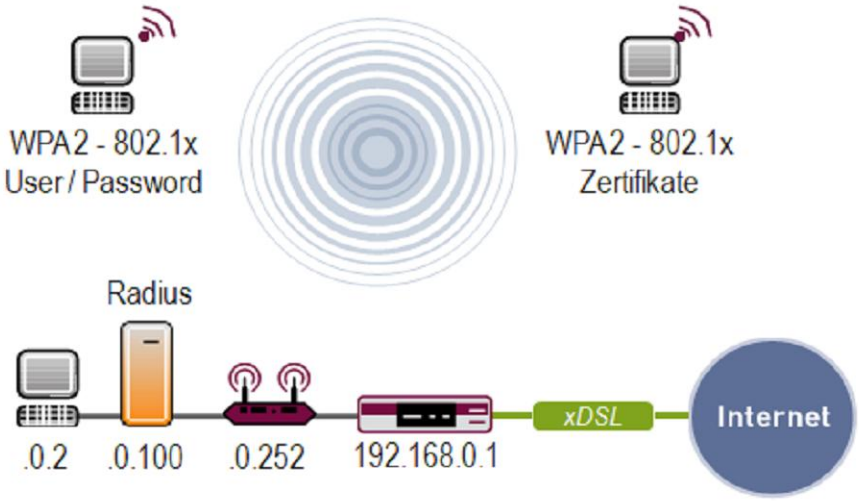
4. Access Point im Enterprise Mode (802.1x)



4.1 Einleitung

Im Folgenden wird die Konfiguration des Access Point Mode gezeigt. Zur Absicherung der Daten, Generierung der Schlüssel für die Verschlüsselung und zur Authentifizierung wird der Verschlüsselungsalgorithmus WPA2-Enterprise Mode mit AES verwendet. Die Benutzer-Authentifizierung wird dabei von einem RADIUS Server übernommen und kann sowohl mit Benutzernamen und Kennwort, als auch mit Zertifikaten erfolgen. Zudem zeigt die Konfiguration die Vergabe von IP-Adressen im Wireless LAN mittels DHCP.

Zur Konfiguration wird hierbei das Setup-Tool verwendet.

4.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein Bootimage ab Version 7.6.1.
- Grundkonfiguration des Gerätes.
- 1x Computer mit Wireless LAN Client.
- 1x Windows Server 2003 inkl. IAS
- Optional ein Zertifikatsserver

4.3 Konfiguration

Um den Access Point Mode zu aktivieren und die globalen Parameter zu konfigurieren, gehen Sie in folgendes Menü:

Setup Tool → WLAN

```
W2002 Setup Tool                    Funkwerk Enterprise Communications GmbH
[WLAN-1]: Configure WLAN Interface                                  w2002
-------------------------------------------------------------------------

          Operation Mode            Access Point >

          Location                  Germany

          Radio Band                2,4 GHz

          Channel                   auto

          VSS Configuration >


          Advanced >

                    SAVE                              CANCEL
-------------------------------------------------------------------------
```

Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Operation Mode	Bestimmen Sie den Wireless LAN Modus.
Location	Geben Sie den Standort des Gerätes an.
Radio Band	Wählen Sie die zu verwendende Frequenz aus.
Channel	Geben Sie den Kanal der Frequenz an.

