



DFNRoaming/Eduroam Supplikanten

Ralf Paffrath, Torsten Kersting
paffrath@dfn.de
kersting@dfn.de

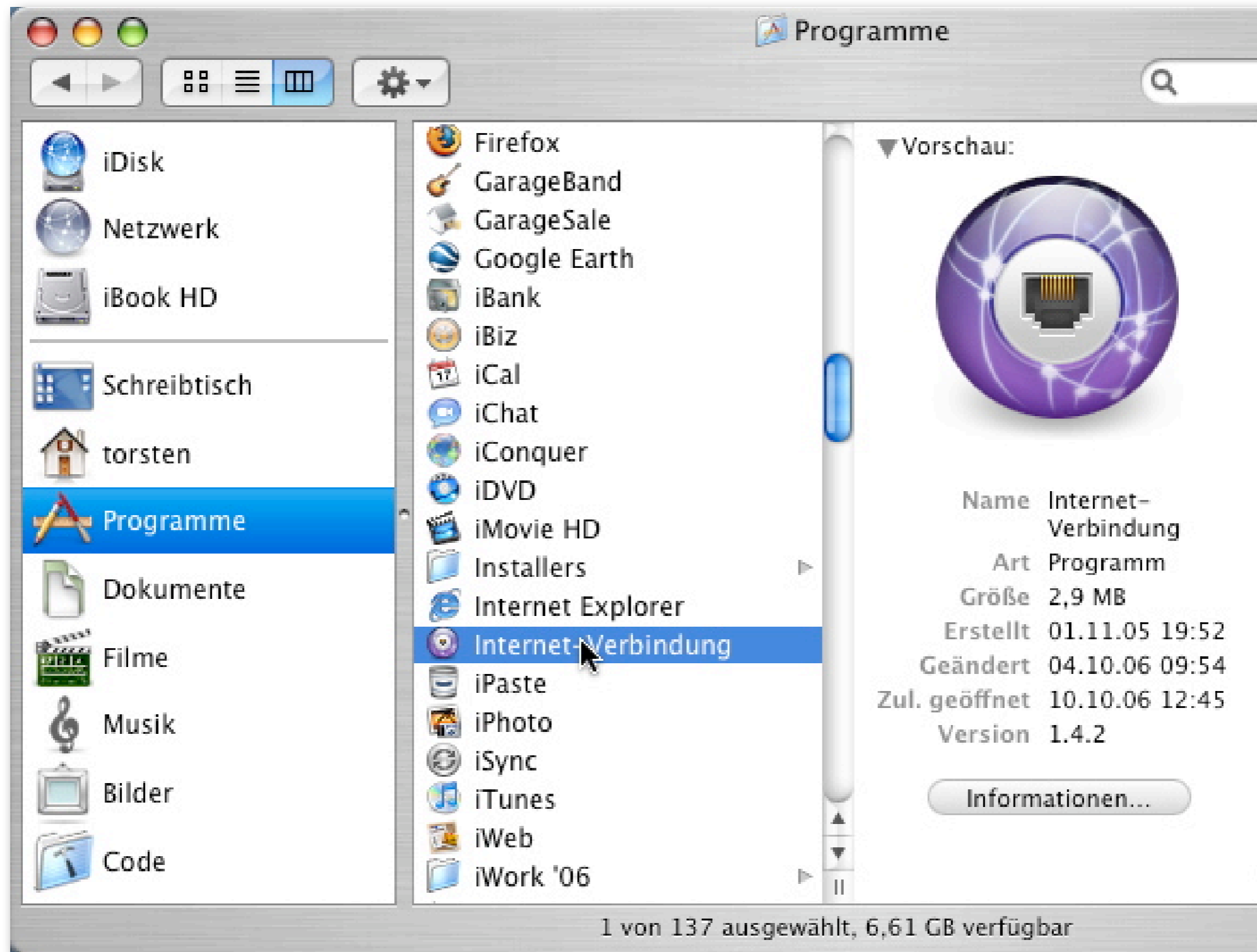
Begriffsbestimmung

- Sup|pli|kant, der; -en, -en [zu lat. supplicans (Gen.: supplicantis), 1. Part. von: supplicare= bitten, flehen] (veraltet): *Bittsteller*. © Duden - Deutsches Universalwörterbuch, 6. Aufl. Mannheim 2006 [CD-ROM].

