



**WLAN über WPA mit auf Smart Cards abgelegten  
digitalen Zertifikaten absichern  
- Short How-To -**

## INHALT

INHALT.....	2
Voraussetzungen.....	3
Serverseitige Einstellungen.....	3
Policy-Setup.....	3
RADIUS-Authentifizierung.....	6
Einstellungen am Access Point.....	7
Clientseitige Einstellungen.....	9
Protokollierung.....	11

## Voraussetzungen

Das Dokument setzt eine Microsoft-Systemumgebung auf Client- und Serverseite voraus. Die hier beschriebene Vorgehensweise stammt von einem Windows Server 2003 mit Active Directory Einbindung. Um in einer Windows Domain digitale Zertifikate ausstellen zu können, ist eine CA (Certificate Authority) notwendig, welche ebenfalls im Lieferumfang des Windows Servers (2000, 2003 und auch Small Business Server) enthalten ist. Prinzipiell könnte die gesamte Konfiguration auf einem einzigen SBS-Server umgesetzt werden. In einer derartigen Single-Server-Testumgebung wird allerdings von einer Konfiguration mit mehreren Subnetzen ausdrücklich abgeraten, da sich sonst die Problematik mit Multi-homed Domain Controllern ergibt.

- 1) Auf Seite der Server wird folgende Umgebung und Dienste benötigt:
  - Active Directory integrated Domain
  - Microsoft Enterprise Certificate Authority installiert (beim Server dabei)
  - Microsoft Internet Authentication Service (beim Server dabei)
  - Microsoft Routing and Remote Access (beim Server dabei)
- 2) WLAN Access Point oder Router mit WPA-Funktionalität.
- 3) Auf der Clientseite wird folgende Konfiguration eingesetzt:
  - Windows XP Service Pack 2 (funktioniert auch ohne, allerdings wurde in SP2 die WLAN-Anbindung überarbeitet)
  - Interne oder Externe WLAN-Karte
  - Smart Card Reader mit PC/SC-Treiber
  - Smart Card mit CSP (z.B. von Gemplus oder G&D)

## Serverseitige Einstellungen

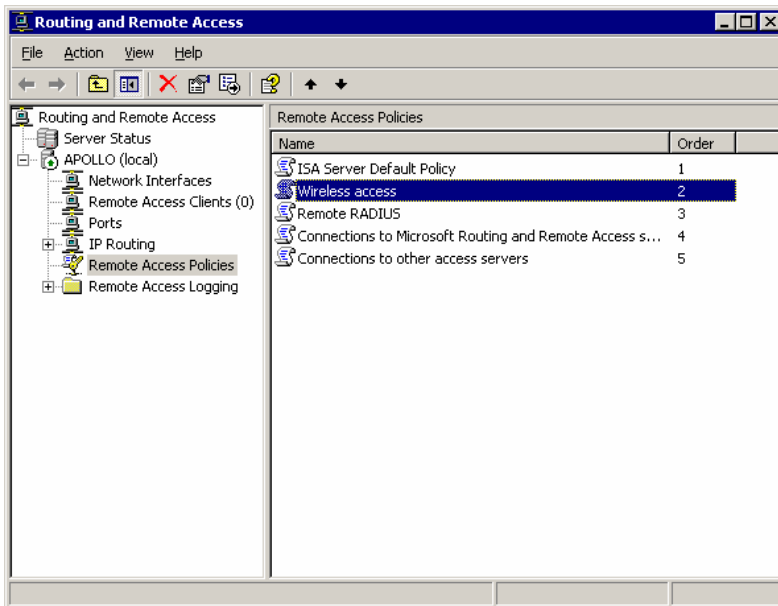
Die Installation der angeführten Komponenten ist nicht Teil von diesem Kurzüberblick. Ebenso ist die Konfiguration der CA und das entsprechende Ausstellen von Zertifikaten auf einer Smart Card einer Separaten Anleitung zu entnehmen. Sie können von den bestehenden sowohl das „Smart Card User“- als auch das „Smart Card Logon“-Template benutzen.

