



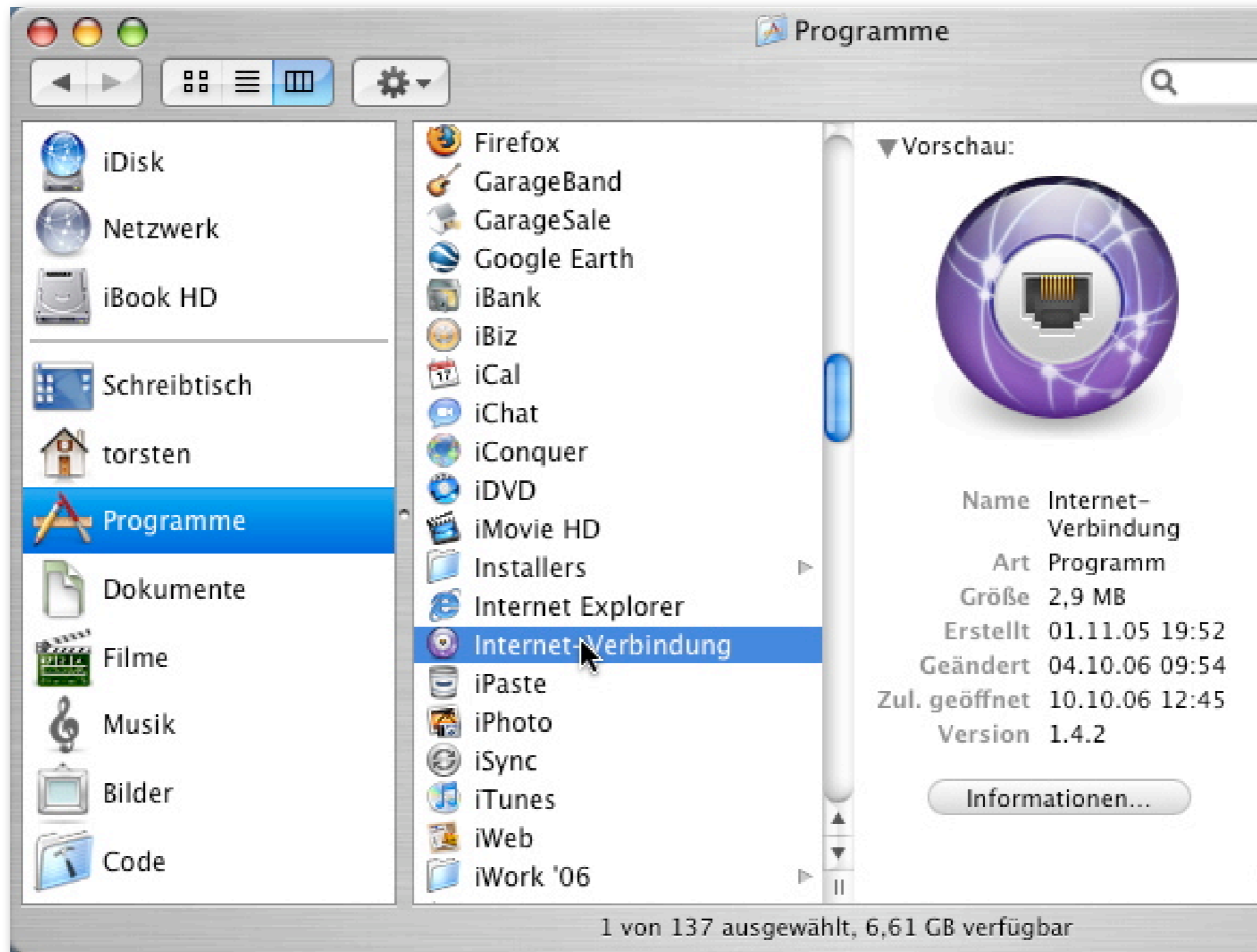
DFNRoaming/Eduroam Clients

Torsten Kersting
kersting@dfn.de

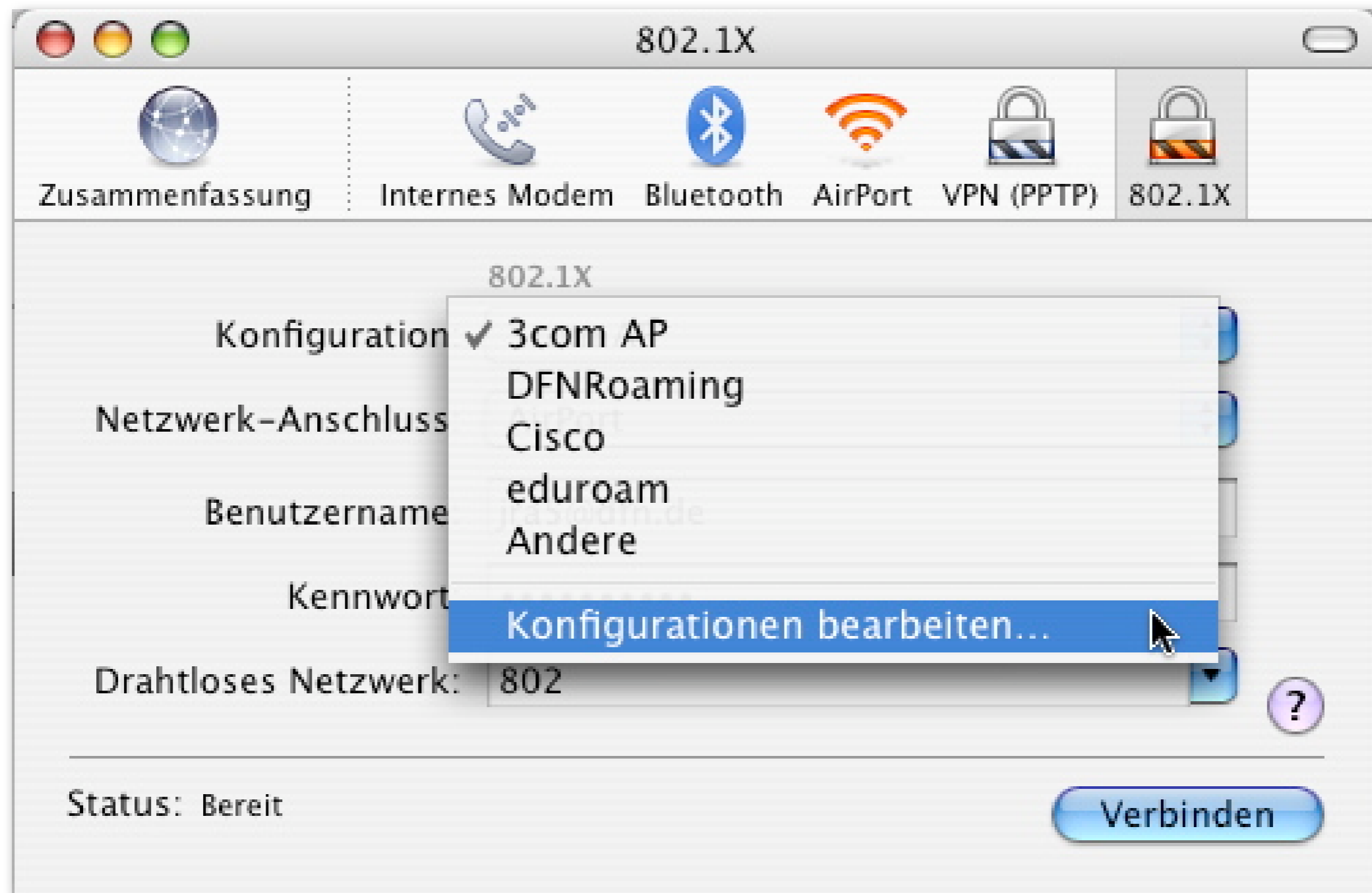
- Mac OSX Supplicant
- wpa_supplicant
- SecureW2

- Standard 802.1X Client
- keine Änderungen nötig
- sehr einfache Konfiguration
- komfortable GUI

Mac OS X Supplicant



Mac OSX Supplicant



Mac OSX Supplicant

The screenshot shows the Mac OSX Supplicant configuration window for the 'eduroam' network. The window is divided into several sections:

- Left Panel:** A list of configurations: 'Konfiguration', '3com AP', 'DFNRoaming', 'Cisco', and 'eduroam' (highlighted).
- Description:** 'Beschreibung: eduroam'
- Network Connection:** 'Netzwerk-Anschluss: AirPort' (dropdown menu)
- Username:** 'Benutzername: kersting@dfn.de'
- Password:** 'Kennwort:
- Wireless Network:** 'Drahtloses Netzwerk: eduroam' (dropdown menu)
- Authentication:** 'Identifizierung:' section with a table of protocols:

Ein	Protokoll
<input checked="" type="checkbox"/>	TTLS
<input type="checkbox"/>	TLS
<input type="checkbox"/>	EAP-FAST
<input type="checkbox"/>	LEAP
<input type="checkbox"/>	PEAP
- Buttons:** 'Konfigurieren...', 'Abbrechen', and 'OK'.
- Footer:** '+ -' zoom controls.

Wählen Sie die unterstützten Identifizierungsprotokolle oben aus und ordnen Sie sie in der gewünschten Reihenfolge an.