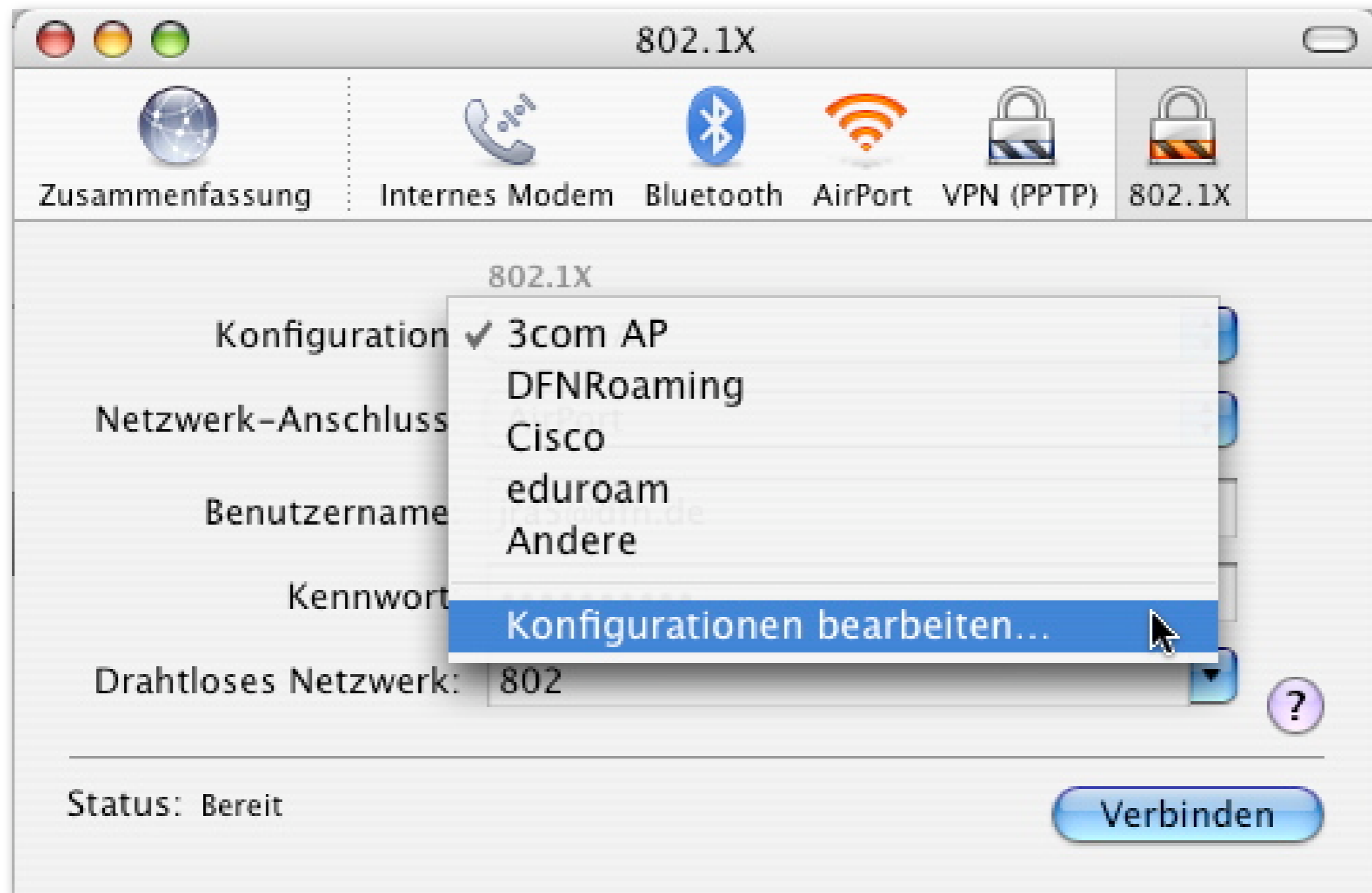
- Mac OSX Supplikant
- wpa_supplicant (open source)
- SecureW2 (open source)

- Standard 802.1X Supplikant
- keine Änderungen nötig
- sehr einfache Konfiguration
- komfortables GUI

Mac OSX Supplicant (2)



Mac OSX Supplicant (3)



Mac OSX Supplicant (4)

The screenshot shows the Mac OSX Supplicant configuration window for the 'eduroam' network. The window is titled 'eduroam' and contains the following fields and options:

- Beschreibung:** eduroam
- Netzwerk-Anschluss:** AirPort
- Benutzername:** kersting@dfn.de
- Kennwort:** [Redacted]
- Drahtloses Netzwerk:** eduroam
- Identifizierung:** A list of protocols with checkboxes:

Ein	Protokoll
<input checked="" type="checkbox"/>	TTLS
<input type="checkbox"/>	TLS
<input type="checkbox"/>	EAP-FAST
<input type="checkbox"/>	LEAP
<input type="checkbox"/>	PEAP

At the bottom of the window, there are three buttons: '+', '-', and 'OK'. A 'Konfigurieren...' button is also visible near the bottom right of the configuration area.

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

Mac OSX Supplicant (5)