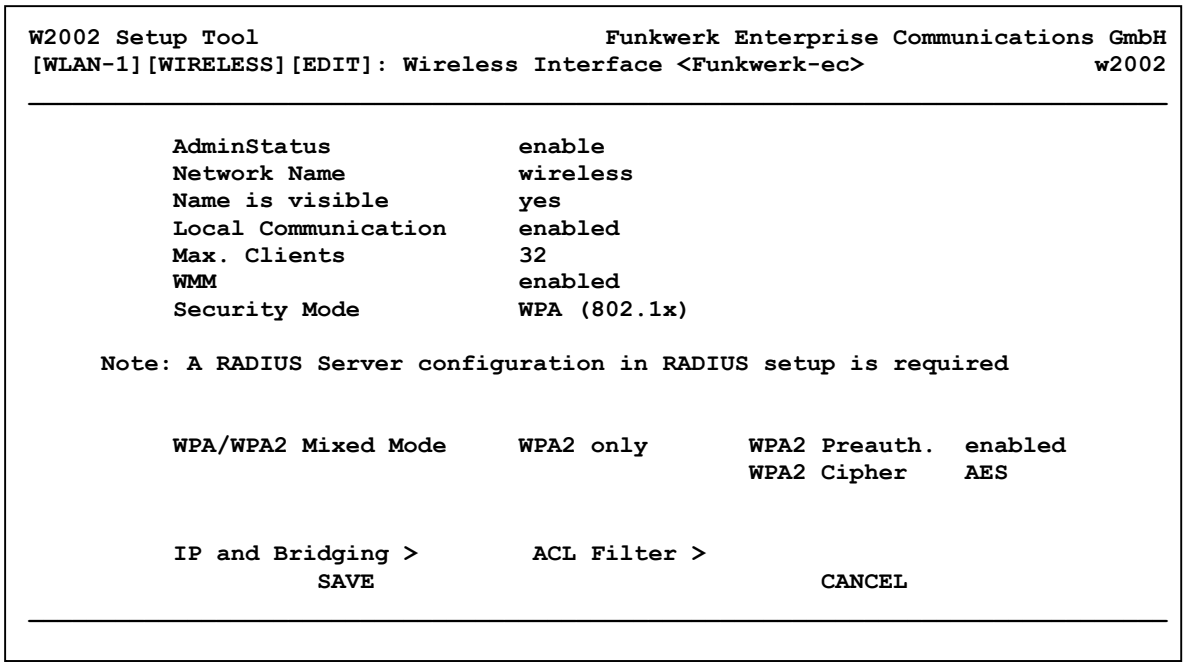
Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Setzen Sie den Operation Mode auf **Access Point**.
- Wählen Sie als Location **z.B. Germany**.
- Das Radio Band setzen Sie auf **z.B. 2,4 GHz**.
- Stellen Sie den Channel auf **z.B. auto**.

4.3.1 WPA2- Verschlüsselung (AES)

Das WPA2 Protokoll (802.11i) nutzt für die Verschlüsselung per default das Protokoll AES und ist somit noch sicherer als WPA-TKIP. Zur Konfiguration des Access Point Modus in Kombination mit der Verschlüsselung WPA2/AES/802.1x gehen Sie in folgendes Menü:

Setup Tool → WLAN → VSS Configuration → ADD / EDIT



Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
AdminStatus	Aktivieren oder deaktivieren Sie die SSID.
Network Name	Geben Sie den Namen des Netzwerks an.
Name is visible	Geben Sie an, ob das Netzwerk bei der Suche sichtbar ist.
Local Communication	Erlauben Sie die Kommunikation zwischen den WLAN Clients.
Security Mode	Dies ist der Algorithmus für die Authentifizierung.
WPA/WPA2 Mixed Mode	Entscheiden Sie zwischen WPA und WPA2 Algorithmus.
WPA2 Preauth.	Schalten Sie die WPA2 Vorauthentifizierung ein oder aus.
WPA2 Cipher	Bestimmen Sie das Protokoll zur Verschlüsselung.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Setzen Sie den AdminStatus auf **enable**.
- Wählen Sie als Network Name **z.B. wireless**.
- Setzen Sie Name ist visible auf **z.B. yes**.
- Die Local Communication stellen Sie auf **z.B. enabled**.
- Bei Security Mode wählen Sie **z.B. WPA (802.1x)**.
- Wählen Sie bei WPA/WPA2 Mixed Mode **z.B. WPA2 only**.
- Die WPA2 Preauth. setzen Sie auf **z.B. enabled**.
- Als WPA2 Cipher nutzen Sie **z.B. AES**.

INFO

Um zu verhindern, dass jeder auf Anhieb das WLAN Netzwerk sieht, können Sie die SSID Broadcasts abschalten. Das Abstellen der Broadcasts ist nur eine geringe Erhöhung der Sicherheit in Ihrem Netzwerk. Außerdem sollten Sie einen Netzwerknamen wählen, der nicht auf den Standort oder die Firma schließt.

INFO

Bei der WPA2 Preauthentication müssen sich die Clients beim Roaming nicht Komplett am neuen Access Point authentifizieren. Dies hat bei Radius Implementierung spürbare Geschwindigkeits Vorteile.

