NCP
SECURE COMMUNICATIONS

Secure Entry
CE Client

NCP
SECURE COMMUNICATIONS

Secure Entry CE Client

Version 2.33
Mai 2007

Copyright

Alle Programme und das Handbuch wurden mit größter Sorgfalt erstellt und nach dem Stand der Technik auf Korrektheit überprüft. Alle Haftungsansprüche infolge direkter oder indirekter Fehler, oder Zerstörungen, die im Zusammenhang mit den Programmen stehen, sind ausdrücklich ausgeschlossen.

Die in diesem Handbuch enthaltene Information kann ohne Vorankündigung geändert werden und stellt keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Gesamtherstellung dieses Handbuchs:
Michael Lösel
Dokumentation + Publikation
doku@michael-loesel.de
Schweppermannstr. 44
90408 Nürnberg
0172 / 82 58 238

Network
Communications
Products engineering GmbH

Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet http:// www.ncp.de

NCP Hotline

Die NCP Hotline begleitet Sie mit technischem Sachverstand von der Beratung und Projektierung zur Installation, zum firmenspezifischen Training, bis zum Support in Ihrem Anwendungsumfeld.

Für eine umfassende Betreuung der NCP-Produkte im täglichen Einsatz bietet NCP Support von Montag bis Freitag, von 8:00 bis 17:00, der per Fax oder E-Mail kostenlos erreichbar ist, via Telefon per Dienstleistungsauftrag (siehe unten).

Service-Verträge werden nach Produkt-Gruppen abgeschlossen und umfassen alle dazugehörigen Produkte. Detaillierte Auskünfte zu Service-Verträgen erteilen NCP-Mitarbeiter unter: 09 11 / 99 68-0

Dienstleistungsauftrag nach Aufwand

Auch ohne Service-Vertrag können Sie Dienstleistungen von NCP in Anspruch nehmen. Allerdings nur in beschränktem Umfang und nach einer schriftlichen Auftragserteilung Ihrerseits. In diesem Falle werden die von NCP erbrachten Leistungen nach Aufwand in Rechnung gestellt.

Software Downloads und Auskünfte

Software Downloads und Informationen sind unter der Homepage von NCP erhältlich:
http://www.ncp.de
FTP-Server: ftp://ftp.ncp.de

Inhalt

1. Produktübersicht

Dieses Handbuch beschreibt Installation, Konfiguration, Leistungsumfang und Benutzeroberfläche der Secure Communications-Komponenten:

- **NCP Secure Entry CE Client**
- **NCP Secure Entry CE Client Configurator**

Die NCP Secure Client Software arbeitet nach dem Prinzip einer LAN Emulation für Ethernet und unterstützt die routbaren Protokolle TCP/IP.

Weitere Informationen zu Ausbaustufen und Produktvarianten erhalten Sie auf der NCP Website: http://www.ncp.de

1.1 Zum Umgang mit diesem Handbuch

Damit Sie sich in dieser Dokumentation schnell zurecht finden, ist im folgenden kurz ihr Aufbau dargestellt.

Das Handbuch ist in sechs größere Abschnitte untergliedert, die Step-by-Step oder dem Aufbau der grafischen Benutzeroberfläche folgend den jeweiligen Gegenstand beschreiben. Diesen Abschnitten folgen zwei Anhänge, die dem Verständnis und dem Auffinden von Fachtermini dienen.

1. Produktübersicht mit kurzer Beschreibung des Leistungsumfangs der Software
2. Installationsanweisungen
3. Beschreibung der grafischen Benutzeroberfläche, sowie der Konfigurationsmöglichkeiten
4. Beschreibung der im Telefonbuch aufgelisteten Parameter
5. Beschreibung eines Verbindungsaufbaus
6. Beispiele und Erklärungen, insbesondere zu IPSec

– Anhänge mit einem Glossar (Abkürzungen und Begriffe) und einem Index

Querverweise sind im Text in Klammern gesetzt und geben die Verweisstelle mit dem Titel, bzw. nach einem Komma, mit dem Untertitel an. Texte, die am Seitenrand mit einem Ausrufezeichen markiert sind, sollten besonders beachtet werden.

Selbstverständlich verfügt die Software auch über eine kontextsensitive Online-Hilfe.

1.2 NCP Secure Entry Client – universeller IPSec Client

Der NCP Secure Entry Client kann in beliebigen VPN-Umgebungen eingesetzt werden. Er kommuniziert auf der Basis des IPSec-Standards (siehe →Beispiele und Erklärungen, Security, IPSec) mit den Gateways verschiedenster Hersteller* und ist die Alternative zu der am Markt angebotenen, einheitlichen IPSec-Client-Technologie. Der Secure Entry Client verfügt über zusätzliche Leistungsmerkmale, die dem Anwender den Einstieg in eine ganzheitliche Remote Access VPN-Lösung ermöglichen.

