# 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:

| 🔒 TekCERT - Sel    | f Signed Certificate Generator |                                   |
|--------------------|--------------------------------|-----------------------------------|
| Certificate Genera | tion Browse Certificates       |                                   |
| Issued to          |                                | Options                           |
| Name :             | Test                           | Key Length : 1024 💌               |
| Organization :     | Test Organization              | Purpose : Server Authentication 💌 |
| City :             | Istanbul                       | Valid for [Day(s)] : 30           |
| State :            |                                | Serial # : 6e0f438287d65a8b       |
| Country :          | TR                             | - Oti                             |
|                    |                                | Operation                         |
|                    |                                | 🎦 Reset 🛛 💾 Generate Certificate  |
|                    |                                |                                   |
| TekCERT is ready   |                                | 🙆 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.

| Issuer             | Issued to          | Not Before | Not After  | Purpose               | P.Key | Key Legth |     |
|--------------------|--------------------|------------|------------|-----------------------|-------|-----------|-----|
| USER\Administrator | USER\Administrator | 04.10.2010 | 04.10.2011 | N/A                   | Yes   | 1024      |     |
| BBerry             | BBerry             | 10.05.2010 | 06.03.2011 | Server Authentication | Yes   | 1024      |     |
| Test               | Test               | 30.10.2010 | 29.11.2010 | Server Authentication | Yes   | 1024      |     |
| Erzurum            | Erzurum            | 18.10.2010 | 18.10.2011 | Client Authentication | Yes   | 1024      |     |
| Acer               | Acer               | 16.10.2010 | 11.10.2011 | Client Authentication | Yes   | 2048      |     |
| Tulu               | Tulu               | 16.10.2010 | 11.10.2011 | Server Authentication | Yes   | 2048      |     |
| Van                | Van                | 19.10.2010 | 07.05.2011 | Client Authentication | No    | 2048      | - 1 |
| Sivas              | Sivas              | 18.10.2010 | 06.05.2011 | Client Authentication | Yes   | 2048      |     |
| TEKRAD             | TEKRAD             | 12.10.2010 | 07.10.2011 | Server Authentication | Yes   | 1024      |     |

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*);

TekRADIUS - Creating and Installing a Self Signed Certificate for PEAP Authentication

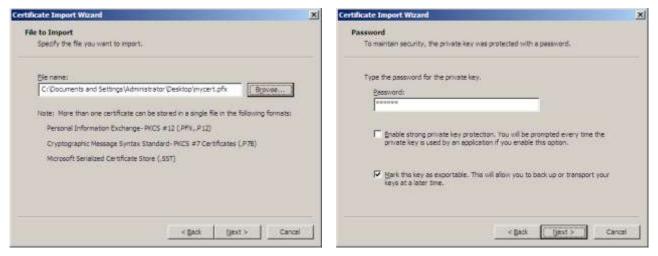


Figure 6. - Certificate Import Wizard dialog

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.

| Arka Properties  | <u> 2 × </u> | IPAQ properties  | States of the local division in which the local division in the lo |
|--|--------------|--|--|
| General Witeless Networks   Advanced   | 1            | Association Authenboasion  | Connection   |
| ₩ Use Windows to configure my wireless network setting   | ()           | Network game (SSID):   | PRQ.   |
| Available getworks<br>To connect to, deconnect from, or find out more informat<br>about weekes networks in range, click the button below<br>View Wireless Netw |              | Cognect even if this ne<br>Wireless network key<br>This network requires a key |  |
| Enferted networks<br>Automatically connect to available networks in the order<br>below:  | listed       | Network Authentication.<br>Data encryption                                     | WPA<br>TKIP  |
| PAQ (Menual)  Moon   |              | Network Ley<br>Ogetrometeck Lap  |  |
| Add Benove Properties  | noed         | <b>10</b> The set = provided by  |  |
| CK   | Cancel       | The all expendence com<br>access points are not use                            |  |

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.

? | x

•

Cancel

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

| IPAQ properties  | ? X         Protected EAP Properties         ?  | Ľ× |
|--|---|----|
| Association Authentication Connection Select this option to provide authenticated network access for wireless Ethernet networks.   | When connecting:           Image: Walidate server certificate           Image: Connect to these servers:  |    |
| Enable IEEE 802.1x authentication for this network      EAP type: Protected EAP (PEAP)      Propertie      Authenticate as computer when computer information is     available      Authenticate as guest when user or computer information is     unavailable | UTN-USERFirst-Olient Authentication and Email   |    |
| OKCan  | Select Authentication Method:<br>Secured password (EAP-MSCHAP v2)  Enable Fast Reconnect Enable Quarantine checks Disconnect if server does not present cryptobinding <u>T</u> LV  Cancel OK Cancel |    |

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.