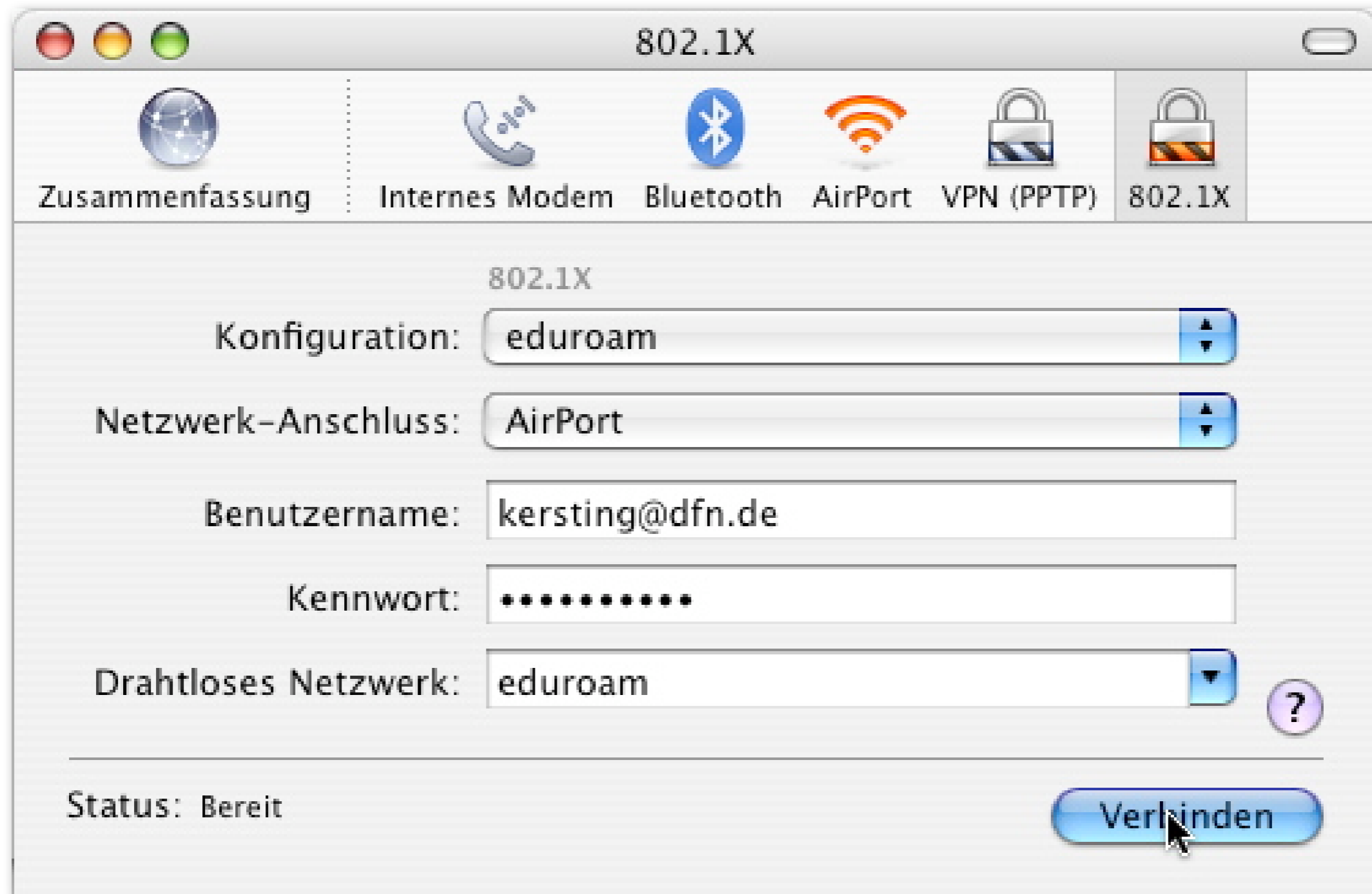
TTLS

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

Internes TTLS-Identifizierungsverfahren:

Externe Identität: (Optional)

Mac OSX Supplicant (6)



- open source 802.1X
Supplikant
- Linux, BSD, MS Windows
- Desktops/Laptops, Embedded
Systems
- [http://hostap.epitest.fi/
wpa_supplicant](http://hostap.epitest.fi/wpa_supplicant)

WPA_Supplicant: unterstützte Protokolle (1)

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

WPA_Supplicant: unterstützte Protokolle (2)

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

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

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

WPA_Suppllicant: Ablauf Verbindungsaufbau (1)

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

WPA_SupPLICANT: Ablauf Verbindungsaufbau (2)

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

WPA_Supplicant: Konfiguration (1)

```
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: Konfiguration (2)

```
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"  
}
```

WPA_Supplicant: sonstiges

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

- Da Windows (auch Vista) 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

SecureW2: Konfiguration (1)