Der NCP Secure Entry Client bietet:

☑ Unterstützung aller gängigen Betriebssysteme

☑ Einwahl über alle Übertragungsnetze

☑ Kompatibilität mit den VPN-Gateways unterschiedlichster Hersteller

☑ Integrierte Personal Firewall für mehr Sicherheit

☑ Dialer-Schutz (keine Bedrohung durch 0190er- und 0900er-Dialer)

☑ Bedienungskomfort (grafische Oberfläche)

☑ Zentrales Management**

**) Kompatibilitätsliste kann angefordert werden unter marketing@ncp.de*
***) optional*

1.3 Leistungsumfang

Der NCP Secure Entry Client unterstützt alle gängigen Betriebssysteme (Windows 98se, ME, NT, 2000, XP, Windows CE und Linux). Die Einwahl in das Firmennetz erfolgt unabhängig vom Mediatyp (siehe →Konfigurationsparameter, Telefonbuch, Zielsystem), z.B. beim Secure Entry CE Client neben PSTN (analoges Fernsprechnetz), GSM und GPRS wird auch LAN-Technik wie im WLAN (am Firmengelände und Hotspot) oder lokalem Netzwerk (z.B. Filialnetz) unterstützt.

Ein Szenario könnte so aussehen, dass ein Mitarbeiter mit ein und demselben Endgerät von unterschiedlichen Lokationen auf das Firmennetz zugreifen muss:

– in der Filiale über WLAN
– in der Zentrale über LAN
– unterwegs an Hotspots und beim Kunden über WLAN bzw. GPRS

1.3.1 Client Monitor – Grafische Benutzeroberfläche

Die grafische Oberfläche (siehe →Client Monitor) des Secure Entry Clients schafft Transparenz während des Einwahlvorganges und Datentransfers. Sie informiert u.a. über:

– aktuelles Datenvolumen,
– verbleibende Zeit bis zum nächsten Timeout (Short Hold Mode),
– Verbindungsparameter (Verschlüsselung etc.)

1.3.2 NCP Dialer

Ein eigener Dialer ersetzt den sonst üblichen Microsoft DFÜ-Dialer. Daraus ergeben sich Vorteile gleich in mehrfacher Hinsicht:

– intelligentes Line Management (Short Hold Mode) in Wählnetzen
– integrierte Personal Firewall-Mechanismen
– Schutz vor “automatischen Dialern”

1.3.3 Line Management

Um die Übertragungsgebühren möglichst gering zu halten, werden aktive Verbindungen automatisch unterbrochen, wenn keine Daten fließen. Liegen erneut Daten für die Übertragung vor, wird die ruhende Verbindung ohne Einwirkung des Benutzers aktiviert. Gebühren fallen immer nur dann an, wenn Daten übertragen werden.

1.3.4 Personal Firewall

Der NCP Secure Entry Client verfügt über alle erforderlichen Personal Firewall Funktionalitäten um den PC-Arbeitsplatz umfassend gegenüber Angriffen aus dem Internet und anderer LAN-Teilnehmer (WLAN oder LAN) zu schützen. Weiter besteht keine Möglichkeit, dass der NCP Dialer von automatischen 0190er- und 0900er-Dialern für ungewollte Verbindungen missbraucht wird.

Die wesentlichen Security-Mechanismen sind IP-NAT und Protokollfilter. NAT (Network Address Translation) ist ein Security-Standard zum Verbergen der individuellen IP-Adressen gegenüber dem Internet. NAT bewirkt eine Übersetzung der von außen sichtbaren Adresse in entsprechende Client-Adressen und umgekehrt. Ankommende Datenpakete werden auf der Basis eines ausgeklügelten Filterings nach genau definierten Eigenschaften überprüft und bei Nichtübereinstimmung abgewiesen. Das heißt: Der Internet-Port des jeweiligen Rechners wird vollständig getarnt und der Aufbau von unerwünschten Verbindungen unmöglich.

1.3.5 PKI-Unterstützung

Die Zugangssicherheit zum PC und damit dem Firmennetz kann durch den Einsatz elektonischer Zertifikate in Form von Software (PKCS#12) oder Smart Cards (PKCS#11, PC/SC) erhöht werden. Der NCP Secure Entry Client unterstützt hierfür die Einbindung in eine PKI (Public Key Infrastruktur).

Public Key Infrastruktur

Public-Key-Infrastrukturen (PKI) beschreiben ein weltweit genutztes Verfahren, um zwischen beliebigen Kommunikationspartnern auf elektronischem Wege Schlüssel sicher auszutauschen. Die PKI bedient sich dabei sogenannter Schlüsselpärchen aus jeweils einem öffentlichen und einem privaten Schlüssel.

In der Welt des elektronischen, globalen Informationsaustausches wird so eine Vertrauensbasis aufgebaut, wie wir sie in der traditionellen Geschäftswelt auf Papierbasis kennen. Die digitale Signatur in Verbindung mit Datenverschlüsselung ist das elektronische Äquivalent zur händisch geleisteten Unterschrift und belegt Ursprung sowie die Authenizität von Daten und Teilnehmer.