Mac OSX Supplicant

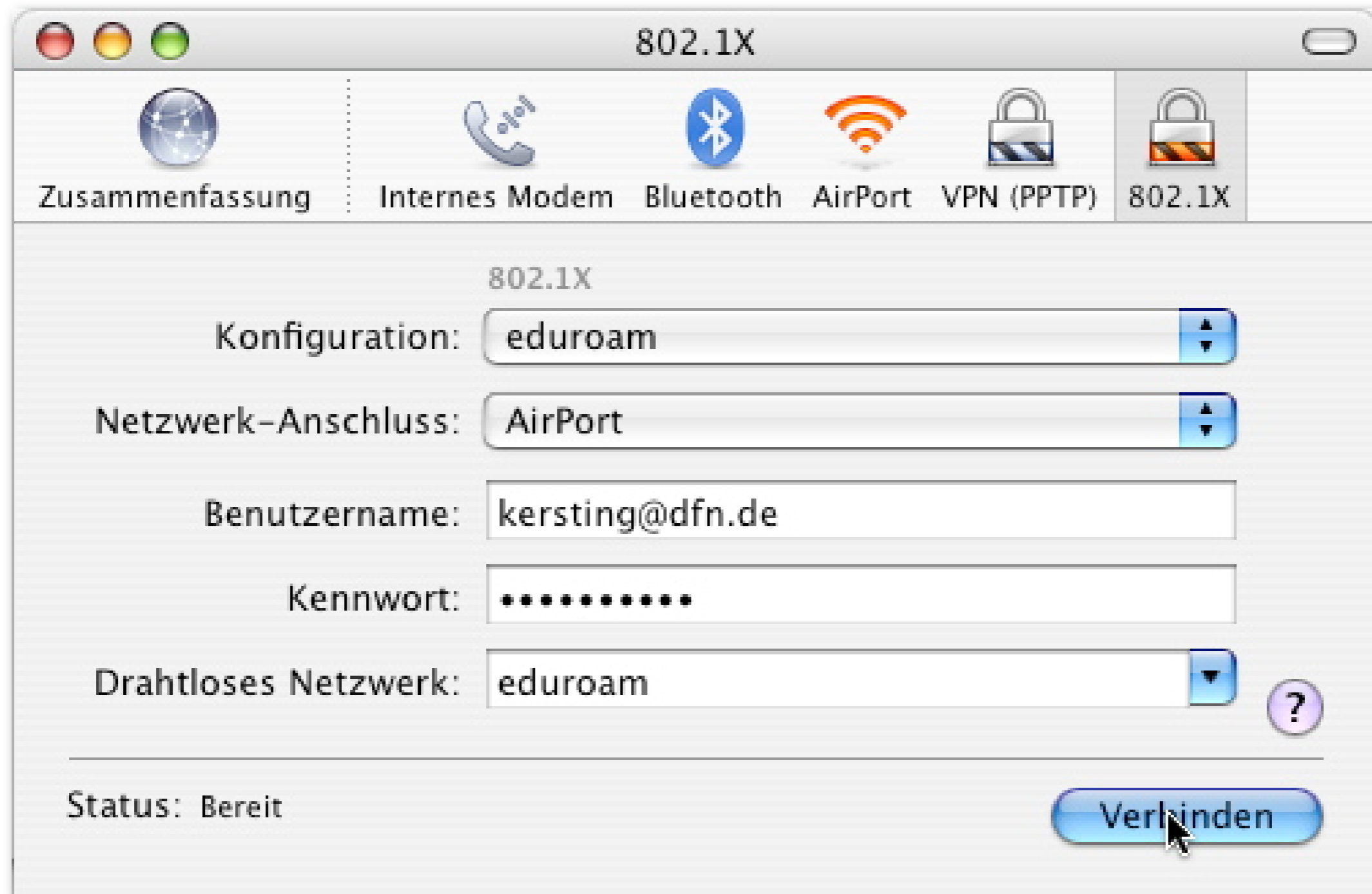
TTLS

Geben Sie Ihre TTLS-Identifizierung unten ein. Nach außen erfolgt keine Verschlüsselung.

Internes TTLS-Identifizierungsverfahren:

Externe Identität: (Optional)

Mac OSX Supplicant



- Open Source 802.1X Client
- Linux, BSD, MS Windows
- Desktops/Laptops, Embedded Systems
- http://hostap.epitest.fi/wpa_supplicant

- WPA-PSK
- WPA mit EAP
- CCMP, TKIP, WEP104, WEP40
- WPA und IEEE 802.11i/RSN/
WPA2
- RSN: PMKSA caching, preauth

- EAP-TLS
- EAP-PEAP
- EAP-TTLS
- EAP-SIM
- EAP-AKA

- Prism2/2.5/3
- Agere Systems (Hermes)
- madwifi (Atheros arc521x)
- Broadcom wl.o Treiber
- Intel ipw2100 ipw2200

- Daemon Programm
- Verschiedene Frontends
- Kostenlos + Kommerziell
- Flexible Build Konfiguration

- Anfrage an Kernel Treiber BSS scannen
- Auswahl passenden BSS
- Anfrage an Kernel zu assoziieren
- WPA-EAP: Integrierter 802.1X Client

- 4 Wege Handshake mit AP
- Verschlüsselungskeys konfigurieren
- Normale Pakete

WPA_Supplicant

```
ctrl_interface=/var/run/wpa_supplicant
```

```
network{
```

```
    ssid="eduroam"
```

```
    key_mgmt=WPA-EAP
```

```
    anonymous_identity="anonymous@dfn.de"
```

```
    ca_cert="/etc/eduroam/ca.cer
```

```
    identity="kersting@dfn.de"
```

```
    eap=TTLS
```

```
    password="geheim"
```

```
    phase2="auth=PAP"
```

```
}
```