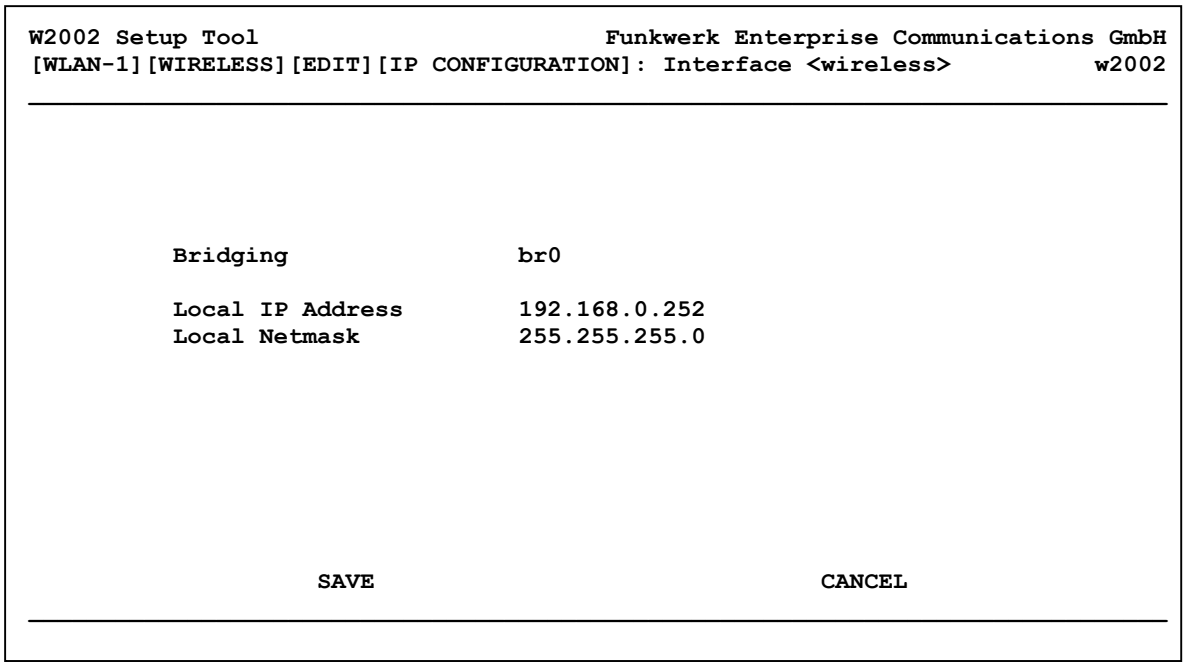
INFO

Damit Fehler beim Verbindungsaufbau bei einigen Wireless LAN Clients ausgeschlossen sind, sollten Sie die Protokolle **WPA** und **WPA2** als auch die Algorithmen **TKIP** und **AES** nicht kombinieren, sondern nur einzeln aktivieren.

4.3.2 Routing und Bridging

Für das Wireless LAN Interface müssen Sie Bridging aktivieren, sofern die WLAN Clients sich im gleichen Segment befinden sollen, wie die LAN Clients. Gehen Sie in folgendes Menü, um das Bridging zu aktivieren:

Setup Tool → WLAN → VSS Configuration → ADD / EDIT → IP and Bridging



Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Bridging	Wählen Sie eine Bridging Gruppe aus oder erstellen eine Neue.
Local IP Address	Tragen Sie die IP-Adresse vom Ethernet Interface ein.
Local Netmask	Tragen Sie die Subnetzmaske vom Ethernet Interface ein.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Setzen Sie Bridging auf **z.B. br0**.
- Wählen Sie als Local IP Address **z.B. 192.168.0.252**.
- Setzen Sie die Local Netmask auf **z.B. 255.255.255.0**.

INFO

Wenn Sie Bridging im Wireless LAN Interface aktiviert haben, müssen Sie im LAN Interface die gleiche Bridging Gruppe auswählen, damit die Kommunikation untereinander Möglich ist. Um Routing zu aktivieren, wählen Sie bei Bridging **no** aus und geben als IP-Adresse ein anderes IP-Subnetz für das Wireless Interface an.