Im Folgenden Finden Sie die Einstellungen Step-By-Step:

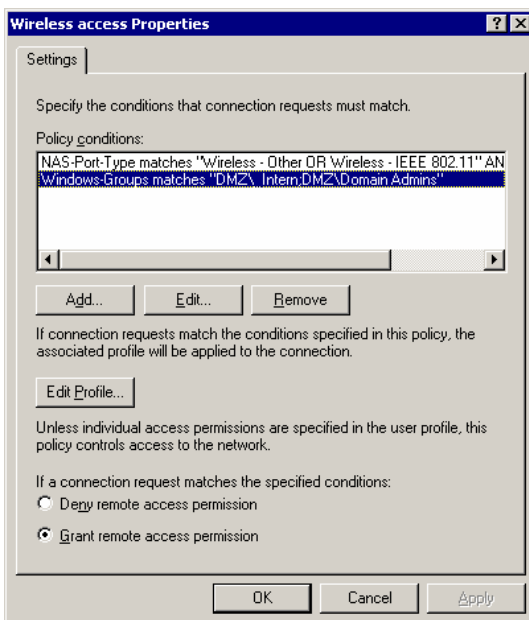
### ***Policy-Setup***

Start\Administrative Tools\Routing and Remote Access aufrufen:

Mit der rechten Maustaste auf der Remote Access Policy lassen sich neue Policies anlegen. Damit ließe sich auch über einen unsicheren Kanal (z.B. mit WEB-Verschlüsselung, wenn die bestehende Infrastruktur kein WPA unterstützt) noch eine Absicherung mit Zertifikaten und Smart Card auf einer Ebene höher umsetzen (VPN mit EAP-Authentifizierung). Legen Sie eine neue Policy für den WLAN-Zugang an. Hier wurde diese Bedingung mit „Wireless Access“ benannt.

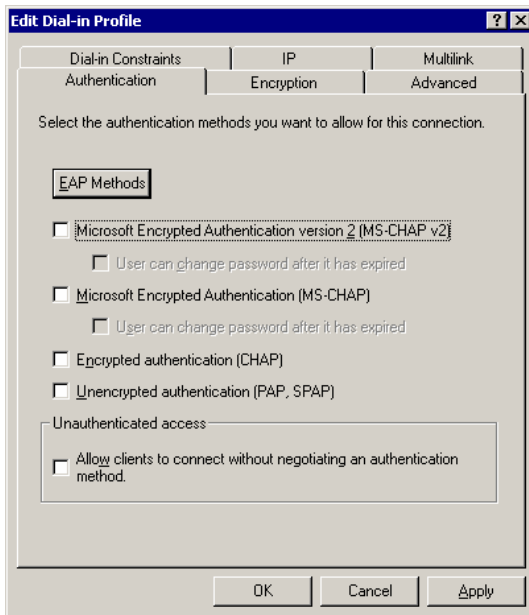


Bei den Eigenschaften der Policy müssen die Bedingungen konfiguriert werden:

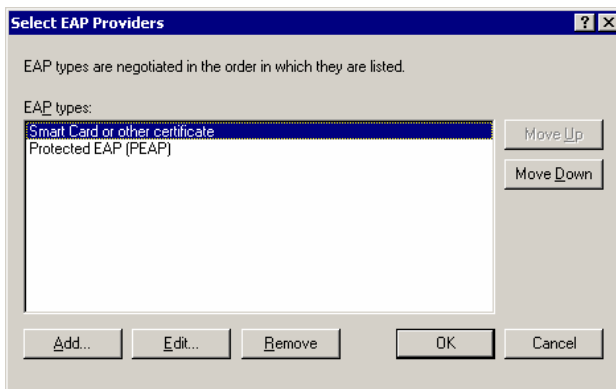


Sie können mit „Add...“ conditions hinzufügen und bestimmen, bei welchen Verbindungen diese Policy gilt. Nachdem es sich hier um ein Wireless-Interface handelt wird die erste Einschränkung mit dem NAS-Port-Type (wird vom WLAN-AP/Router mitgesendet) mit "Wireless - IEEE 802.11" und "Wireless - Others" gemacht - sieht man nachher im log, was tatsächlich gesendet wird. Die zweite Einschränkung betrifft die Benutzergruppe: für wen darf diese Regel angewandt werden.

