# *Creating and Installing a Self Signed Certificate for PEAP/EAP-TLS Authentication*

A server side X.509 digital certificate is required for PEAP/EAP-TLS 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

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:

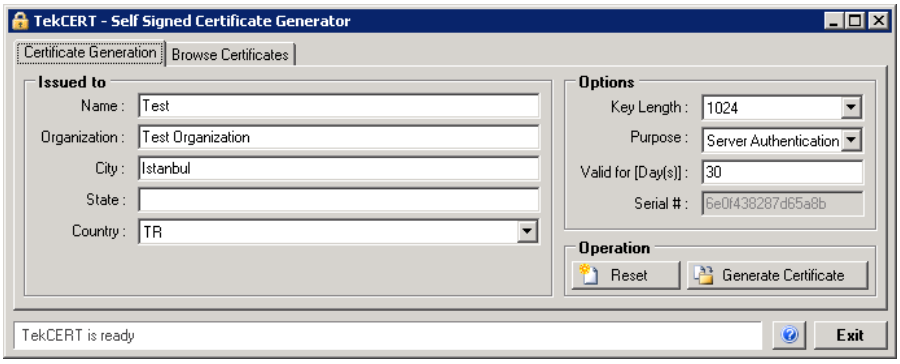


**Figure 1.** - TekCERT certificate parameters

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

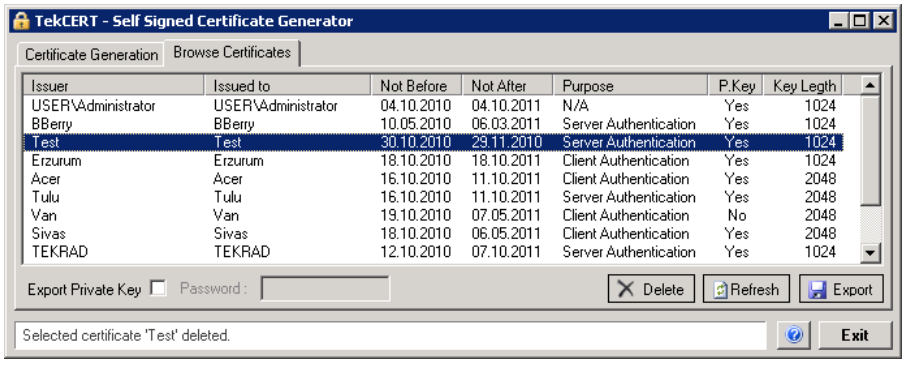


**Figure 2.** - Browse certificates

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.

You can also create client certificates using TekCERT. Select “Client Certificate” as Purpose to create Client Certificates in certificate parameters. You must export client certificate with its associated private key for client deployment in .pfx format.

## Certificate Deployment at Client Side

You do not need to deploy a root certificate on clients as long as you don't 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.

### Server Certificate

Copy the file contains server 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 3.** - 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.

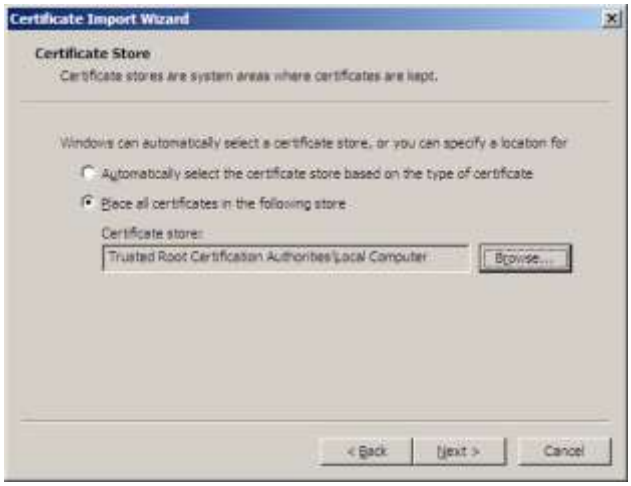


**Figure 4.** - Certificate Import Wizard dialog


**Figure 5.** - Certificate Import Wizard dialog

### Client Certificate

Copy the file contains client certificate to client computer. Locate the certificate file on the client computer; double click on the certificate file. Click next *(Figure 19)*;