Eine PKI basiert auf digitalen Zertifikaten, die – von einer öffentlichen Zertifizierungsstelle (Trust Center) ausgestellt – als persönliche “elektronische Ausweise” fungieren und idealerweise auf einer Smart Card abgespeichert sind. Sicherheitsexperten und der IETF (Internet Engineering Task Force) sind sich darüber einig, dass ein nachhaltiger Schutz vor Man-In-The-Middle-Attacken nur durch den Einsatz von Smart Cards mit Zertifikaten erreicht werden kann.

Smart Card

Smart Cards sind die ideale Ergänzung für hochsichere Remote Access-Lösungen. Sie bieten doppelte Sicherheit beim Login-Vorgang, nämlich Wissen über PIN (Persönliche Identifikations Nummer) und Besitz der Smart Card. Der Anwender identifiziert sich mit der Eingabe der PIN eindeutig als rechtmäßiger Besitzer (Strong Authentication). Die PIN ersetzt das Passwort und die Eingabe der User-ID (Basistechnologie für Single Sign On). Der Anwender weist sich nur noch gegenüber der Smart Card aus. Der Check gegenüber dem Netz erfolgt zwischen Smart Card und Security-System. Alle sicherheitsrelevanten Operationen laufen vollständig im Inneren der Karte – also außerhalb des PCs – ab. Das System ist neben individuellen Anpassungen an Schutzmechanismen offen für multifunktionalen Einsatz (z. B. als Company Card). Auch biometrische Verfahren lassen sich integrieren.

Weitere Informationen erhalten Sie unter info@ncp.de

1.4 Optionale Erweiterungen

1.4.1 Administration

Für die Administration der entfernten PC-Arbeitsplätze stehen optional leistungsfähige Management-Tools zur Verfügung (Secure Client Manager, Secure Update Server, Secure PKI Manager). Diese bieten alle Funktionalitäten für den Aufbau und Betrieb eines professionellen Remote Access VPNs.

Im Wesentlichen geht es um die Bereiche Rollout und Betrieb.

Rollout:
– Anlegen der User-Konfigurationen
– Initialisierung bei der Ersteinwahl
– Ausstellen und Verteilen von Zertifikaten

Betrieb:
– Userverwaltung
– Software-Updates
– Verwaltung von Zertifikaten
– Remote Helpdesk (Remote Control)

1.4.2 NCP Secure High Availability Services

Für Ausfallsicherheit und gleichmäßige Auslastung mehrerer NCP Secure VPN Gateways sorgen die High Availability-Services, bestehend aus Secure Failsafe Server und Load Balancing Server. Während der Secure Failsafe Server Backup-Funktionalität für ein VPN Gateway bietet, verteilt der Laod Balancing Server die VPN-Verbindungen (Tunnel) gleichmäßig auf alle verfügbaren NCP Secure VPN Systeme.

2. Installation

Die Installation der Secure Entry CE Client Software erfolgt für alle Windows-Systeme komfortabel über Setup. Der Installationsablauf ist für alle Versionen des Secure Clients identisch.

Bevor Sie die Software installieren, müssen, zur vollen Funktionsfähigkeit die Installationsvoraussetzungen, wie im folgenden Kapitel beschrieben, erfüllt sein.

Bitte beachten Sie zudem, dass die Software NCP Secure Entry CE Client aus zwei Komponenten besteht, die getrennt installiert werden müssen:

- **PC-Komponente**

  Die PC-Komponente verfügt über den NCP Secure Entry CE Client Configurator zur Erstellung einzelner Profile. Von diesem Configurator werden über ActiveSync die Profil-Einstellungen auf den PDA kopiert.

- **PDA-Komponente**

  Die PDA-Komponente besteht aus dem NCP Secure Entry CE Client Service (kurz: NCP Client Service), der die Daten für das Modem (bzw. Handy) oder einen LAN-Adapter und den Chipkartenleser auswertet, und dem NCP Secure Entry CE Client Monitor (kurz: NCP Client Monitor) zur Auswahl des Zielsystems und dem Verbindungsaufbau dorthin.

Reihenfolge von der Installation bis zur Inbetriebnahme

Halten Sie sich bitte an folgende Reihenfolge!

☑ Installation der PC-Komponente

☑ Installation des Chipkartenlesers am PDA (bei Einsatz von Smart Cards)

☑ Installation der PDA-Komponente

☑ Start des NCP Client Drivers am PDA (bei Einsatz der Strong Security-Version)

☑ Konfiguration des Zielsystems am PC

☑ Übertragung des Profile (und der Zertifikate für die Strong Security-Version)

☑ Inbetriebnahme am PDA

2.1 Installationsvoraussetzungen

Betriebssystem

Die PC-Komponente der Secure Entry CE Software kann auf Computern mit den Betriebssystemen Microsoft Windows 2000, Windows XP oder Windows Vista installiert werden. Halten Sie für die Dauer der Installation unbedingt die Datenträger (CD oder Disketten) für das jeweils im Einsatz befindliche Betriebssystem bereit, um Daten für die Treiberdatenbank des Betriebssystems nachladen zu können!