```
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
```

SecureW2: Konfiguration (2)

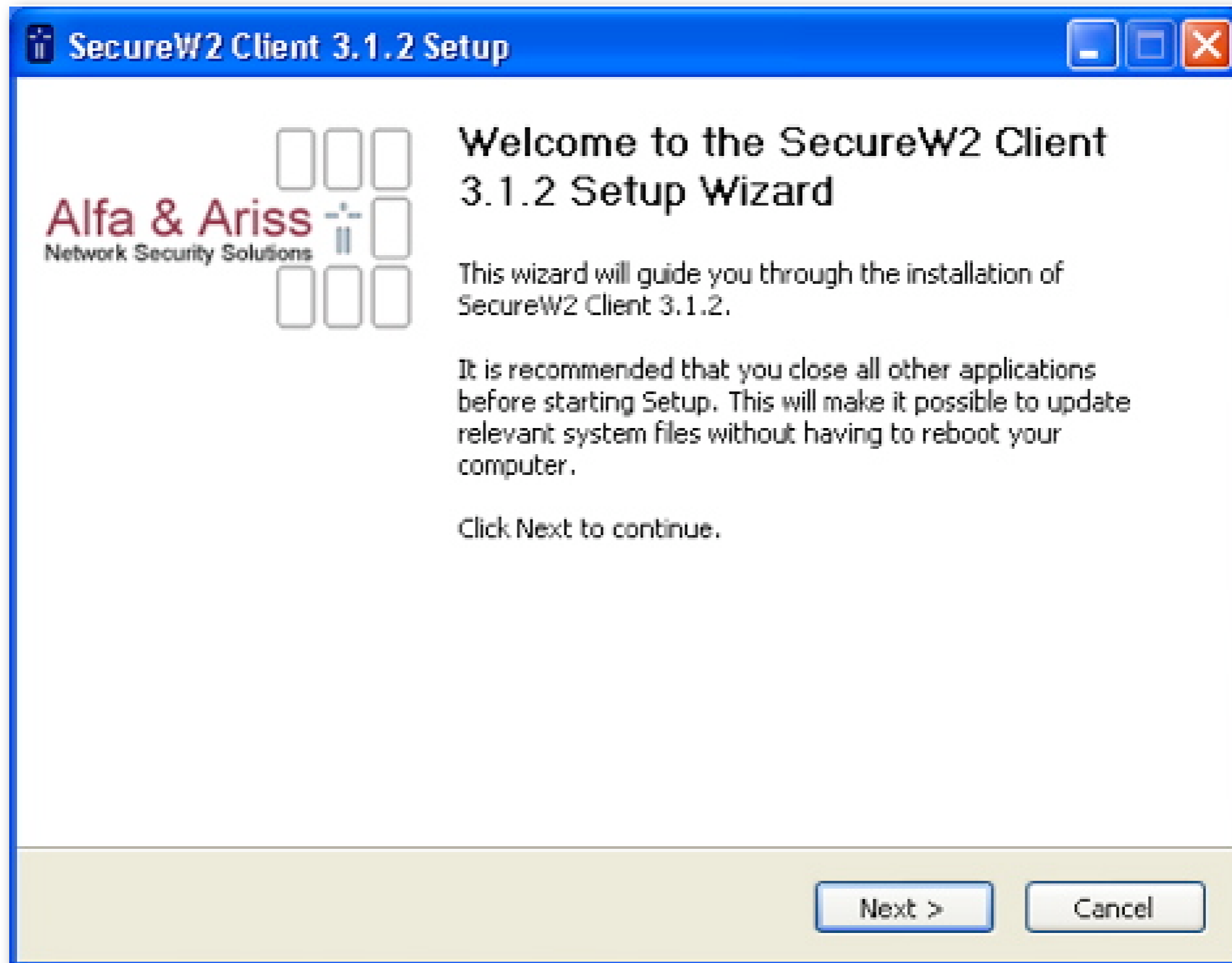
```
;-----
!define APPLICATION "SecureW2 installer"
!define VERSION "1.0.0"
;-----
    !include "MUI.nsh"
;General
;Name and file
    Name "${APPLICATION} ${VERSION}"
    OutFile "SecureW2_312_Test.exe"
;-----
;Interface Settings
    !define MUI_ICON "your_icon.ico"
    !define MUI_UNICON your_icon.ico
    !define MUI_ABORTWARNING
Section "${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: Konfigurationsverzeichnis