4.3.3 Radius Konfiguration

Damit die WLAN Clients authentifiziert werden, müssen Sie einen Radius Server aus dem LAN angeben. Gehen Sie für die Konfiguration in folgendes Menü:

Setup → IP → Remote Authentication → RADIUS Authentication and Accounting → ADD

```
W2002 Setup Tool                          Funkwerk Enterprise Communications GmbH
[IP][RADIUS][ADD]                                                          w2002

  Protocol                    802.1x

  IP Address                  192.168.0.100
  Password                    secret

  Priority                    0
  Policy                      authoritative

  Port                        1812
  Timeout (ms)                1000
  Retries                     1
  State                       active
  Validate                    enabled
  Dialout                     disabled
  Alive Check (if inactive)   enabled

                    SAVE                                  CANCEL
```

Folgende Punkte sind hier relevant:

Feld	Bedeutung
Protocol	Das zu verwendende Radius Protocol.
IP Address	Die IP-Adresse vom Radius Server im LAN.
Password	Tragen Sie das Passwort für den Radius Server ein.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Setzen Sie Protocol auf **z.B. 802.1x**.
- Verwenden Sie als IP Address **z.B. 192.168.0.100**.
- Setzen Sie das Password auf **z.B. secret**.

4.3.4 DHCP Server Konfiguration

Wenn Sie den Clients im Netzwerk eine IP-Adresse per DHCP vergeben möchten, müssen Sie in dem Router den DHCP Server konfigurieren. Gehen Sie dazu in folgendes Menü, um einen neuen Eintrag zu erzeugen.

Setup Tool → IP → IP Address Pools → Pools → ADD

```
W2002 Setup Tool                          Funkwerk Enterprise Communications GmbH
[IP][DYNAMIC][POOL][ADD]: Define Range of IP Addresses                      w2002
------------------------------------------------------------------------------


     Identifier                                0
     Description                               LAN
     IP Address                                192.168.0.10
     Number of Consecutive Addresses           10
     Primary Domain Name Server                0.0.0.0
     Secondary Domain Name Server              0.0.0.0




                    SAVE                                   CANCEL
------------------------------------------------------------------------------
```

Folgende Punkte sind hier relevant:

Feld	Bedeutung
Identifier	Die Identifikationsnummer vom Pool.
Description	Eine Beschreibung für den Pool.
IP Address	Geben Sie hier die erste IP-Adresse an aus dem Pool an.
Number of Consecutive Addresses	Bestimmen Sie hier die Größe des IP-Adressen Pools.

Gehen Sie folgendermaßen vor, um den DHCP Server zu konfigurieren:

- Als Identifier verwenden Sie **z.B. 0**.
- Bei Description tragen Sie **z.B. LAN** ein.
- Unter IP Address tragen Sie **z.B. 192.168.0.10** ein.
- Das Feld Number of Consecutive Addresses setzen Sie auf **z.B. 10**.

Gehen Sie für die IP-Pool Zuweisung auf ein Interface in folgendes Menü:

Setup Tool → IP → IP Address Pools → DHCP → ADD

```
W2002 Setup Tool                          Funkwerk Enterprise Communications GmbH
[IP][DYNAMIC][DHCP][ADD]: Define DHCP Pool Usage                          w2002
-------------------------------------------------------------------------------


     Interface                                 br0
     Pool                                      LAN
     Assignment Mode                           local
     Lease Time (minutes, 0=disabled)          120
     Gateway                                   0.0.0.0
     First TFTP Server                         0.0.0.0
     Second TFTP Server                        0.0.0.0
     Radius Accounting                         disabled
     Radius Group Id                           0
     Alive Check                               disabled
     Alive Test Period (seconds, 0=disabled)   0
     Admin State                               enabled

                    SAVE                                CANCEL
```

Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Interface	Das Interface, wo der DHCP Server aktiv ist.
Pool	Beschreibung von dem angelegten Pool.
Admin State	Aktiviert oder deaktiviert den Pool.

Gehen Sie folgendermaßen vor, um den DHCP Server zu konfigurieren:

- Als Interface verwenden Sie **z.B. br0**.
- Bei Pool wählen Sie **z.B. LAN** aus.
- Den Admin State setzen Sie auf **z.B. enabled**.