Auf dem PC muss vorher das Programm Microsoft ActiveSync 3.0 oder höher installiert worden sein. Über dieses Programm wird die PDA-Komponente installiert und erfolgt der Datenaustausch zwischen PDA und PC.

Lokales System

Die Einwahl an das Zielsystem erfolgt über einen PDA (Personal Digital Assistant). Da zur Einwahl alternativ der NCP-Dialer oder der Microsoft RAS-Dialer genutzt werden kann, werden alle marktgängigen PDA-Handy-Kombinationen unterstützt. Entsprechende CE-kompatible Treiber sind Voraussetzung.

- **Analoge Modems und Handys**

Für die Kommunikation über Modem (bzw. Handy) muss das Modem korrekt von Windows CE erkannt worden sein.

Treiber für Modems, die den Hayes-Befehlssatz unterstützen, sind in Windows CE integriert. Ebenso unterstützt Windows CE die meisten Handys mit IR-Schnittstelle oder Bluetooth und eingebautem Modem.

Die Modemdaten werden beim Start der PC-Komponente oder über die Configurator-Oberfläche der PC-Komponente (siehe → Client-Configurator, Konfiguration) vom PDA herunter geladen. Bitte achten Sie darauf, dass zu diesem Zeitpunkt eine ActiveSync-Verbindung zwischen PC und PDA besteht.

- **LAN-Adapter (LAN/WLAN over IP)**

Um die Client-Software mit der Verbindungsart “LAN over IP” in einem Local Area Network betreiben zu können, muss ein LAN-Adapter (Ethernet oder Wireless LAN) am PDA installiert sein.

Voraussetzungen für die Strong Security-Version

Wenn Sie die Software VPN/PKI CE Client (Strong Security-Version des Clients) nutzen, die Zertifizierung (X.509) unterstützt, so muss entweder ein Chipkartenleser am PDA angeschlossen sein oder ein Soft-Zertifikat dort eingespielt sein.

■ Chipkartenleser (PC/SC-konform)

Die Client Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind. Diese Chipkartenleser werden nur in der Liste der Chipkartenleser aufgenommen, nachdem der Leser angeschlossen und die zugehörige Treiber-Software installiert wurde. Beim Start des “NCP Client Driver” am PDA wird der Chipkartenleser im System gesucht. Deshalb ist es unbedingt nötig, dass der Kartenleser zu diesem Zeitpunkt installiert und angeschlossen ist!

Zertifikats-Konfiguration

Bitte beachten Sie unbedingt: Bevor Sie mit der PC-Komponente des Clients eine Zertifikats-Konfiguration vornehmen (siehe → Client Configurator der PC-Komponente, Konfiguration, Zertifikate), müssen die Informationen über vorhandene Chipkartenleser vom PDA auf den PC übertragen worden sein. Da diese vom NCP Client Driver erstellt werden, muss dieser vor dem Start der PC-Komponente geladen worden sein. Zur Übertragung dieser Daten ist eine bestehende ActiveSync-Verbindung notwendig.

■ Chipkarten (Smart Cards)

Die Strong Security-Version des Clients unterstützt Chipkarten von Signtrust, NetKey 2000 und TC Trust (CardOS M4). NCP arbeitet ständig daran, neue Chipkartenleser und Chipkarten zu unterstützen. Konsultieren Sie deshalb die NCP Website, um die aktuellste Liste der unterstützen Produkte abzufragen.

■ Chipkarten oder Token (PKCS#11)

Die PKCS#11-Module von Fremdherstellern werden über deren Treiberbibliothek (DLL) unterstützt.

■ Soft-Zerifikate (PKCS#12-Datei)

Anstatt das Zertifikat von einer Smart Card über einen Chipkartenleser auszulesen, kann auch ein Soft-Zertifikat (PKCS#12-Datei) verwendet werden.

Zertifikats-Konfiguration

Bitte beachten Sie: Pfad und Name der für die Konfiguration erforderlichen PKCS#12-Datei (siehe → Client Configurator – Konfiguration – Zertifikate) muss zu dem Ort der Datei auf dem PDA passen!

Zur Übertragung der PKCS#12-Datei kann im Configurator der PC-Komponente der Menüpunkt “Konfiguration / Übertrage PKCS#12-Datei zum PDA” verwendet werden. Wird diese Funktion genutzt, so kann der Pfad folgendermaßen angegeben werden:

```
%INSTALLDIR%\certs\<PKCS#12-Dateiname>
```

2.2 Installation der PC-Komponente

Die Software der PC-Komponente wird unter den Betriebssystemen Windows 2000/XP und Vista ohne Unterschiede installiert. Bitte achten Sie jedoch darauf, ob Sie von Festplatte, CD oder Diskette installieren. Sollten Sie bereits eine ältere Version der Software installiert haben, beachten Sie bitte das Kapitel “Update und Deinstallation”.