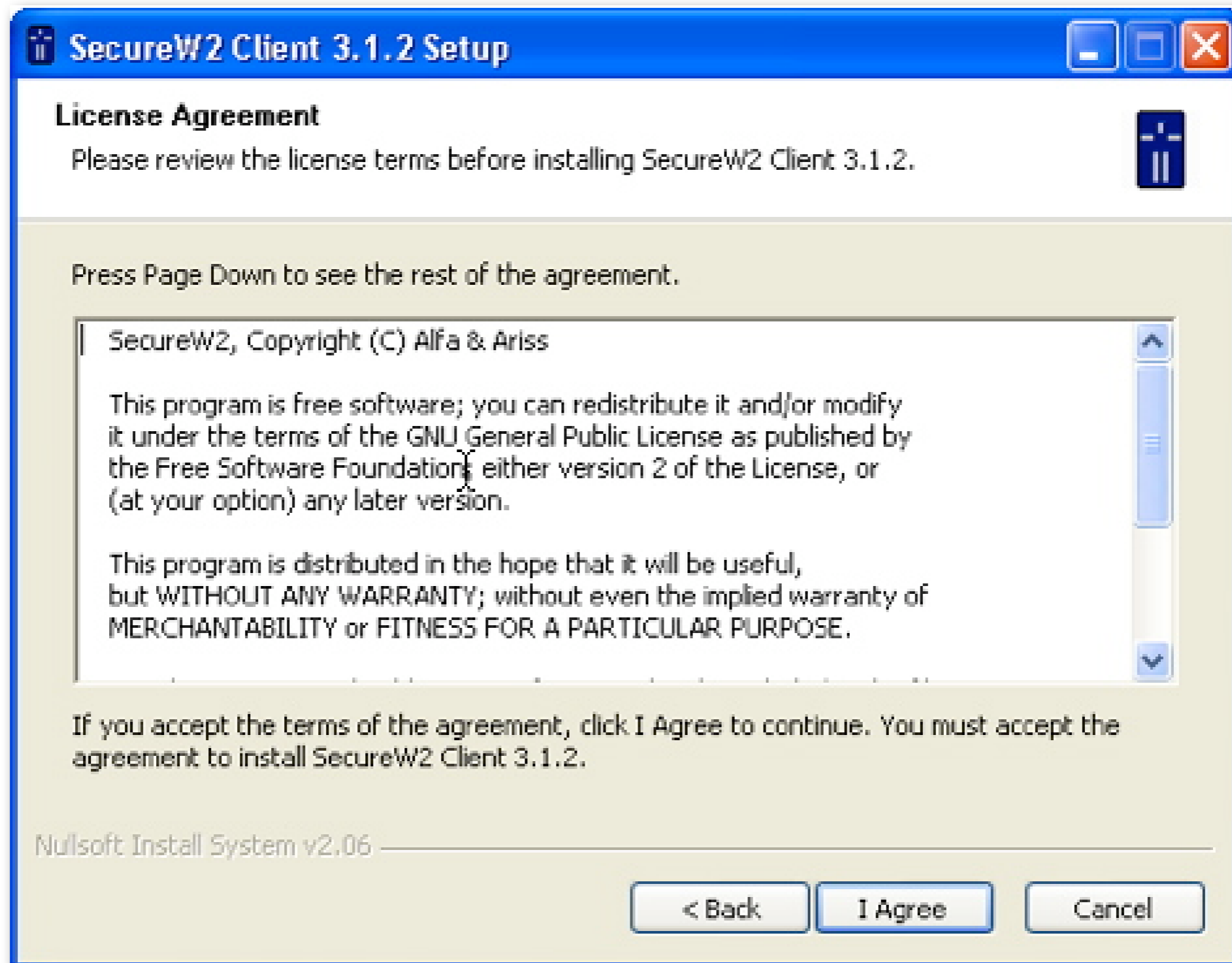
- SecureW2.INF Datei
- Konfig Datei SecureW2.NSI
- Original SecureW2.exe
- Icon Datei icon.ico
- Zertifikat