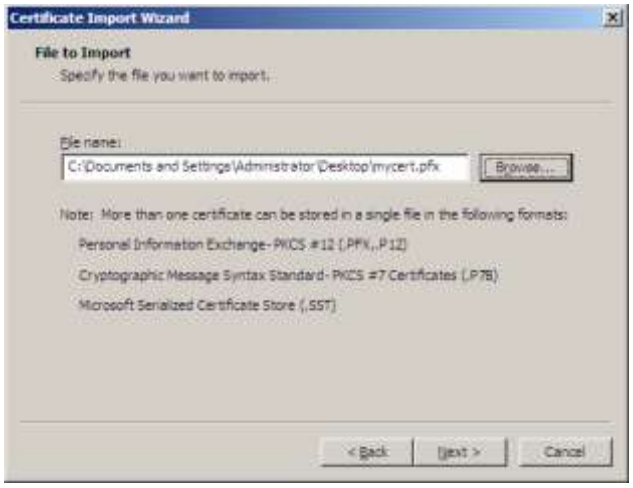


**Figure 6.** - Certificate Import Wizard dialog

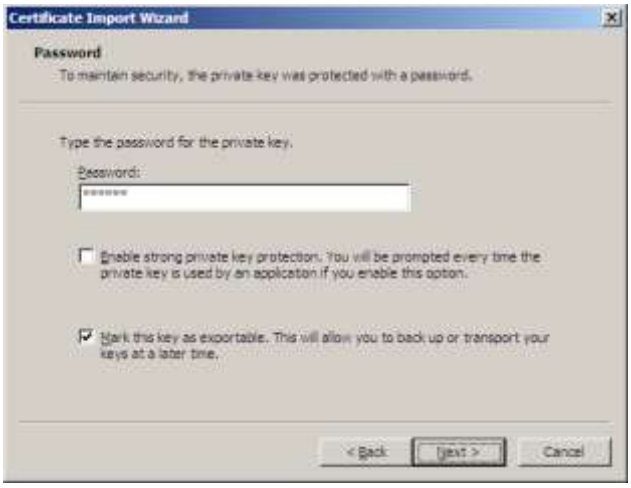


**Figure 7.** - Certificate Import Wizard dialog

Enter private key password, select "Mark this key as exportable…" and click Next. Select "Automatically select the certificate store based on the type of certificate" and click Next. Click Finish at the latest dialog.

## Client PEAP Configuration

Although there are commercially and freely available PEAP supported 802.1X supplicant alternatives for Windows, Windows editions have 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 8.** - Wireless Networks Connection/Wireless Networks tab.

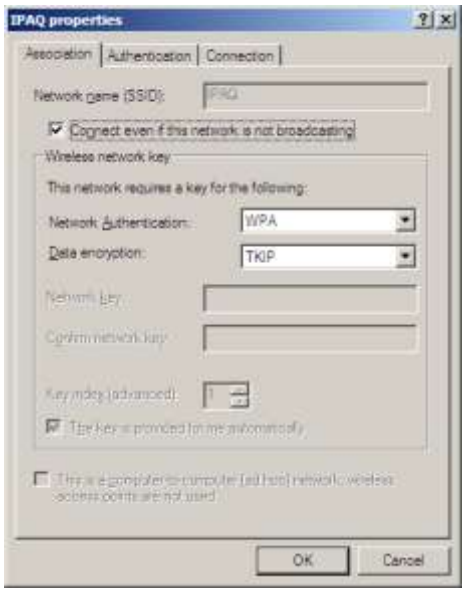


**Figure 9.** - Association parameters.

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.

Configure "Association" parameters as shown in Figure 7. Jump to "Authentication" tab select "Protected EAP (PEAP)" as "EAP Type" then click "Properties".