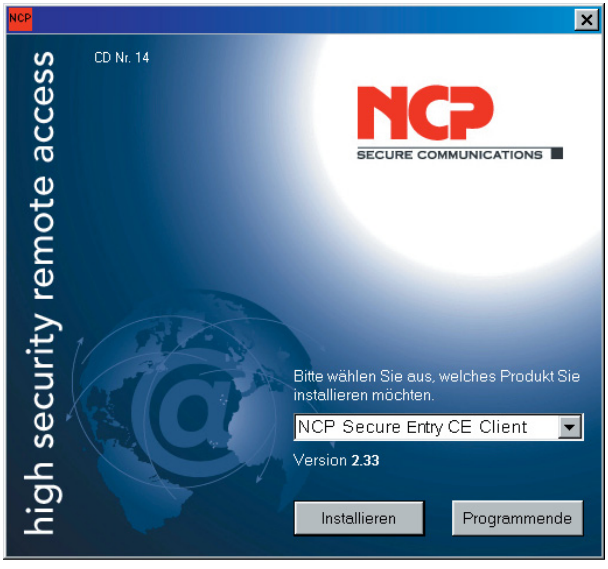
Installation und Lizenzierung

Der NCP Secure Entry Client wird zunächst immer als Testversion installiert. Haben Sie eine Lizenz erworben, so können die Lizenzierungsdaten nach der Installation und einem Reset am PDA im Popup-Menü des Monitors unter “Aktivierung” eingegeben werden. Spätestens in den letzten 10 Tagen vor Ablauf der 30-tägigen Gültigkeitsdauer der Testversion werden Sie im Client-Monitor daran erinnert, dass eine Lizenzierung vorgenommen werden muss, wenn die Client Software weiter verwendet werden soll. Bitte beachten Sie zur Lizenzierung die Beschreibung im Handbuchabschnitt zum Popup-Menüpunkt “Aktivierung”.

Installation von der Festplatte

Wenn Sie die Software nach einem Download vom NCP FTP-Server installieren möchten, entpacken Sie zunächst die ZIP-Datei. Beim Entpacken werden automatisch die Verzeichnisse “DISK1”, “DISK2”, “DISK3” etc. angelegt. Wenn zu Beginn der Installation die Aufforderung “Programm von Diskette oder CD installieren” erscheint, so klicken Sie “Weiter” und anschließend “Durchsuchen”, um SETUP.EXE im Verzeichnis “DISK1” zu wählen. Alle weiteren Installationsvorgänge sind mit denen der Standard-Installation identisch.

Installation von CD



Nachdem Sie die CD in das Laufwerk Ihres Computers eingelegt haben, erscheint nach einigen Sekunden automatisch die NCP-Begrüßungsmaske auf Ihrem Configurator (siehe Bild links).

Sie wählen aus, welches Produkt Sie installieren möchten und klicken anschließend auf “Installieren”. Das weitere Verfahren ist mit der Installation von Diskette ab “Wählen der Setup-Sprache” identisch.

2.2.1 Standard-Installation

Sollten Sie vorkonfigurierte Installationsdisketten von Ihrem Administrator erhalten, folgen Sie bitte seinen Anweisungen zur Installation.

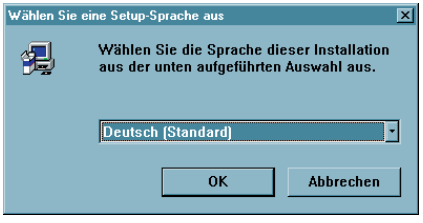
Als ersten Installationsschritt wählen Sie im Windows-Hauptmenü “Start / Einstellungen / Systemsteuerung.”

In der Systemsteuerung wählen Sie “Software”.

Klicken Sie anschließend auf den Button zum “Installieren”.

Legen Sie jetzt die erste Diskette mit der Client Software in das Laufwerk Ihres Computers (siehe Bild links), wenn Sie es noch nicht getan haben, und klicken Sie “Weiter”...

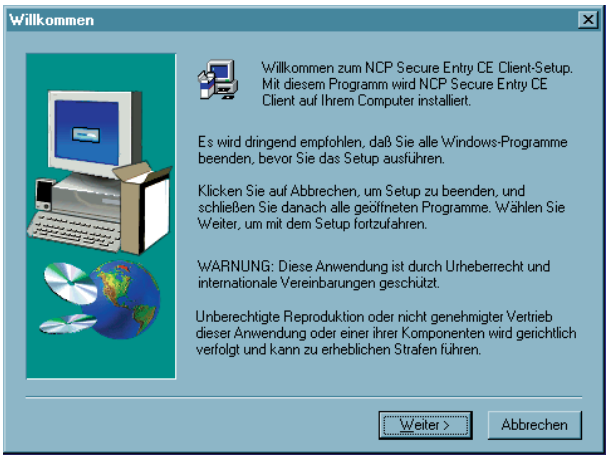
Wenn “SETUP.EXE” angezeigt wird, klicken Sie auf “Fertigstellen”.