- 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`

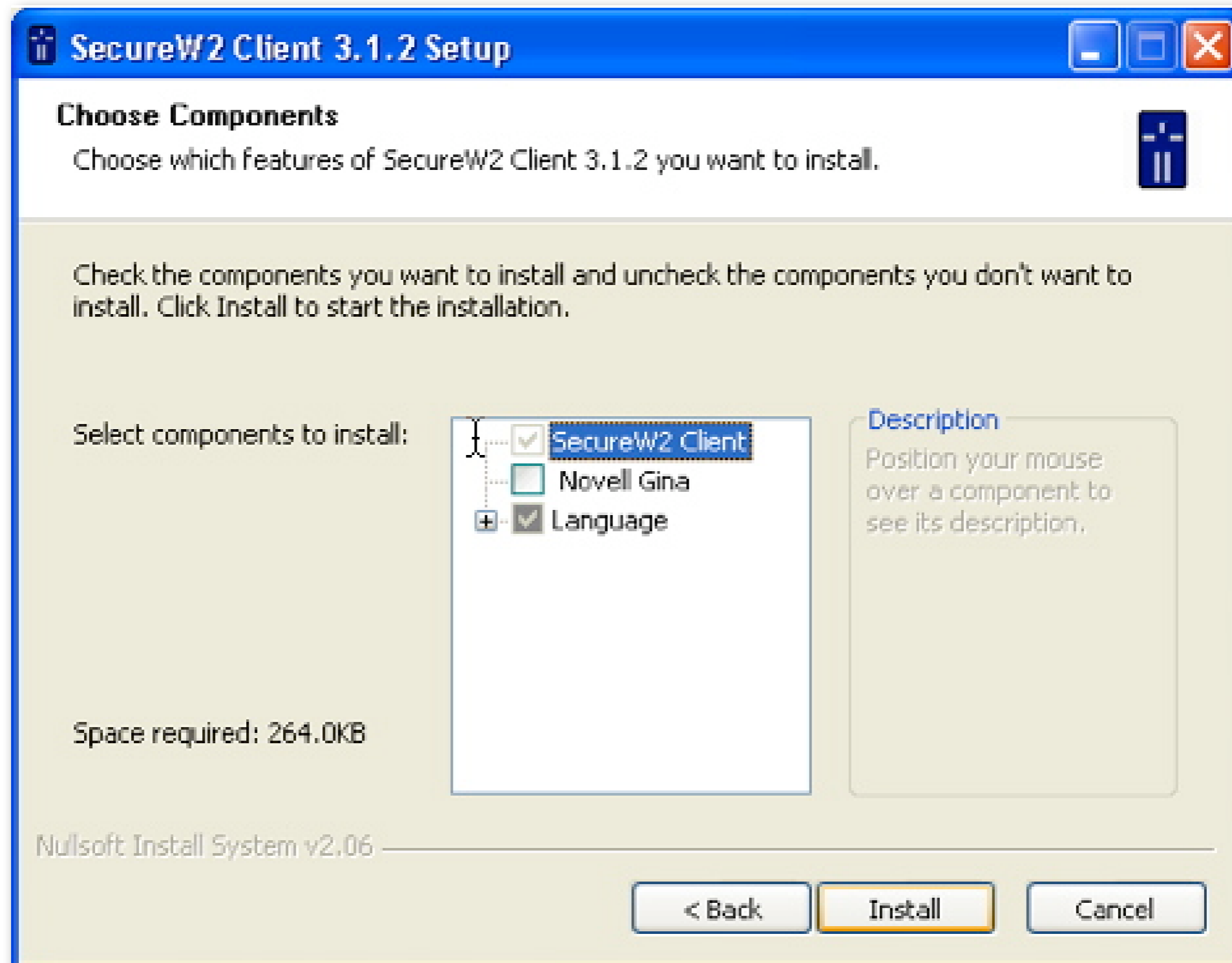
SecureW2: Start Installation



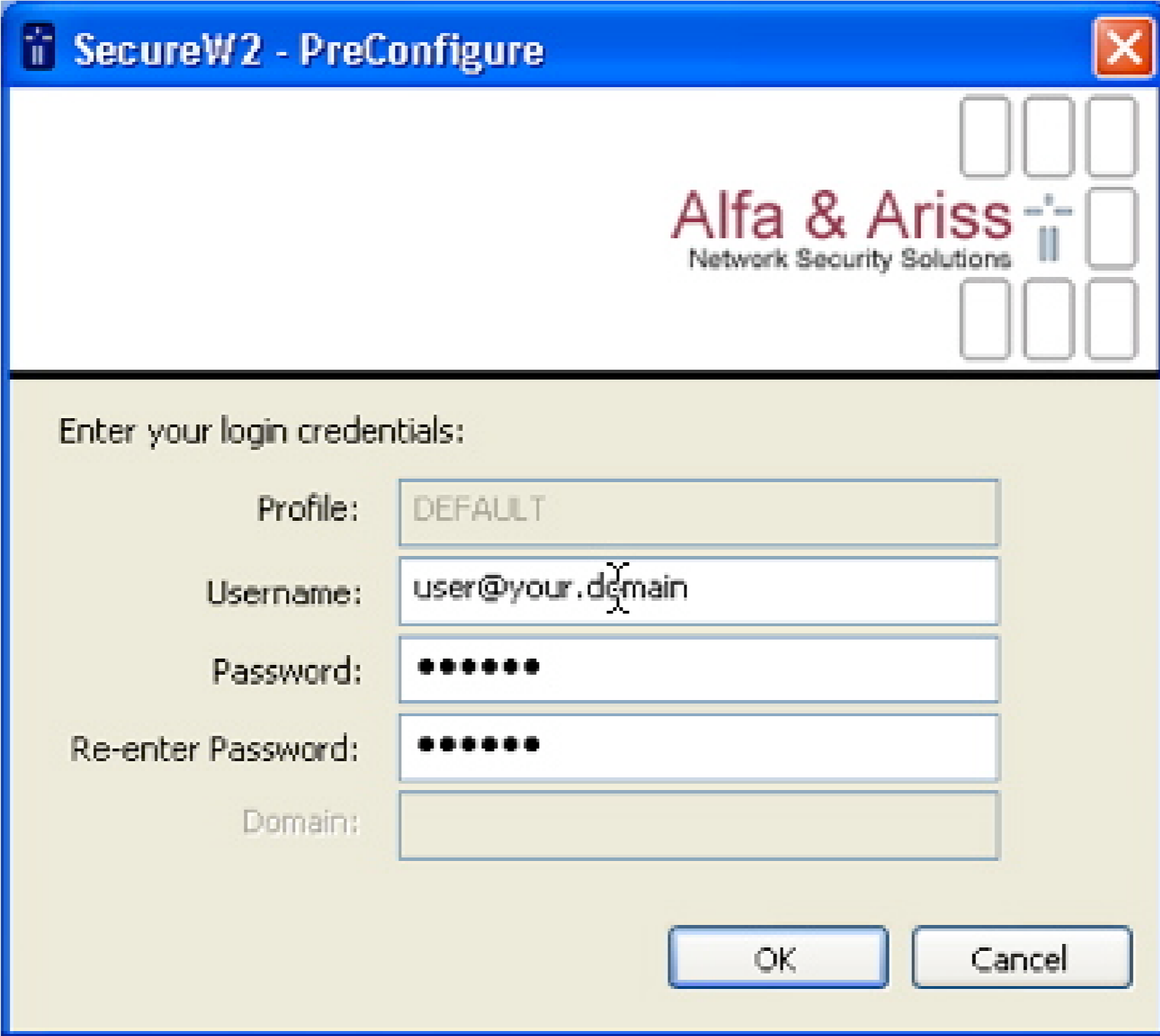
SecureW2: License Agreement



SecureW2: Komponenten auswählen



SecureW2: Credentials eingeben



The image shows a Windows-style dialog box titled "SecureW2 - PreConfigure". The title bar is blue with a standard Windows icon on the left and a red close button on the right. The main area of the dialog is light beige. At the top right, there is a logo for "Alfa & Ariss Network Security Solutions" in red and black text, accompanied by a small icon of a network tower. Below the logo are several empty rectangular boxes. The main content area contains the text "Enter your login credentials:" followed by five input fields: "Profile:" with the value "DEFAULT", "Username:" with the value "user@your.domain", "Password:" with seven black dots, "Re-enter Password:" with seven black dots, and "Domain:" which is empty. At the bottom right, there are two buttons: "OK" and "Cancel".