4.4 Konfiguration des Windows Server 2003

Unter Windows Server 2003 sollten Sie folgende Änderungen machen, um die Dienste Active Directory, Internet Authentication Server und Zertifikatsserver zu nutzen:

- Installieren Sie Active Directory Service (Domäne **z.B. neo-one.de**).
- Installieren Sie den Internet Information Service (Für Zertifikate).
- Installieren Sie eine Organisations-Zertifizierungsstelle.
- Installieren Sie den Internet Authentication Server.
- Erstellen Sie im AD einen User **z.B. user/pass** und geben Sie ihm Einwahlrechte.
- Erstellen Sie im Radius einen Client mit der IP-Adresse vom Access Point und dem Passwort **z.B. password**.
- Erstellen Sie im RADIUS eine RAS Richtlinie mit dem Assistenten:
  - Richtlinienname: **Wireless**.
  - Zugriffsmethode: **Drahtlos**.
  - Zugriff gewähren für: **Benutzer**.
  - EAP-Typ: **PEAP**.
- Bearbeiten Sie die Richtlinie und erteilen Sie die RAS Berechtigung.
- Öffnen Sie das Menü: Profil bearbeiten → Authentifizierung → EAP-Methoden → Hinzufügen und fügen Sie **Smartcard oder anderes Zertifikat** hinzu.

4.5 Wireless LAN Client Konfiguration

Wählen Sie einen dieser Konfigurationspunkte, für eine bestimmte WLAN Authentifizierung:

- **4.5.1 Authentifizierung mit PEAP (Name / Passwort)**
- **4.5.2 Authentifizierung mit Zertifikat**

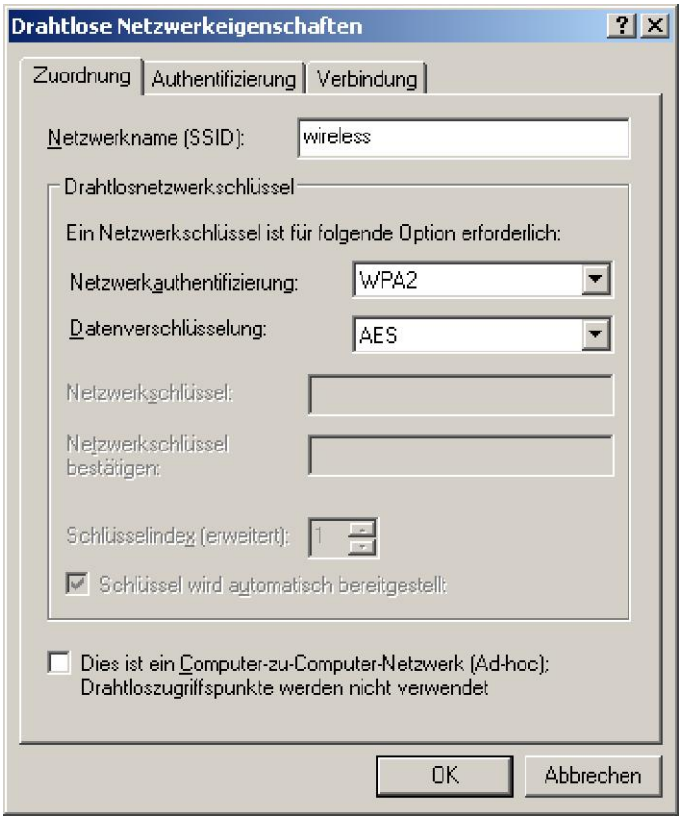
INFO

Wenn bei der Client Konfiguration die Registerkarte **Authentifizierung** in der Wireless Verbindung nicht angezeigt wird, müssen Sie folgende Dienste je nach Betriebssystem starten: **Automatische Konfiguration** und **Konfigurationsfreie drahtlose Verbindung**

4.5.1 Authentifizierung mit PEAP (Name / Passwort)

Für die Konfiguration des Wireless LAN Client, gehen Sie unter Windows in folgendes Menü:

Start → Einstellungen → Netzwerkverbindungen → Drahtlose Netzwerkverbindung → Erweiterte Einstellungen ändern → Drahtlosnetzwerke → Hinzufügen



Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Netzwerkname (SSID)	Der Wireless LAN Netzwerkname.
Netzwerkauthentifizierung	Wählen Sie das Authentifizierungs-Protokoll aus.
Datenverschlüsselung	Bestimmen Sie das Verschlüsselungsprotokoll.