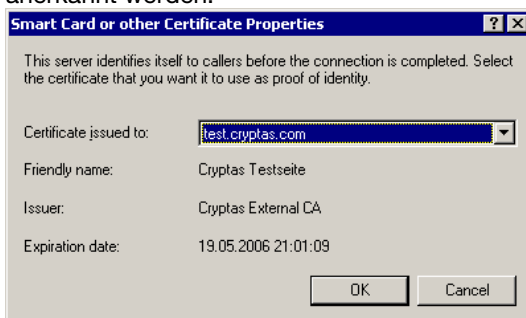
Danach lassen sich mit "Edit Profile..." vor allem die zulässigen Authentifizierungsmechanismen festlegen:



Mit MS-CHAP v2 würde die klassische Windows-Anmeldung mit UN/PWD noch weiter funktionieren, wollen wir aber nicht, da bei uns alles über EAP-Authentifizierung ablaufen soll. In den „EAP-Methods“ finden sich dann folgende Einstellungsmöglichkeiten:

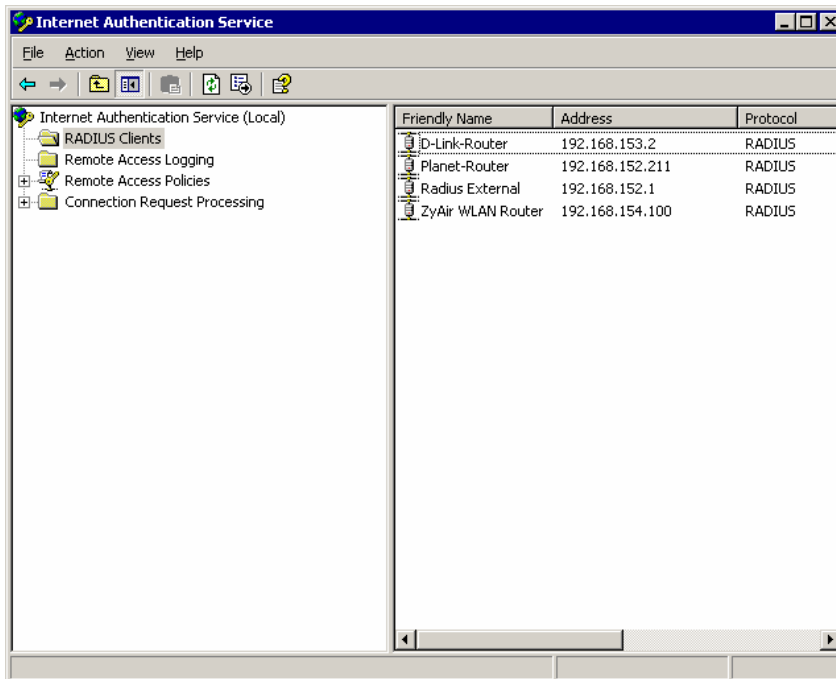


Hier kann man entweder ausschließlich auf Zertifikatsbasierte Authentifizierung setzen, oder zusätzlich noch verschlüsselte Passwörter zulassen (über mehrere Policies kann das dann natürlich auch Benutzerspezifisch passieren). Unter „Edit“ wird die CA festgelegt, welche die Zertifikate für die Anmeldung ausstellt. Sie legt fest, welche Zertifikate für die Authentifizierung anerkannt werden.



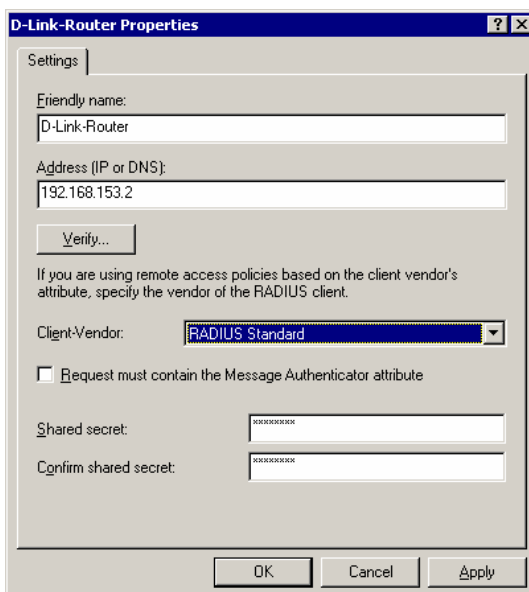
## RADIUS-Authentifizierung

Start\Administrative Tools\Internet Authentication Service aufrufen.