SecureW2 - PreConfigure

Alfa & Ariss
Network Security Solutions

Enter your login credentials:

Profile: DEFAULT

Username: user@your.domain

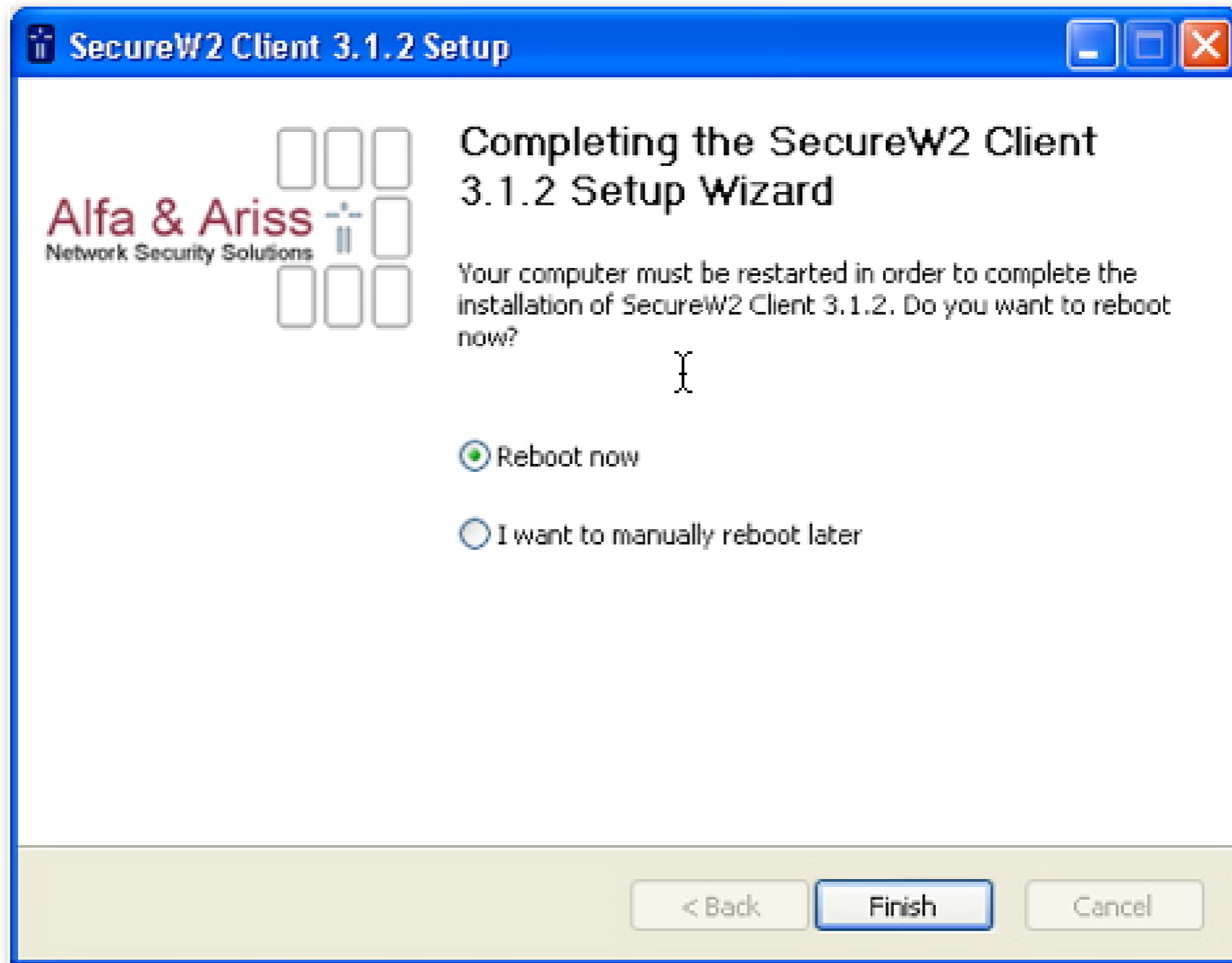
Password: ●●●●●●●

Re-enter Password: ●●●●●●●

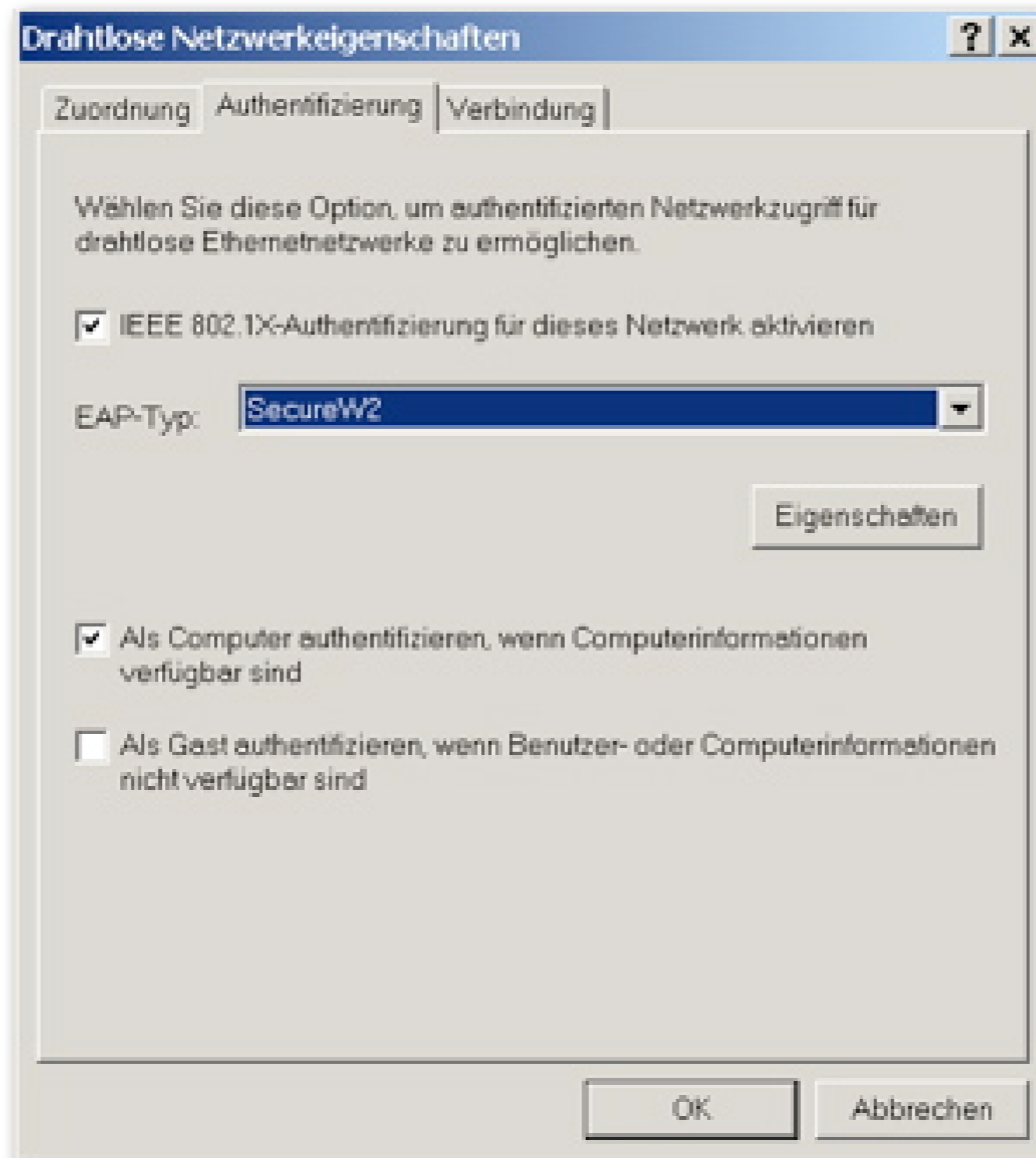
Domain:

OK Cancel

SecureW2: System Neustart



SecureW2: Eigenschaften für Drahtlosnetzwerke



SecureW2: Netzwerk auswählen

The screenshot shows a Windows window titled "Drahtlose Netzwerkverbindung 2". The window is divided into two main sections. On the left, there are two task lists: "Netzwerkaufgaben" and "Verwandte Aufgaben". The main area on the right is titled "Drahtlosnetzwerk auswählen" and contains a list of available wireless networks. The top network, "eduroam", is highlighted in blue and indicates a connection has been established. Below it are five other networks: "FON_ANHALTER01", "mandarnus", "802.1X", "VPN/WEB", and "vodafone". Each network entry shows its name, security status (e.g., "Sicherheitsaktiviertes Drahtlosnetzwerk" or "Ungesichertes Drahtlosnetzwerk"), and a signal strength indicator. A "Trennen" button is located at the bottom right of the window.

Netzwerkaufgaben

- Netzwerkliste aktualisieren
- Drahtlosnetzwerk für Heim- bzw. kleines Firmennetzwerk einrichten

Verwandte Aufgaben

- Weitere Informationen über Drahtlosnetzwerke
- Reihenfolge der Netzwerke ändern
- Erweiterte Einstellungen ändern

Drahtlosnetzwerk auswählen

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

Netzwerkname	Sicherheitsstatus	Verbindungsstatus
eduroam	Sicherheitsaktiviertes Drahtlosnetzwerk (WPA)	Verbindung hergestellt
FON_ANHALTER01	Ungesichertes Drahtlosnetzwerk	Keine Verbindung
mandarnus	Sicherheitsaktiviertes Drahtlosnetzwerk	Keine Verbindung
802.1X	Sicherheitsaktiviertes Drahtlosnetzwerk	Keine Verbindung
VPN/WEB	Ungesichertes Drahtlosnetzwerk	Keine Verbindung
vodafone	Ungesichertes Drahtlosnetzwerk	Keine Verbindung

Trennen

- 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 ?

Ralf Paffrath
paffrath@dfn.de
&
Torsten Kersting
kersting@dfn.de