WPA_SupPLICANT

```
network{  
    ssid="eduroam"  
    key_mgmt=IEEE8021X  
    anonymous_identity="anonymous@dfn.de"  
    ca_cert="/etc/eduroam/ca.cer"  
    identity="kersting@dfn.de"  
    eap=TTLS  
    password="geheim"  
    phase2="auth=PAP"  
}
```

- Skript von Tomasz Wolniewicz
- ca.crt + Credentials eintragen
- eduroam-start eduroam-stop
- wpa_supplicant -Dwext -iwlan0
-c /etc/eduroam/wpa_supplicant.conf

- Windows ohne EAP-TTLS
- Open Source EAP-TTLS Client
- Nutzt MS 802.1X Client
- Vorkonfigurierte .exe

- SecureW2.INF File vorbereiten
- NSIS Config File erstellen
- .exe mit NSIS erstellen
- .exe digital signieren

- .exe herunterladen
- Signatur bestätigen
- starten und Cred. eingeben
- Reboot
- SecureW2 auswählen

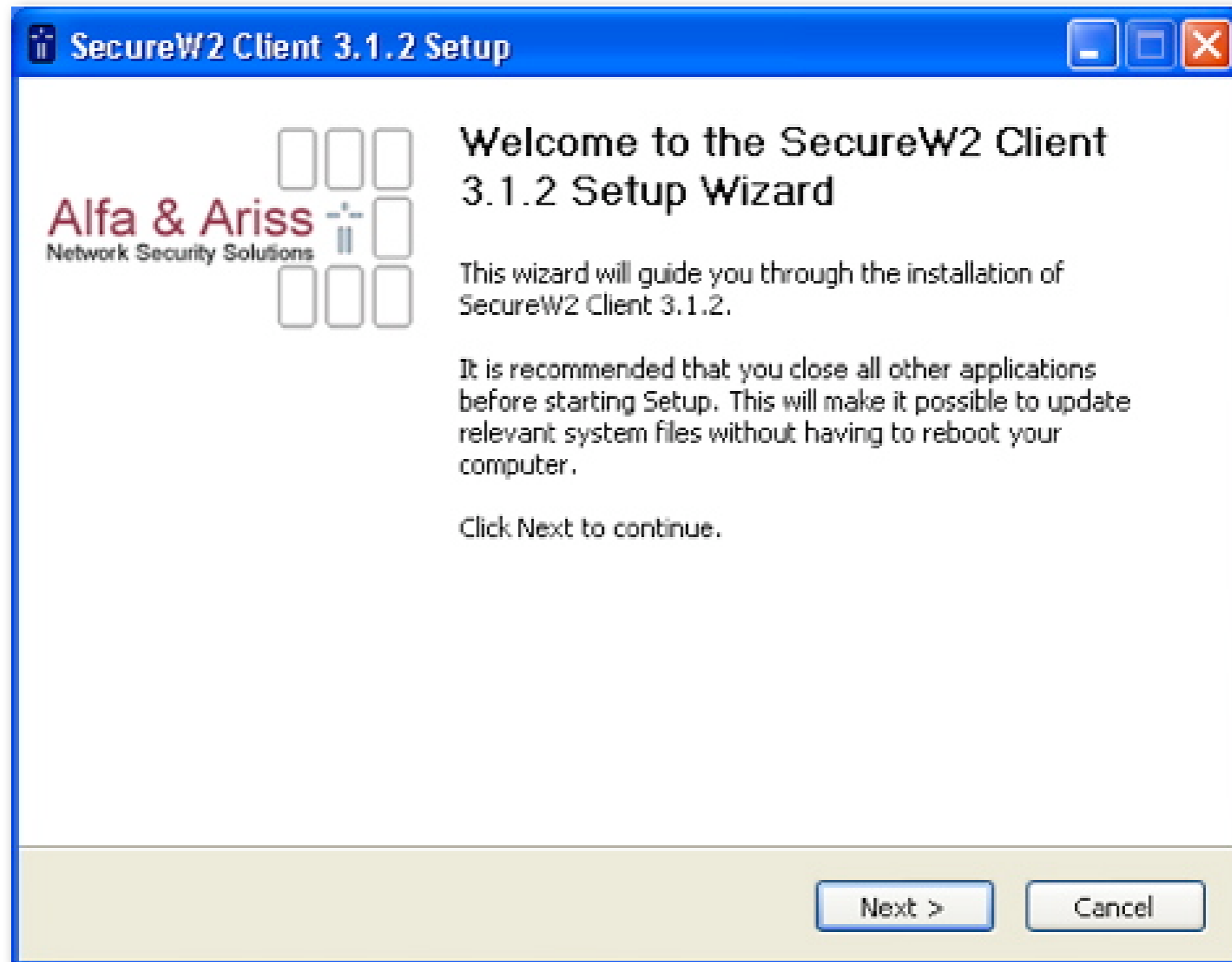
- Nullsoft Scriptable Install System
- .NET Framework SDK von MS
- Schlüssel zum signieren