In den „Properties“ des Dienstes lassen sich neben der Serverbeschreibung und den Logging-Optionen (hier zumindest für den Beginn alles aktivieren) noch die Ports für Authentication (default 1812) und Accounting (1813) festlegen.

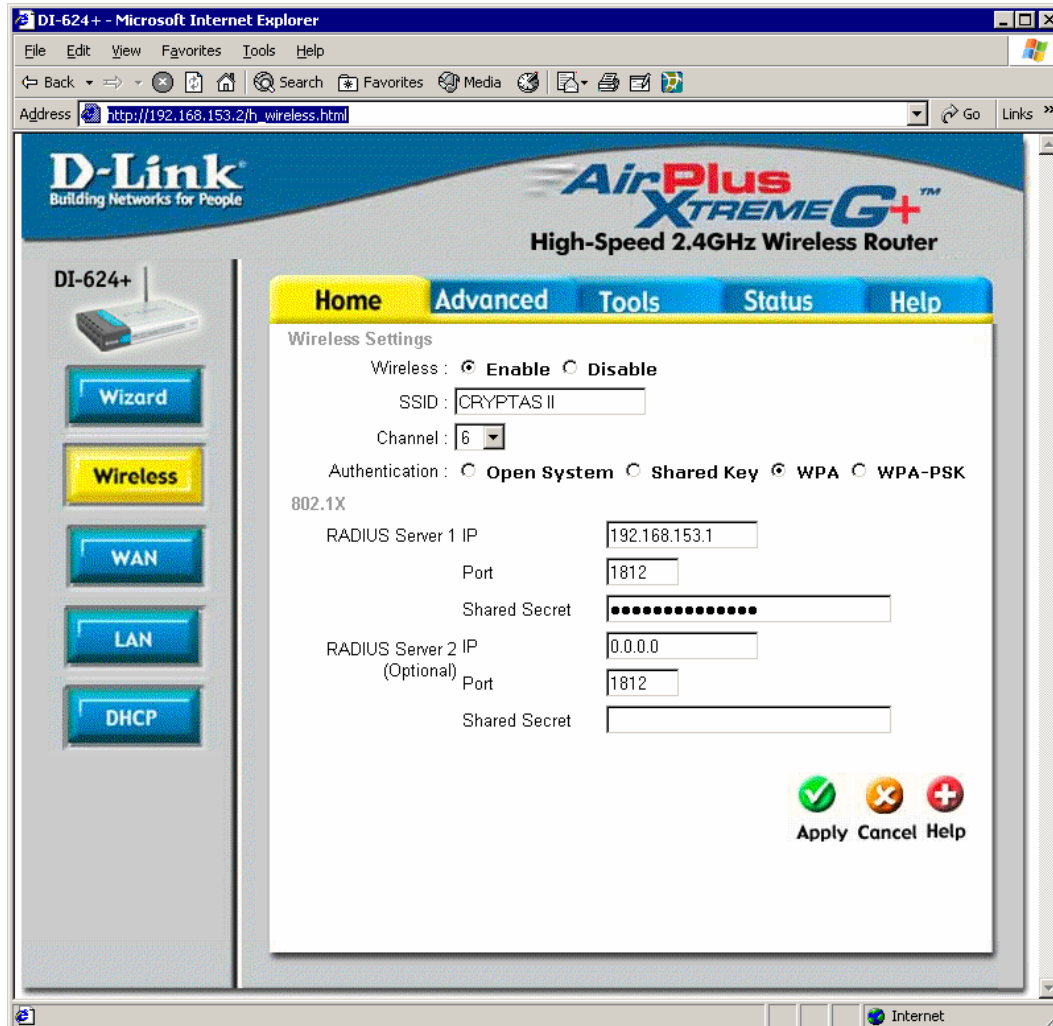
Hier müssen auch die zugelassenen RADIUS-Clients festgelegt werden, nur von den hier eingetragenen Stellen dürfen RADIUS-Anfragen gestellt werden. Mit New RADIUS-Client kann man den „friendly name“ und die IP/DNS eingeben. Das hier zu vergebende „shared secret“ ist ein Passwort, das auch später im WLAN-Access Point eingegeben werden muss.



## Einstellungen am Access Point

Diese funktionieren im Wesentlichen bei den unterschiedlichen Herstellern recht ähnlich. Wir haben einige Beispiele angeführt.