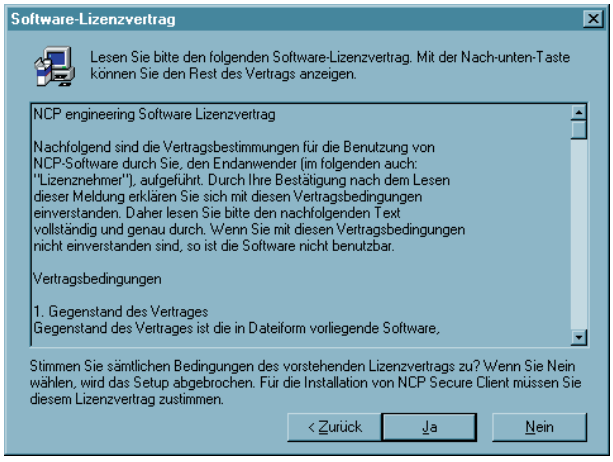
Im folgenden Fenster können Sie die Setup-Sprache auswählen. Klicken Sie danach auf “OK”.

Anschließend bereitet das Setup-Programm den Install-Shield Assistenten vor, mit dessen Hilfe die Installation fortgesetzt wird.

→ *weiter nächste Seite*



Lesen Sie bitte die Hinweise im Willkommen-Fenster des Setup-Programms bevor Sie auf “Weiter” klicken.

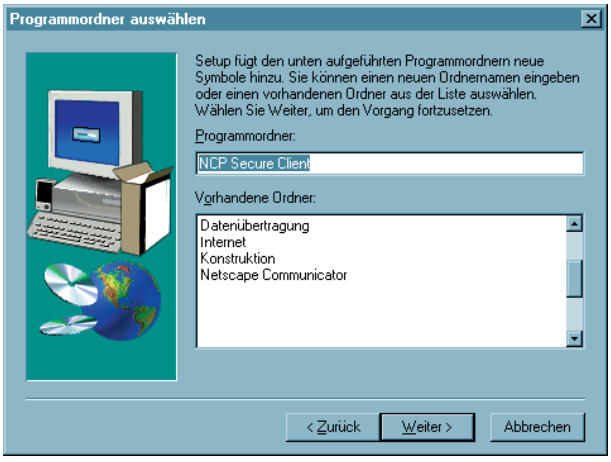


Anschließend werden die Lizenzbedingungen gezeigt. Stimmen Sie dem Vertag mit “Ja” zu, sonst wird die Installation abgebrochen.

(Die Lizenzierung erfolgt über das PDA-Gerät.)

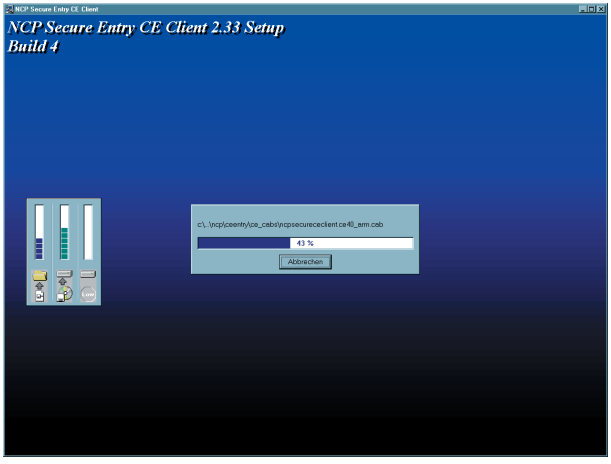
Hier bestimmen Sie das Zielverzeichnis für die Client Software.
(Standard ist Programme\ncp\ceclient).

→ *weiter nächste Seite*



Anschließend können Sie den Programmordner festlegen.

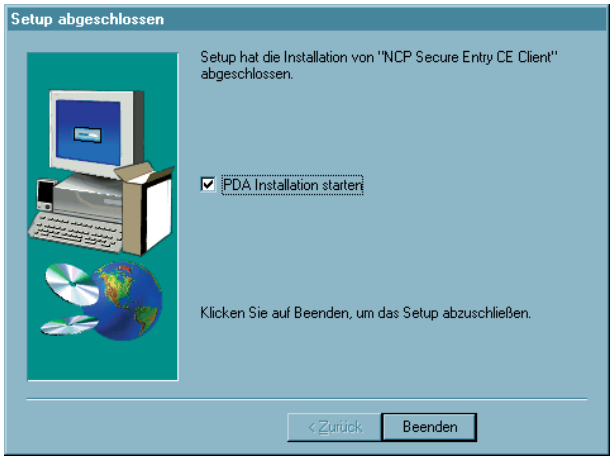
Außerdem kann das Icon auf dem Desktop angezeigt werden.