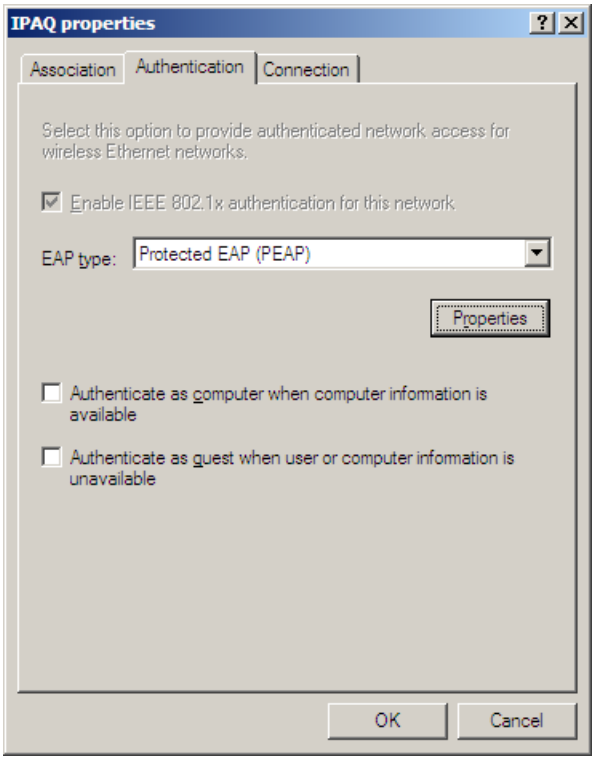


**Figure 10.** - EAP type selection

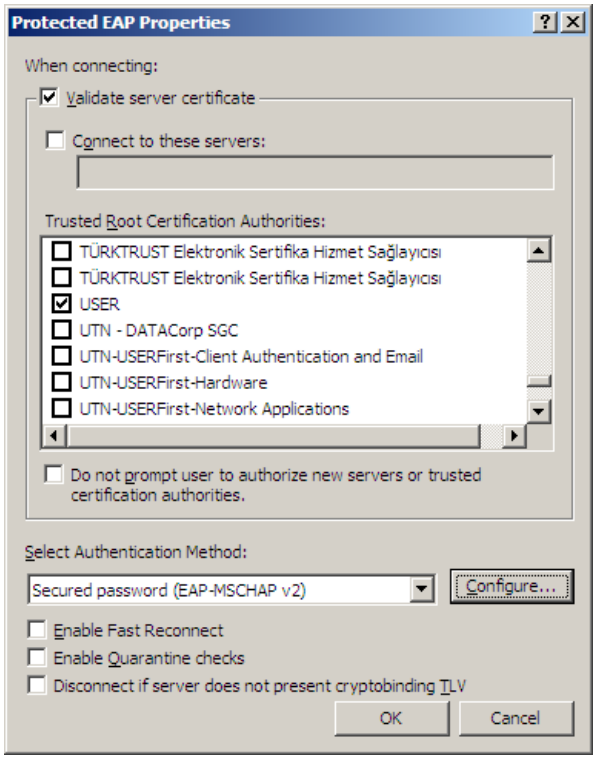


**Figure 11.** - Protected EAP Properties dialog.

Click "Validate server certificate", and select installed server root certificate installed previously in the "Trusted Root Certification Authorities" list optionally. Set other options as shown in Figure 9.

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.