Hier die erforderliche Konfiguration an einem D-Link DI-624+ Router:



The screenshot displays the configuration interface for a D-Link DI-624+ router. The browser window shows the URL [http://192.168.153.2/h\\_wireless.html](http://192.168.153.2/h_wireless.html). The page title is "DI-624+ - Microsoft Internet Explorer". The main content area is titled "D-Link AirPlus Xtreme G+ High-Speed 2.4GHz Wireless Router". The navigation tabs are "Home", "Advanced", "Tools", "Status", and "Help". The "Wireless Settings" section includes the following fields:

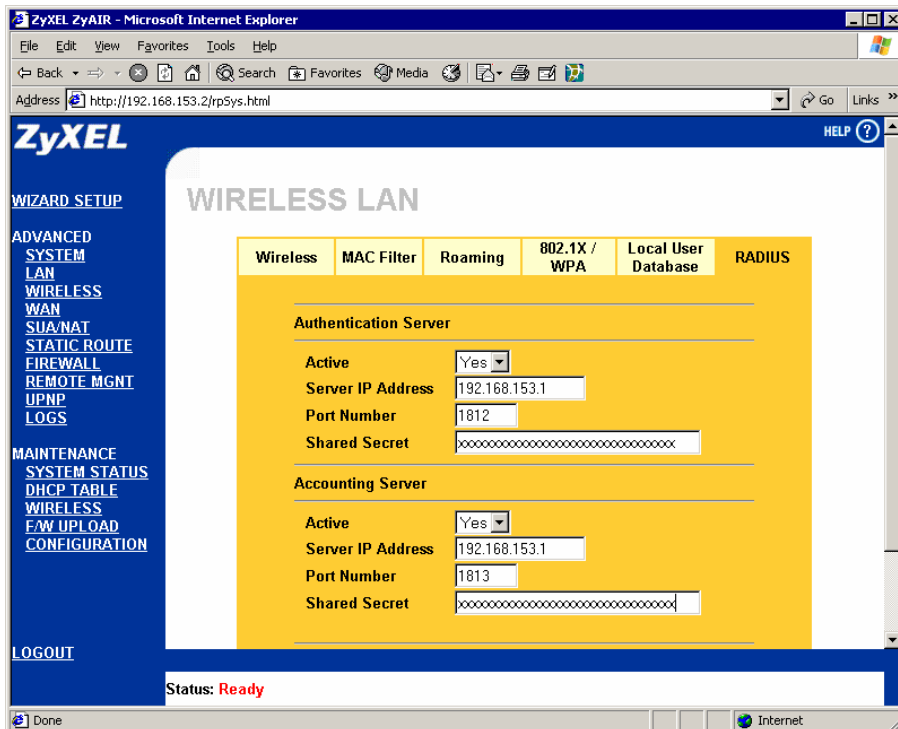
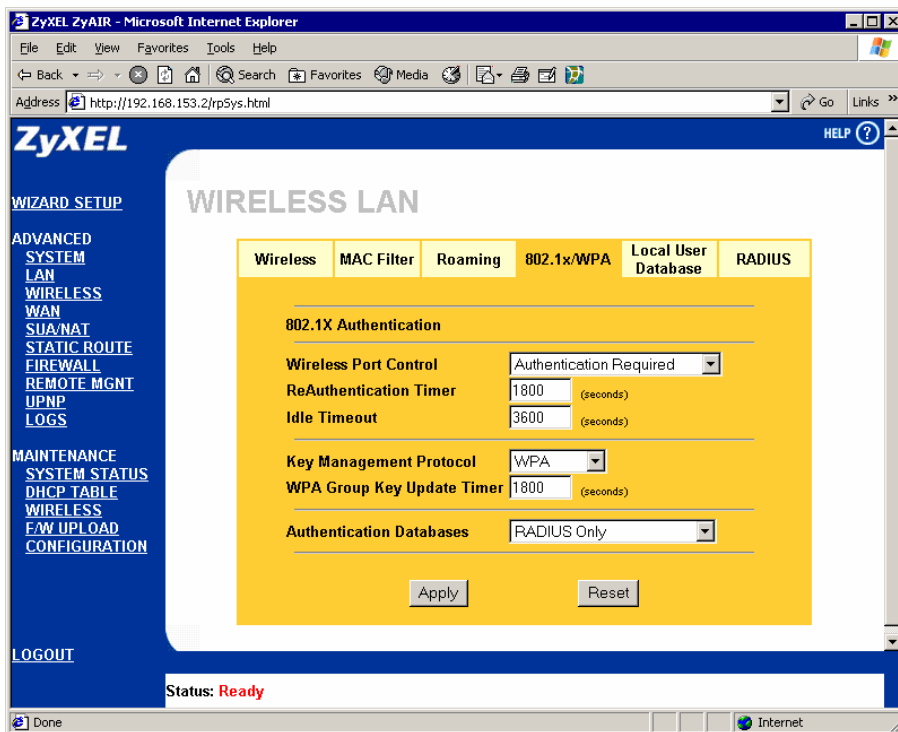
- Wireless:  Enable  Disable
- SSID:
- Channel:
- Authentication:  Open System  Shared Key  WPA  WPA-PSK