TekRADIUS - Creating and Installing a Self Signed Certificate for PEAP Authentication

| /ireless Networks Diagnostic Settings  |                                |
|--|--------------------------------|
| Sunta  | •                              |
| IP Address : 212.58.13.81  | Security : WPA2 Enterprise     |
| Subnet Mask : 255.255.255.0  | Key :                          |
| Default Gateway: 212.58.13.1   | Validate server certificate    |
| DNS 1 : N/A  | Use Windows logon credientials |
| DNS 2 : N/A  | Connect Diagnose               |
| Tests  |                                |
| Conducting test  | Result                         |
| ONS server accessibility   | Failed                         |
| Hotspot server accessibility   | Failed                         |
|  | 75 ms                          |
| Default gateway accessibility  | N/A                            |
| <ul> <li>Default gateway accessibility</li> <li>ISP home page accessibility</li> </ul> | 078                            |
|  | 178 ms                         |

**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.

| Arka Properties   | <u>? × </u>  | IPAQ properties   | ?    |
|---|--|---|------|
| ieneral Wireless Networks Advanced  | 1  | Association Authentication Connection   |      |
| 🔽 Use Windows to configure my wheless network set   | Inge   | Network game (SSID):  |      |
| Available getworke  | annes de la  | Cognect even if this network is not broadcasting  |      |
| To connect to, deconnect from, or find out more infor<br>about wireless networks in range, click the button bel |  | Wineless network key  |      |
| Vew Wireless N  | CONTRACTOR OF THE OWNER | This network requires a key for the following:  |      |
| Parlemed petworks   |  | Network Authentication. WPA   | •    |
| Automatically connect to available networks in the on<br>below.   | der listed   | Deta enoyption:   | •    |
| T (PAQ (Menue))   | sovietati i  | Network Ley   |      |
|   | on gions ]   | Cgelen netwerk kep  | 1    |
| 3ddBenove Properties  |  | Say ndeg (advanced)   |      |
|   | tyances  | The tree is provided for the automatically  |      |
| contaunoon  |  | The angle of the second terms of the formation of the second s |      |
| OK.   | Cancel   |   |      |
|   |  | OK Car  | icel |

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".

| Color: If the option to provide and term attraction entropy, access for constant Effective EEE COLOR and term attraction to the network. EAP type: Emeril Color or other Certificate Properties Properties Authenticate as grouputer when computer information is analyticate as grouputer when user or computer information is analyticate as groups when user or computer information is analyticate. | Association | Authentication Connection                            |
|---|-------------|--|
| EAP type: Smart Card or other Certificate  Ptoperties  Ptoperties  Authenticate as gomputer when computer information is available  Authenticate as guest when user or computer information is  |             |  |
| Properties  | F Endbi     | EEE 0021 caution to this network.                    |
| Authenticale as gomputer when computer information is<br>available     Authenticale as guest when user or computer information is   | EAP type    | Smart Card or other Certificate                      |
| T Authenticate as guest when user or computer information is  |             | ficale as gomputer when computer information is      |
|   |             | ficate as guest when user or computer information is |
|   |             | iddae  |

| When connecting C Use my great card C Use a gettificate on this computed G Use significate on this computed G Use signific certificate selection (Recommended) C Validate server certificate |    |
|--|----|
| <ul> <li>Use a getificate on this computed</li> <li>Use siggle certificate selection (Recommended)</li> </ul>  |    |
| Use siggle certificate selection (Recommended)   |    |
|  |    |
| T Yaldate server certificate   |    |
|  |    |
| Carried to there are used  | -  |
| I used East Catherine Autostan   |    |
| AAA Certificale Services   |    |
| Ac Reiz Certicenere S.A.   | 11 |
| AC RAIZ DNIE   |    |
| AC RAIZ FNMT-REM   |    |
| ACEDICOM Root  |    |
| Acer   |    |
| Acti   | 4  |
|  | 9  |
| View Certificate   |    |
| Use a different user name for the connection   |    |
|  | 31 |
| OK Cancel  | _  |

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.