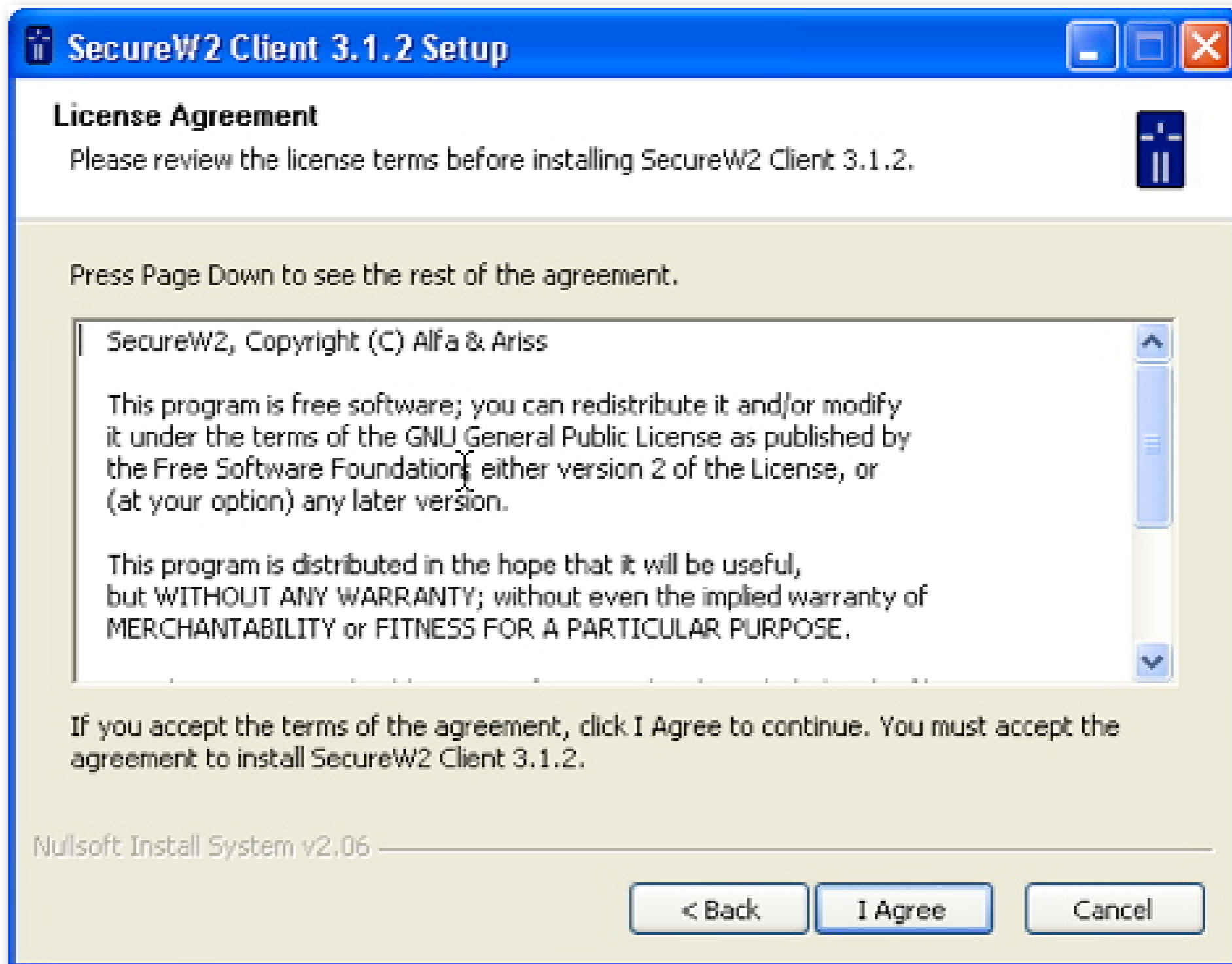
```
Signature = "$Windows NT$"  
Provider = "Alfa & Ariss"  
Config = 7  
  
[Certificates]  
Certificate.1 = your_ca_cert.der  
  
[WZCSVC]  
Enable = AUTO  
  
[SSID.1]  
Name = "eduroam"  
Profile = "DEFAULT"  
[Profile.1]  
AuthenticationMethod = PAP  
EAPType = 0  
Name = "DEFAULT"  
Description = "Enter your login credentials:"  
UseAlternateIdentity = FALSE  
VerifyServerCertificate = TRUE  
PromptUserForCredentials = FALSE  
TrustedRootCA.0 = your_ca_cert_fingerprint  
UserName = PROMPTUSER
```