The "802.1X" section includes the following fields:

- RADIUS Server 1 IP:
- Port:
- Shared Secret:
- RADIUS Server 2 IP (Optional):
- Port:
- Shared Secret:

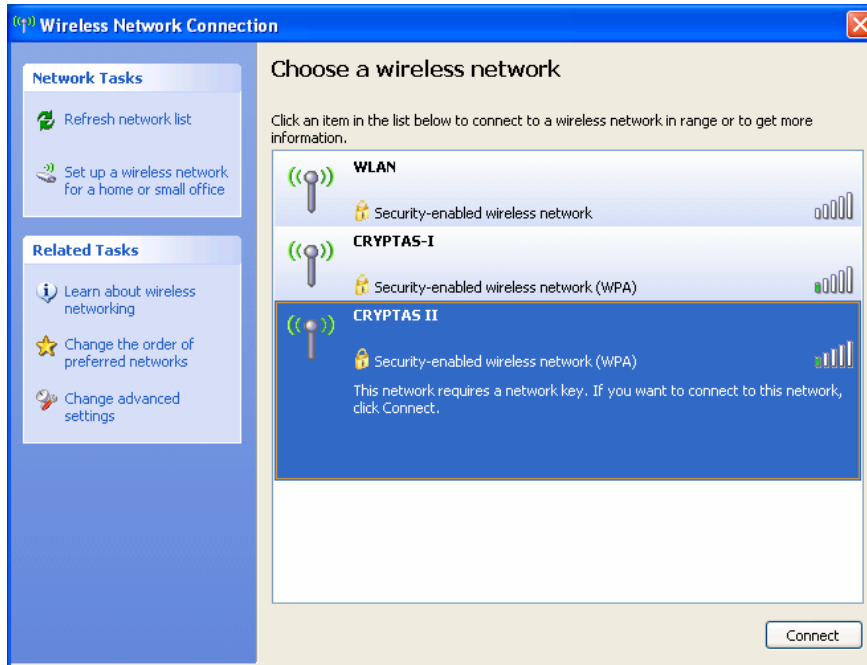
At the bottom right of the configuration area, there are three buttons: "Apply" (with a green checkmark icon), "Cancel" (with an orange X icon), and "Help" (with a red plus icon).

Hier die erforderliche Konfiguration an einem ZyXEL G-2000 Router:

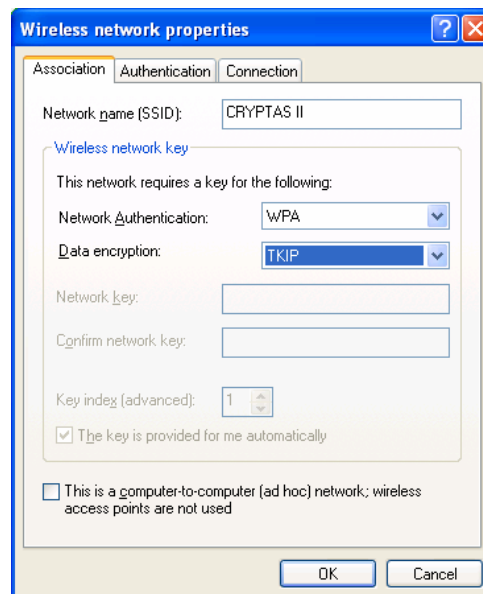
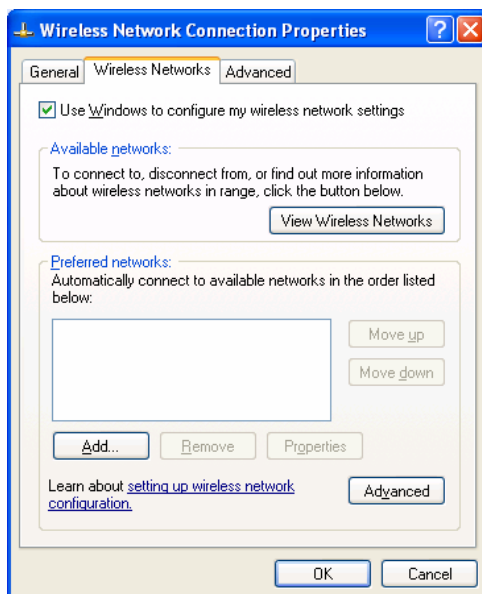