Anschließend werden die Dateien eingespielt.

(Folgen Sie den Anweisungen auf dem Bildschirm und wechseln Sie die Disketten, sofern Sie dazu aufgefordert werden.)

→ *weiter nächste Seite*



Nachdem alle benötigten Dateien von den Installationsdisketten eingespielt wurden und die Programmgruppe angelegt wurde, klicken Sie auf “Beenden”, um das Setup abzuschließen.

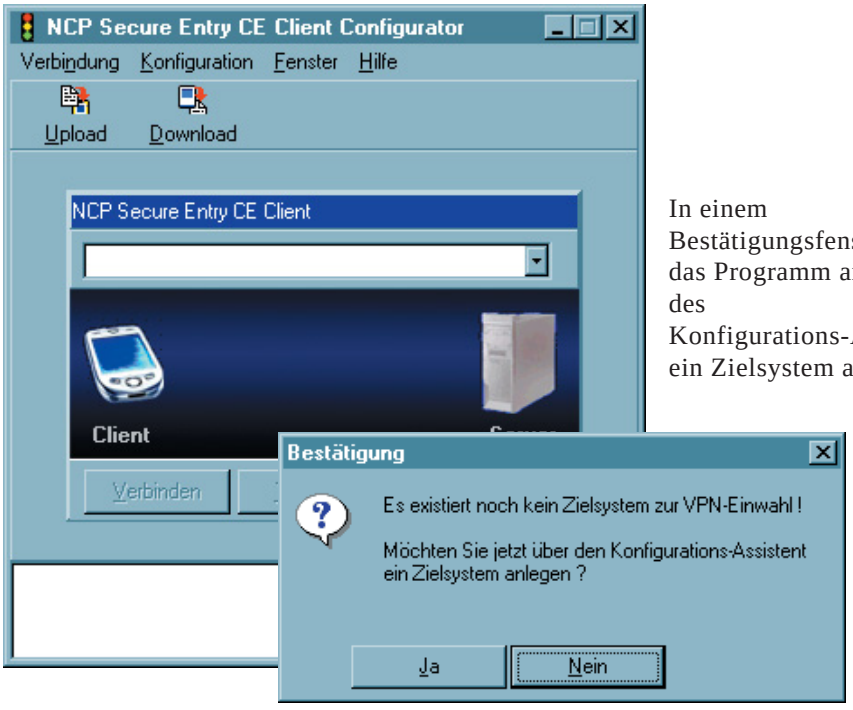
Belassen Sie die Einstellung “PDA-Installation starten”, so wird automatisch nach Beendigung der Installation der PC-Komponente die PDA-Komponente installiert. Entfernen Sie die Installationsautomatik, so kann die PDA-Komponente auch zu einem späteren Zeitpunkt installiert werden. Siehe dazu

→ *2.6 Installation der PDA-Komponente*

Im Windows-Startmenü finden Sie nach der Installation in der Programmgruppe “NCP Secure Client” das Programm “Secure Entry CE Client Configurator”.
Mit diesem Configurator erfolgt die Konfiguration der Zielsysteme, die Zusammenstellung der Profil-Einstellungen und die Übertragung der Profile auf den PDA (siehe → Client Configurator).

2.2.2 Vor der Inbetriebnahme

Nach der Installation zeigt sich der NCP Secure Entry CE Configurator wie in untenstehender Abbildung. Um den Secure Entry CE Client nutzen zu können, muss zunächst in den Profil-Einstellungen ein Eintrag für ein Zielsystem erzeugt werden, zu dem eine IPSec-Verbindung hergestellt werden kann.



In einem Bestätigungsfenster bietet das Programm an, mit Hilfe des Konfigurations-Assistenten ein Zielsystem anzulegen.

Klicken Sie auf “Ja”, so wird der Assistent gestartet. Beachten Sie dazu die Beschreibung zu “3. Client Configurator” und dort vor allem die Beschreibungen unter
– Konfiguration / Profil-Einstellungen

Zu einer weiteren Parametrisierung beachten Sie bitte
– 5. Profil-Einstellungen (Die Parameterfelder zur Konfiguration der Verbindung)

Erst nach der Einrichtung eines Zielsystems und der Übertragung der Profile zum PDA kann eine Verbindung zwischen PDA und Zielsystem hergestellt werden. Siehe dazu
– 6. Eine Verbindung herstellen

2.2.3 Übertragen der Profile und der Zertifikate

■ Profile

Vor dem Übertragen der Profile muss zunächst das Zielsystem am PC konfiguriert werden und die Profil-Einstellungen komplettiert sein. Beachten Sie deshalb zunächst die Abschnitte “Client-Configurator der PC-Komponente” und “Konfigurationsparameter” in diesem Handbuch.