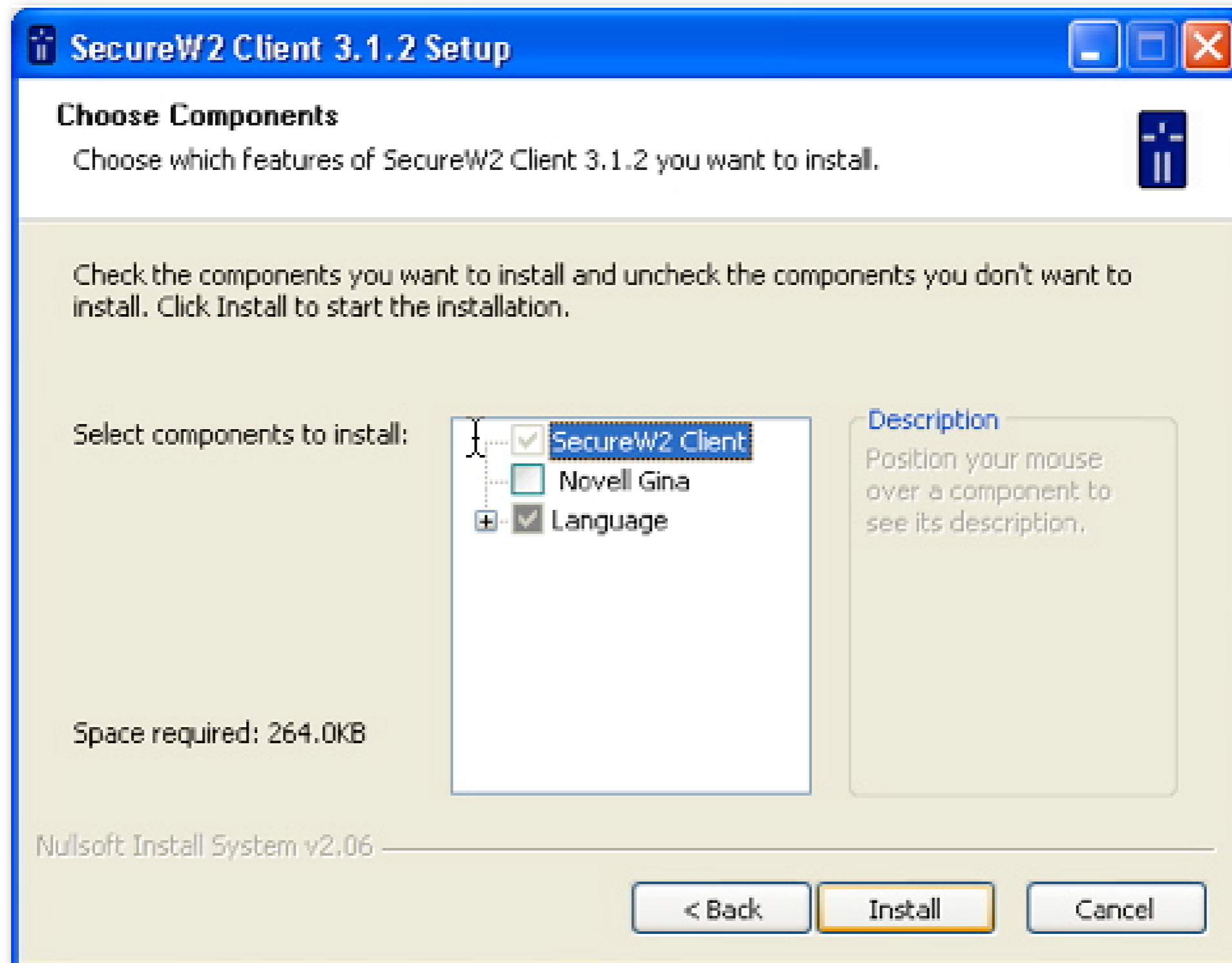
```
;-----
!define APPLICATION "SecureW2 installer"
!define VERSION "1.0.0"
;-----
    !include "MUI.nsh"
;General
;Name and file
    Name "${APPLICATION} ${VERSION}"
    OutFile "SecureW2_312_Test.exe"
;-----
;Interface Settings
    !define MUI_ICON "your_icon.ico"
    !define MUI_UNICON your_icon.ico
    !define MUI_ABORTWARNING
Section "${APPLICATION}" SecInstall
SectionIn RO
; Extract all file to the temp dir
    SetOutPath $TEMPDIR
; Define all the files required for the installation here:
    File "SecureW2_312.exe"
    File "SecureW2.INF"
    File "your_ca_cert.der"
    ExecWait "SecureW2_312.exe"
; If an error occurs then goto Error label else goto Continue label
    IfErrors Error
    Goto Continue
; Error Label, show error box and then quit
Error:
MessageBox MB_OK|MB_ICONEXCLAMATION "SecureW2 installation problem, please report to ..."
; Continue Label
Continue:
; Remove temporary files
    Delete "$TEMPDIR\SecureW2_312.exe"
    Delete "$TEMPDIR\SecureW2.INF"
    Delete "$TEMPDIR\your_ca_cert.der"
    Quit
SectionEnd
```

- SecureW2.INF Datei
- Konfig Datei SecureW2.NSI
- Original SecureW2.exe
- Icon Datei icon.ico
- Zertifikat

- rechts-klick auf SecureW2.NSI
- „Compile NSI Script“ wählen
- .exe signieren
 - `C:\Program Files\Microsoft.NET\SDK\v2.0\Bin\signtool sign /a your_installer.exe`
 - `C:\Program Files\Microsoft.NET\SDK\v2.0\Bin\signtool signwizard`







SecureW2 - PreConfigure

Alfa & Ariss
Network Security Solutions

Enter your login credentials:

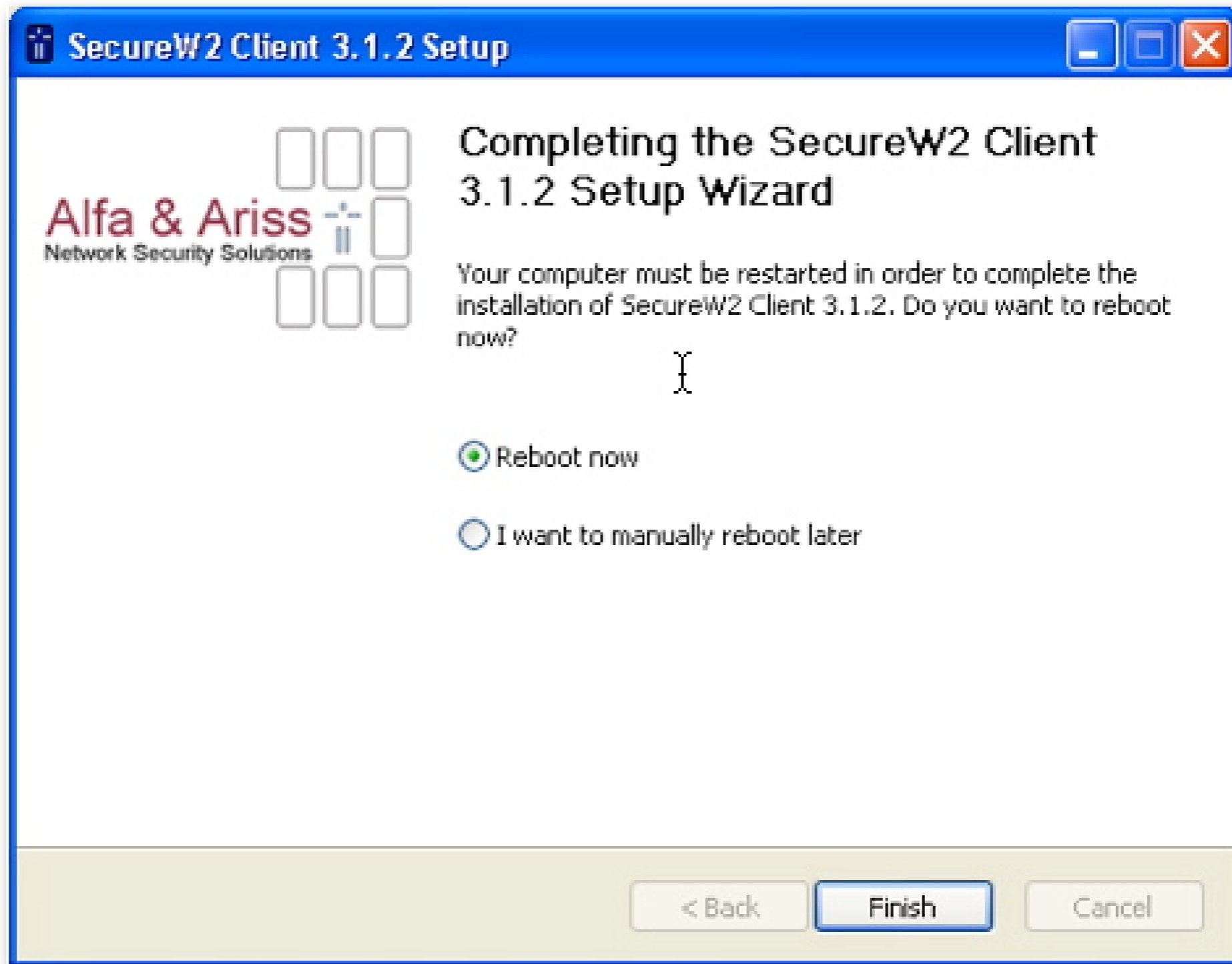
Profile:

Username:

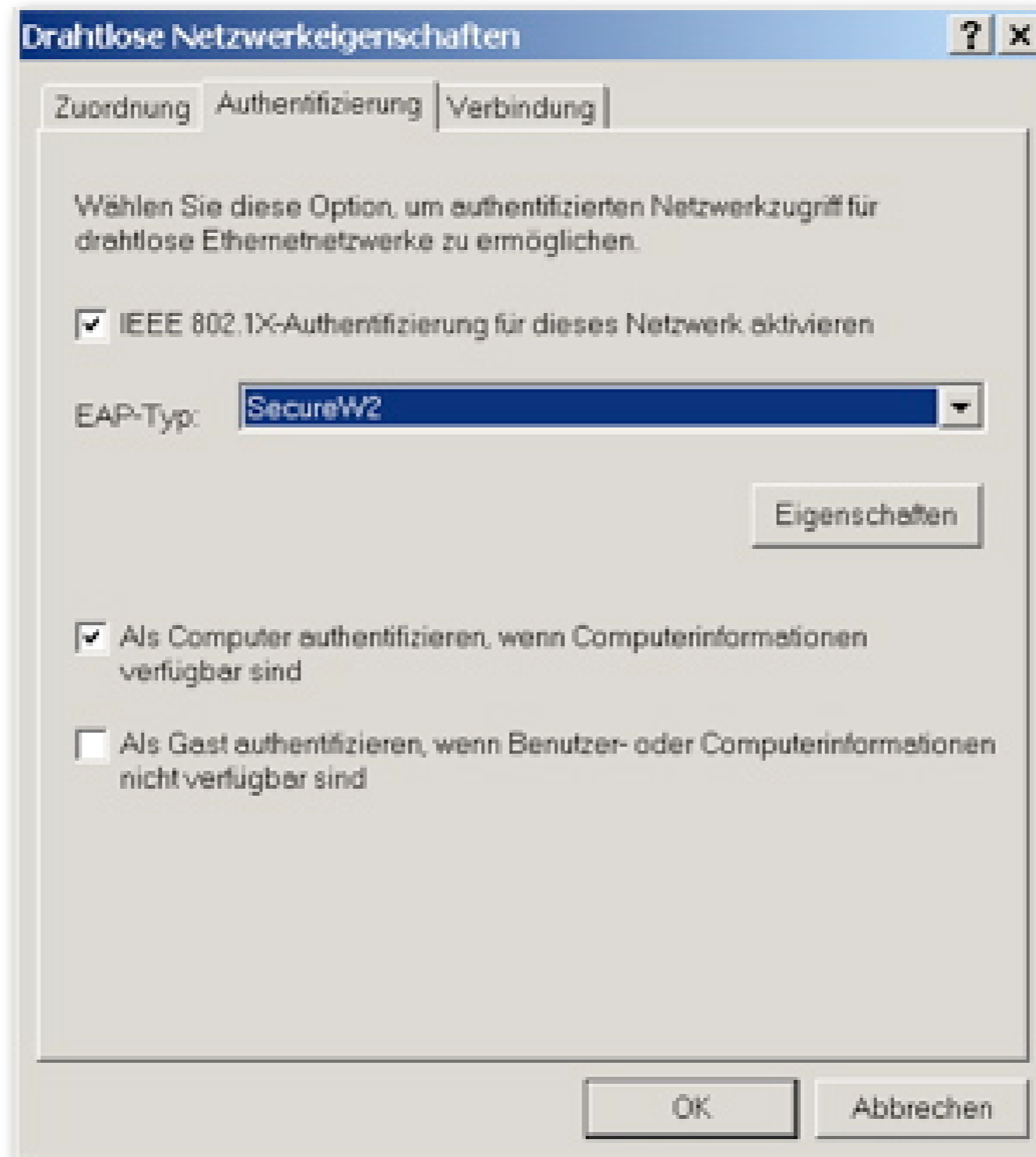
Password:

Re-enter Password:

Domain:



SecureW2



The screenshot shows the Windows Network Connections window for 'Drahtlose Netzwerkverbindung 2'. The window is divided into two main sections: 'Netzwerkaufgaben' (Network Tasks) on the left and 'Drahtlosnetzwerk auswählen' (Select Wireless Network) on the right.

Netzwerkaufgaben (Network Tasks):

- Netzwerkliste aktualisieren (Update network list)
- Drahtlosnetzwerk für Heim- bzw. kleines Firmennetzwerk einrichten (Set up wireless network for home or small business network)

Verwandte Aufgaben (Related Tasks):

- Weitere Informationen über Drahtlosnetzwerke (More information about wireless networks)
- Reihenfolge der Netzwerke ändern (Change network order)
- Erweiterte Einstellungen ändern (Change advanced settings)

Drahtlosnetzwerk auswählen (Select Wireless Network):

Klicken Sie auf ein Element in der Liste unten, um eine Verbindung mit einem Drahtlosnetzwerk in Reichweite herzustellen oder weitere Informationen zu erhalten.

Network Name	Security Type	Status
eduroam	Sicherheitsaktiviertes Drahtlosnetzwerk (WPA)	Verbindung hergestellt (Connection established)
FON_ANHALTER01	Ungesichertes Drahtlosnetzwerk (Unsecured)	Not connected
mandamus	Sicherheitsaktiviertes Drahtlosnetzwerk (WPA)	Not connected
802.1X	Sicherheitsaktiviertes Drahtlosnetzwerk (WPA)	Not connected
VPN/WEB	Ungesichertes Drahtlosnetzwerk (Unsecured)	Not connected
vodafone	Ungesichertes Drahtlosnetzwerk (Unsecured)	Not connected

A 'Trennen' (Disconnect) button is located at the bottom right of the window.

- Grosse OS Abdeckung
- Vorkonfiguration möglich
- Aufwand gering
- Relativ einfach für Nutzer
- Überwiegend Open Source

- RoamingCookbook DJ5.1.5
- <http://docs.info.apple.com>
- http://hostap.epitest.fi/wpa_supplicant
- http://eduroam.pl/Files/prepare_eduroam_config.tgz
- <http://www.securew2.com>

Fragen/Anmerkungen ?

Torsten Kersting
kersting@dfn.de