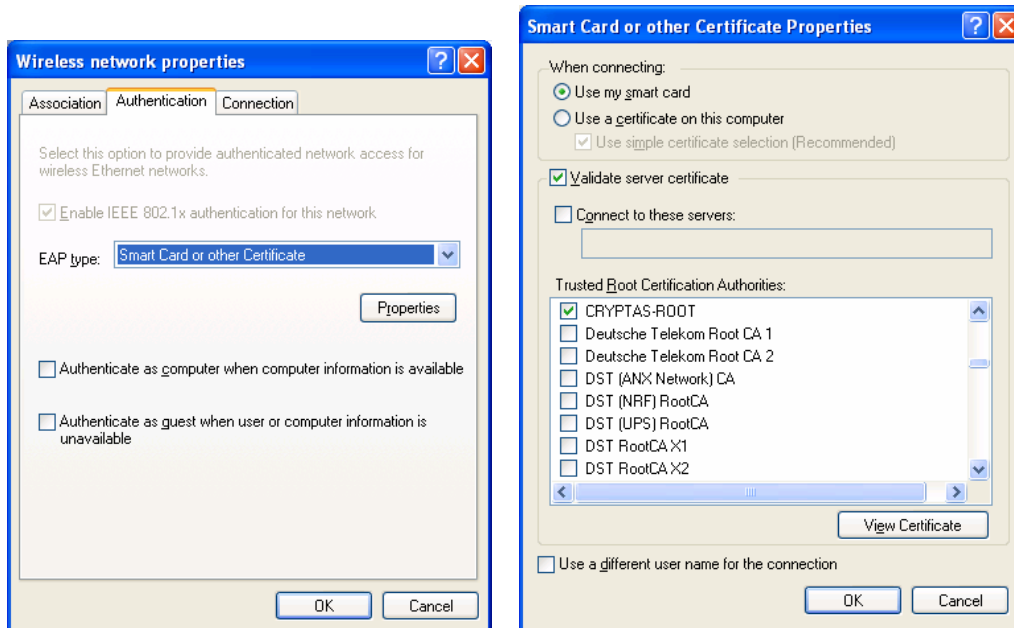
## Clientseitige Einstellungen

Mit Windows XP Service Pack 2 erscheint im Systray links unten das WLAN-Symbol mit einem roten Kreuz drinnen. Beim Doppelklick werden die verfügbaren Netzwerke angezeigt. Sowohl Cryptas I als auch Cryptas II ist über WPA-Verschlüsselung und Authentifizierung geschützt.



Mit „Change advanced settings“ links in den Related Tasks lassen sich die notwendigen Einstellungen vornehmen und mit „Add...“ danach das WLAN-AP-Namen (zB. „CRYPTPTAS II“) eintragen. In den dazu gehörenden Properties wird die Authentifizierung und die Art der Verschlüsselung festgelegt.





Beim Client wird eingestellt, dass es der AP nur WPA-Authentifizierung mit EAP akzeptiert (wir wollen uns im konkreten Fall jedoch mit der Smart Card anmelden).