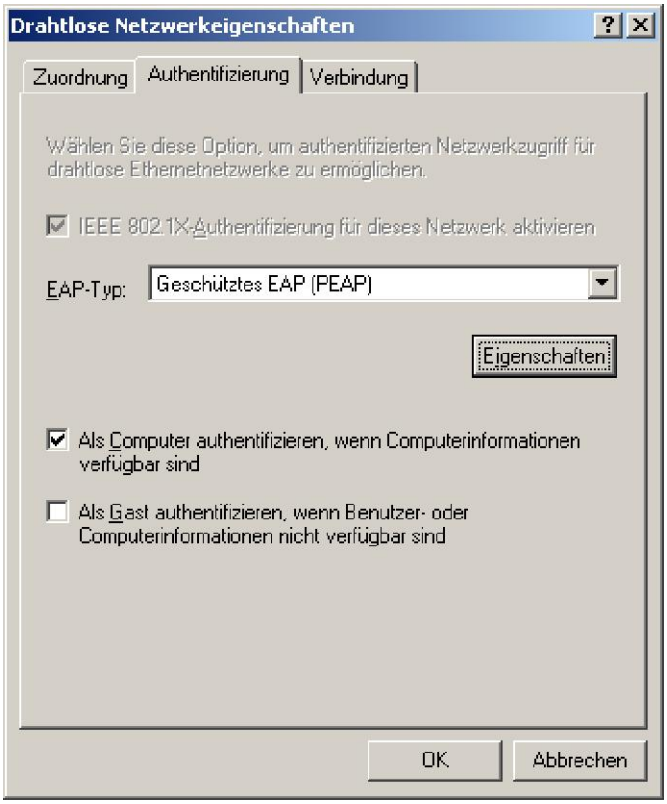
Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Bei Netzwerkname (SSID) tragen Sie **z.B. wireless** ein.
- Unter Netzwerkauthentifizierung wählen Sie: **WPA2** aus.

- Die Datenverschlüsselung setzen Sie auf: **AES**.
- Klicken Sie auf die Registerkarte: **Authentifizierung**.

INFO

Die Authentifizierung bei PEAP ist in der Regel einseitig, so dass der Client sich nur gegenüber dem Server authentifizieren muss.

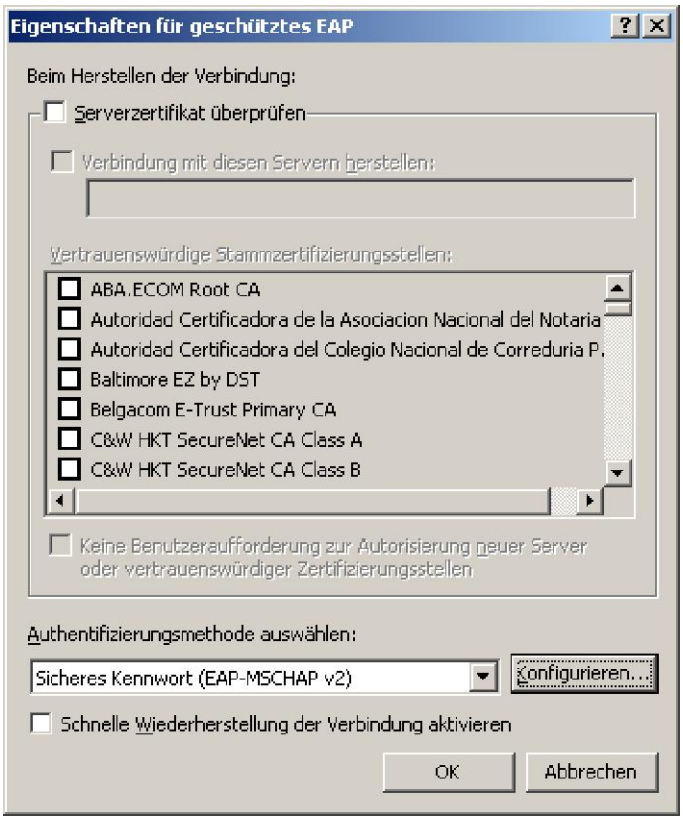


Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
EAP-Typ	Geben Sie die Art der Authentifizierung an (Passwort /Zertifikate).

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Bei EAP-Typ wählen Sie: **Geschütztes EAP (PEAP)**.
- Gehen Sie in das Untermenü: **Eigenschaften**.



Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Serverzertifikat überprüfen	Überprüfen Sie die Identität des Remoteservers.
Authentifizierungsmethode auswählen	Wählen Sie eine Authentifizierungsmethode aus.
Konfigurieren	Weitere Optionen für die Authentifizierung.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Den Haken bei Serverzertifikat überprüfen: **deaktivieren**.
- Bei Authentifizierungsmethode auswählen stellen Sie: **Sicheres Kennwort** ein.
- Im Untermenü Konfigurieren den Haken: **deaktivieren**.
- Bestätigen Sie Ihre Eingaben mit **OK**.

