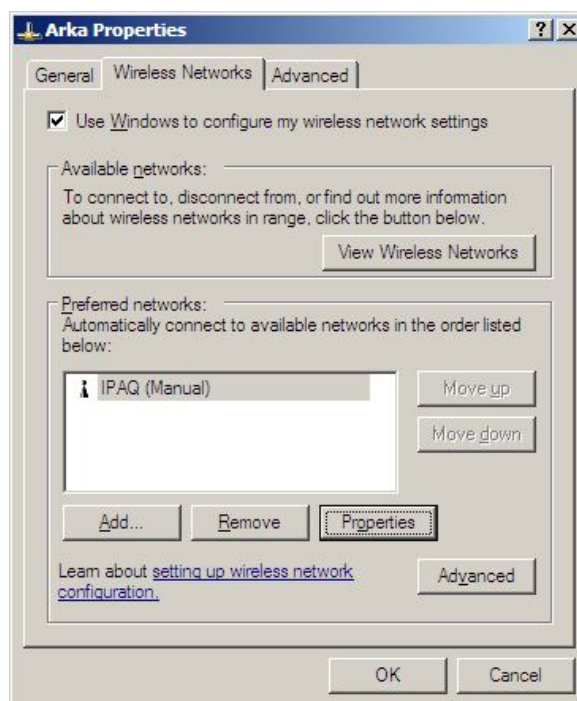


Figure 9. - Wireless Networks Connection/Wireless Networks tab.

You will see detected wireless networks in "Preferred networks" window on "Wireless Networks" tab. Select wireless network which requires PEAP authentication and then click properties.

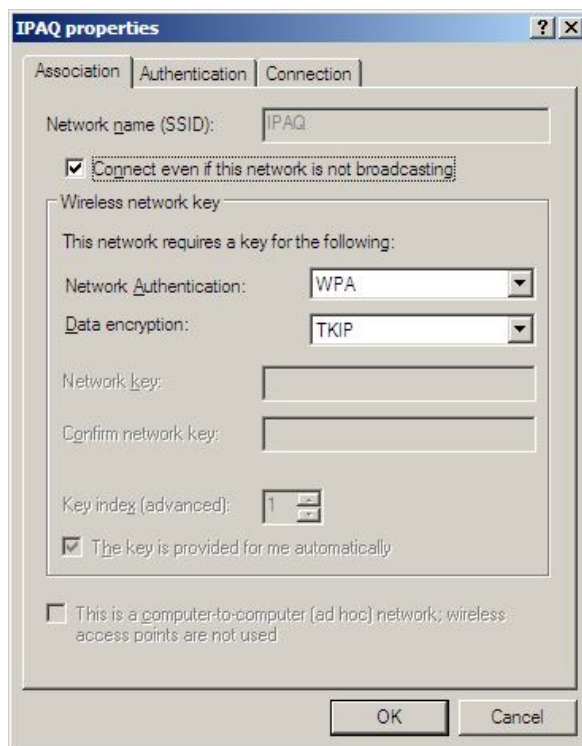


Figure 10. - Association parameters.

Configure “Association” parameters as shown in Figure 8. Jump to “Authentication” tab select “Protected EAP (PEAP)” as “EAP Type” then click “Properties”.

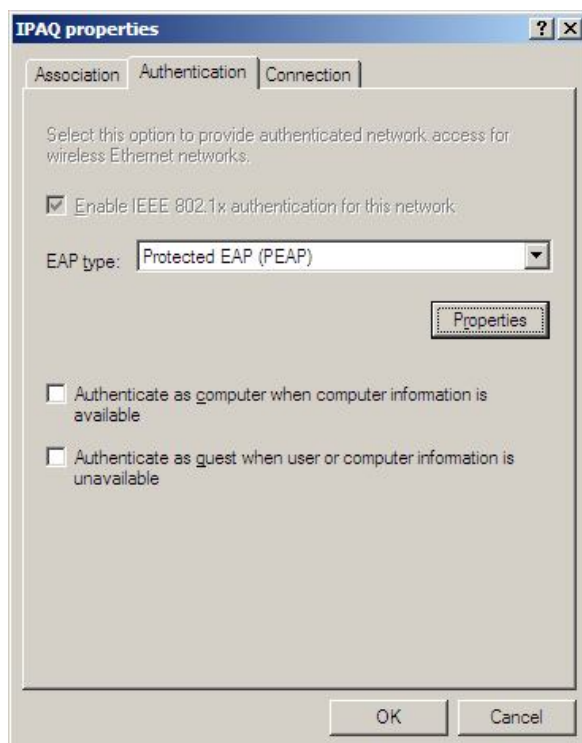


Figure 11. - EAP type selection.

Click “Validate server certificate”, and select installed server root certificate installed previously in the “Trusted Root Certification Authorities” list. Set other options as shown in Figure 10.

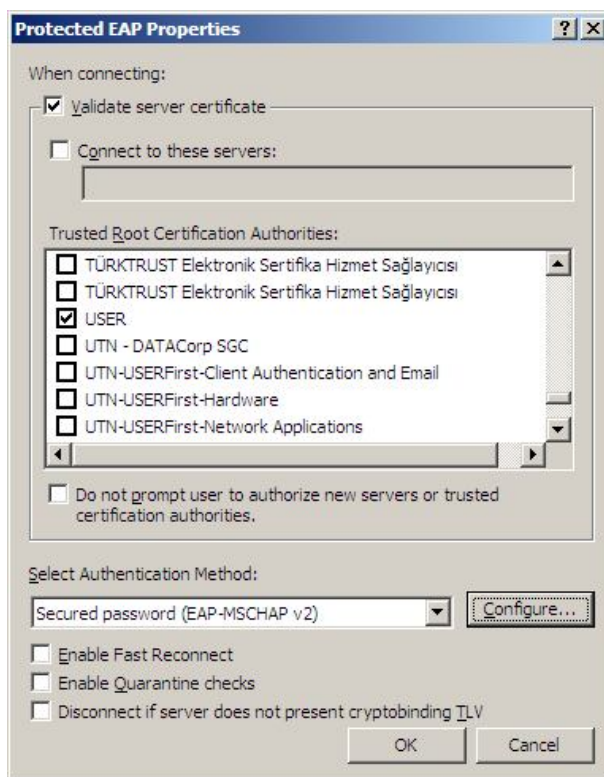


Figure 12. - Protected EAP Properties dialog.

If you plan to authenticate user with a username/password pair other than the user uses to logon to Windows, click “Configure” button on “Protected EAP Properties” dialog and uncheck “Automatically use my Windows logon name and password” on “EAP MSCHAPv2 Properties” dialog and click OK.



Figure 13. - EAP MSCHAPv2 Properties dialog.