Folgende Alternativen wären nach unserer Konfiguration am Server noch möglich:

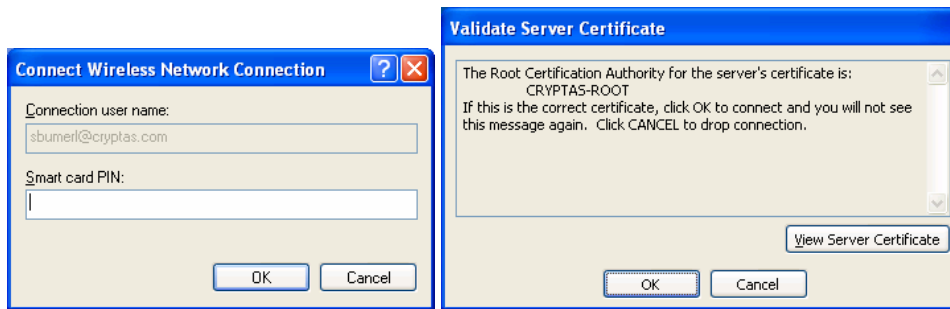
- „Protected EAP“: gesicherte Abfrage von UN/PWD, Abgleich ebenfalls über RADIUS
- „Smart Card or other Certificate“: Abfrage nach Zertifikat, welches entweder auf einer Smart Card abgelegt sein kann oder aus dem Certificate Store stammt

In den „Properties“ kann dann festgelegt werden, ob beim Verbinden im lokalen Certificate Store nach dem verlangten Zertifikat gesucht wird oder ob der Benutzer zum Einstecken einer Smart Card aufgefordert wird. Der Server bestätigt ebenfalls seine Authentizität dem Client gegenüber mittels Zertifikat. Dessen Überprüfung kann auf verpflichtend gesetzt werden und es kann eine Einschränkung der vertrauenswürdigen Wurzenzertifikate vorgenommen werden.

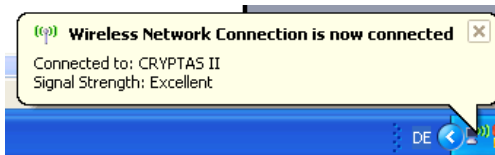


Wenn das WLAN-Netzwerk gefunden wird, erscheint im Systray eine diesbezügliche Verständigung und die Aufforderung, ein Zertifikat auszuwählen. Zu diesem Zweck muss man auf diese Notification klicken.

Daraufhin erscheint ein Dialog, der nach einer Smart Card mit entsprechendem Zertifikat verlangt. Wird diese – für die Karte muss natürlich die zugehörige Software (Crypto Service Provider) installiert sein – eingesteckt, so ist noch die Eingabe der persönlichen PIN erforderlich.



Wenn im Dialog „Smart Card or other Certificate Properties“ „Validate Server Certificate“ gesetzt wurde, so wird anschließend dieses (nur das erste Mal) zur Überprüfung angezeigt (das kann auch mit den Trusted Root CA Options vorab beim Einrichten verhindert werden). Nach der Bestätigung wird der Verbindungsaufbau abgeschlossen.



Der Verbindungsaufbau wurde erfolgreich abgeschlossen.

## Protokollierung

Nach erfolgreicher Authentifizierung sind folgende Informationen (wenn die diesbezügliche Protokollierung aktiviert ist) aus dem Event-Log am Server entnehmbar:

Event Type: Information  
Event Source: IAS  
Event Category: None  
Event ID: 1  
Date: 03.01.2005  
Time: 20:49:31  
User: N/A  
Computer: SERVER  
Description:  
User user@cryptas.com was granted access.  
Fully-Qualified-User-Name = dmz.cryptas.com/DMZ/Test/User  
NAS-IP-Address = 192.168.153.2  
NAS-Identifier = <not present>  
Client-Friendly-Name = D-Link-Router  
Client-IP-Address = 192.168.153.2  
Calling-Station-Identifier = <not present>  
NAS-Port-Type = Wireless - IEEE 802.11  
NAS-Port = <not present>  
Proxy-Policy-Name = Use Windows authentication for all users  
Authentication-Provider = Windows  
Authentication-Server = <undetermined>  
Policy-Name = Wireless access  
Authentication-Type = EAP  
EAP-Type = Smart Card or other certificate

CRYPTAS it-Security & Media Gmbh  
Modecenterstrasse 22/B2  
A-1030 Wien, Austria  
T +43 (1) 798 96 96 – 0  
F +43 (1) 798 96 96 – 99  
info@cryptas.com

[www.cryptoshop.com](http://www.cryptoshop.com)  
[www.cryptas.com](http://www.cryptas.com)  
[www.croptomedia.com](http://www.croptomedia.com)