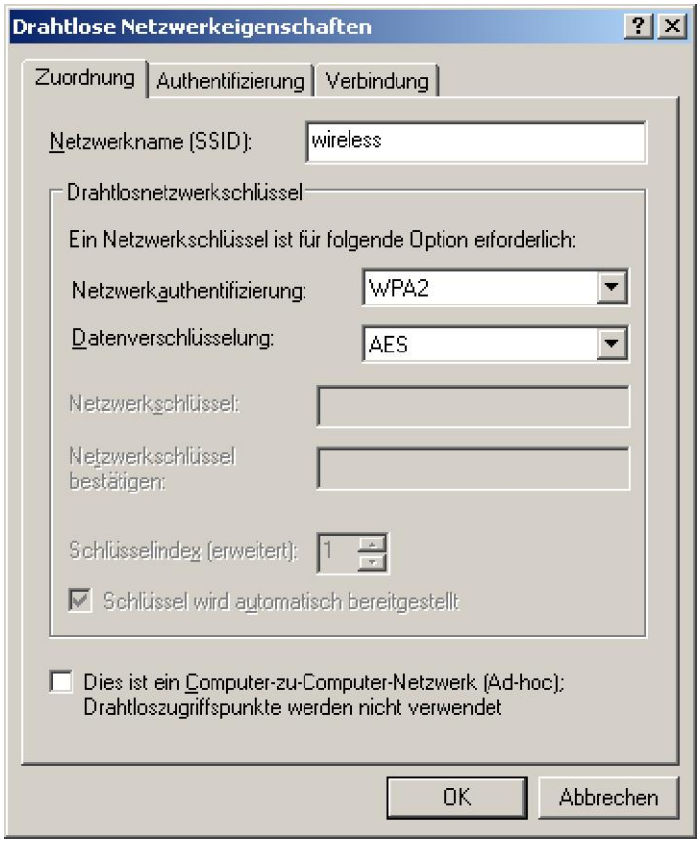
Beim Verbindungsaufbau erscheint ein Login, wo Sie folgende Daten verwenden:

- Benutzer: **user** / Passwort: **pass** / Domäne: **neo-one**

4.5.2 Authentifizierung mit Zertifikat

Nach dem Anfordern und Installieren eines Benutzerzertifikats über die Webdienste von Windows Server 2003 verfügen Sie über ein eigenes Zertifikat und das der Zertifizierungsstelle. PKCS#12 Zertifikate beinhalten alle wichtigen Daten: Eigenes Zertifikat, Privater Schlüssel und CA Zertifikat. Für die Konfiguration der Wireless LAN Verbindung im Client, gehen Sie unter Windows in folgendes Menü:

Start → Einstellungen → Netzwerkverbindungen → Drahtlose Netzwerkverbindung → Erweiterte Einstellungen ändern → Drahtlosnetzwerke → Hinzufügen