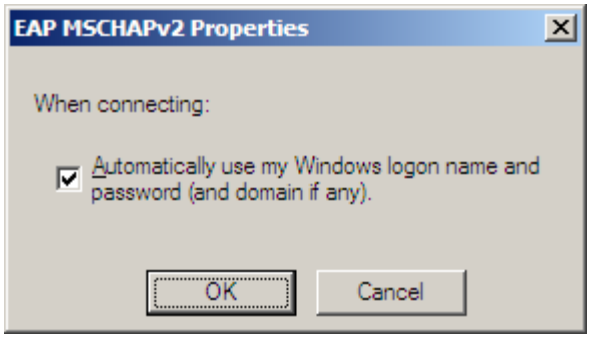


**Figure 12.** - EAP MSCHAPv2 Properties dialog.

You can also deploy TekWiFi on client computers to simplify PEAP provisioning on client side. TekWiFi automatically configures PEAP settings and connects to wireless network. You can download TekWiFi from TekRADIUS web site.

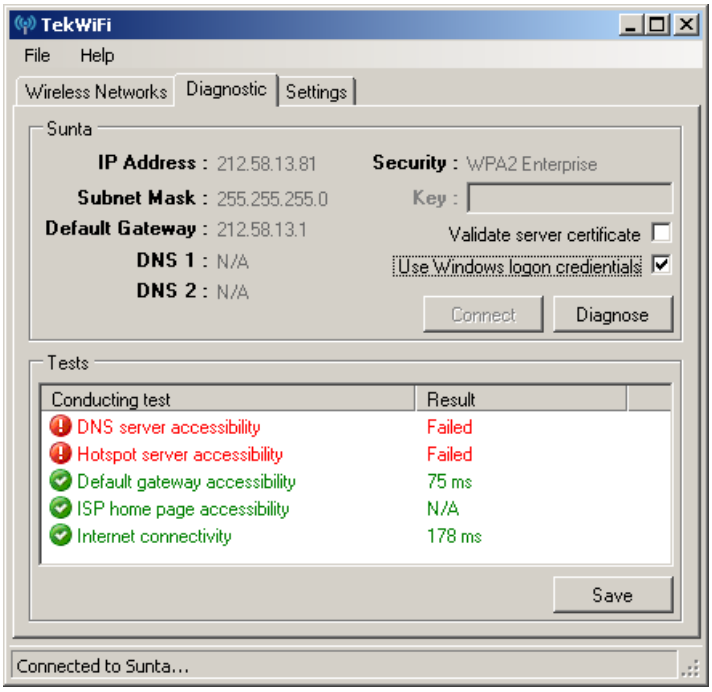


**Figure 13.** – TekWiFi Settings.

## Client EAP-TLS Configuration

In order to configure EAP-TLS Authentication for a Wireless Network Connection, open Network Connections *(Start/Settings/Network Connections)*, right click on particular wireless connection and select properties.


**Figure 14** - Wireless Networks Connection/Wireless Networks tab.


**Figure 15.** - Association parameters.

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.

Configure “Association” parameters as shown in Figure 20. Jump to “Authentication” tab select “Smart Card or Certificate” as “EAP Type” then click “Properties”.


**Figure 16.** - EAP type selection

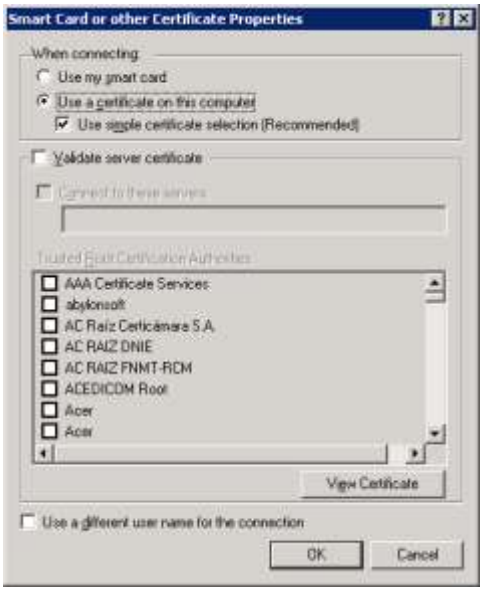


**Figure 17.** - Protected EAP Properties dialog.

Click “Validate server certificate”, and select installed server root certificate installed previously in the “Trusted Root Certification Authorities” list optionally. Set other options as shown in Figure 27.