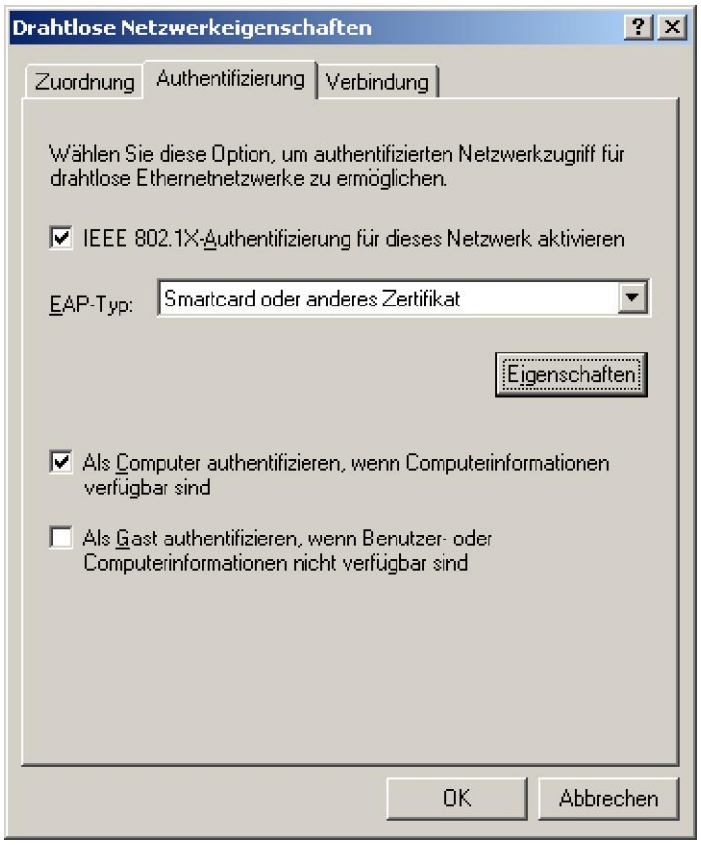


Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Netzwerkname (SSID)	Der Wireless LAN Netzwerkname.
Netzwerkauthentifizierung	Wählen Sie das Authentifizierungs-Protokoll aus.
Datenverschlüsselung	Bestimmen Sie das Verschlüsselungsprotokoll.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Bei Netzwerkname (SSID) tragen Sie **z.B. wireless** ein.
- Unter Netzwerkauthentifizierung wählen Sie: **WPA2** aus.
- Die Datenverschlüsselung setzen Sie auf: **AES**.
- Klicken Sie auf die Registerkarte: **Authentifizierung**.

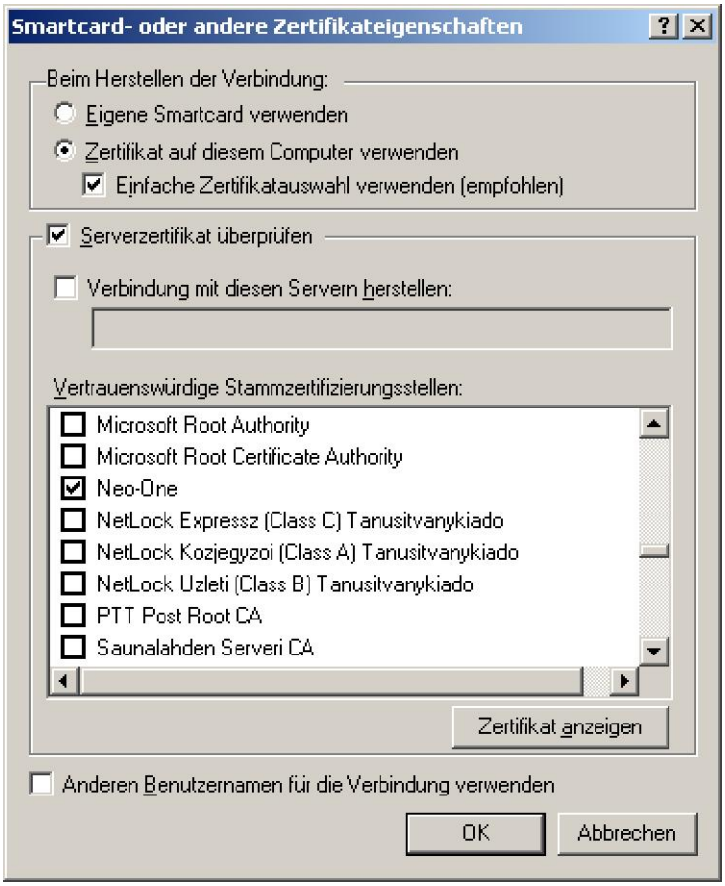


Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
EAP-Typ	Geben Sie die Art der Authentifizierung an (Passwort /Zertifikate).

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Bei EAP-Typ wählen Sie: **Smartcard oder anderes Zertifikat**.
- Gehen Sie in das Untermenü: **Eigenschaften**.



Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Serverzertifikat überprüfen	Überprüfen Sie die Identität des Remoteservers.
Vertrauenswürdige Stamm-zertifizierungsstellen	Wählen Sie eine vertrauenswürdige Stammzertifizierungsstelle aus.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Den Haken bei Serverzertifikat überprüfen: **aktivieren**.
- Wählen Sie bei Vertrauenswürdige Stammzertifizierungsstellen: **z.B. Neo-One** aus.
- Bestätigen Sie Ihre Eingaben mit **OK**.

Beim Verbindungsaufbau wird das eigene Zertifikat automatisch übermittelt und die Remoteidentität mit Hilfe des CA-Zertifikats überprüft.