Nutzen Sie die Strong Security-Version der Software mit Chipkartenleser, so beachten Sie bitte folgendes: Bevor Sie mit der PC-Komponente eine Zertifikats-Konfiguration vornehmen (siehe → Client Configurator der PC-Komponente, Konfiguration, Zertifikate), müssen die Informationen über vorhandene Chipkartenleser vom PDA auf den PC übertragen worden sein. Da diese vom NCP Client Driver erstellt werden, muss dieser vor dem Start der PC-Komponente geladen worden sein. Zur Übertragung dieser Daten ist eine bestehende ActiveSync-Verbindung notwendig.

Das Übertragen des Profile ist im Abschnitt “Upload der Profil-Einstellungen” beschrieben.

■ Zertifikate

Die mitgelieferten Test-Zertifikate von NCP, CA-Zertifikat (ncpsupportca.der) und Benutzer-Zertifikate (user1.p12 und user2.p12) befindet sich nach der Installation der beiden Software-Komponenten bereits auf dem PC und dem PDA.

Nutzen Sie eigene Soft-Zertifikate, so müssen diese vom PC via ActiveSync übertragen werden. Beachten Sie dabei, dass der PDA nur CA-Zertifikate im DER-Formats (Distinguished Encoding Rules) mit den Dateiendungen DER, CER oder CRT lesen kann! Das PEM-Format wird nicht unterstützt.

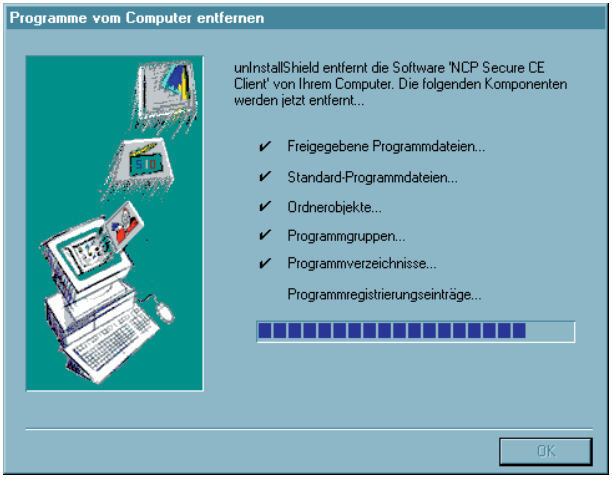
Das Zielverzeichnis auf dem PDA für das CA-Zertifikat heißt:
`\Programme\NCP Secure CE Client\CaCerts`

Das Zielverzeichnis auf dem PDA für das Benutzer-Zertifikat heißt:
`\Programme\NCP Secure CE Client\Certs`

Die Übertragung des Benutzer-Zertifikats und des CA-Zertifikats in sein Verzeichnis kann vereinfacht werden, indem der Menüpunkt “Übertrage PKCS#12-Datei zum PDA” im Configurator der PC-Komponente gewählt wird (siehe → Client Configurator der PC-Komponente, Konfiguration)

2.3 Update und Deinstallation der PC-Komponente

Wenn bei der Installation eine ältere Version der Client Software gefunden wird, haben Sie die Möglichkeit, ein Update durchzuführen. Die Profil-Einstellungen werden bei einem Update in der früher gemachten Konfiguration beibehalten.



Um die PC-Komponente zu entfernen, gehen Sie zu: “Start” →“Einstellungen” →“Systemsteuerung”. Klicken Sie nun auf “Software” und wählen Sie “NCP Secure Entry CE Client” aus der Liste. Klicken Sie dann auf den Button mit “Hinzufügen/Entfernen”. Das Uninstall Shield Programm löscht nun die Client Software von Ihrem PC.

Wichtig: Nachdem die Komponenten entfernt wurden, sind die Profil-Einstellungen des Clients erhalten geblieben, so dass es für neuere Versionen des Secure Entry CE Clients genutzt werden kann. Um die Datei vollständig vom PC zu löschen, müssen Sie per Hand vorgehen. Die Profil-Einstellungen befinden sich im Verzeichnis:

```
\Programme\ncp\ceclient\bin\ncpphone.cfg
```

2.4 Installation der PDA-Komponente

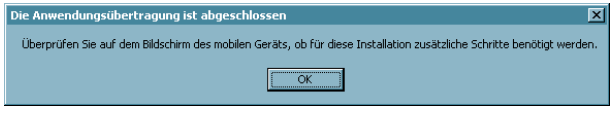
Sofern Sie die Installation der PDA-Komponente nicht automatisch nach der Beendigung der Installation der PC-Komponente vorgenommen haben, so wird die Installation der PDA-Komponente wird vom PC aus angestoßen.

Sie aktivieren im Configurator unter “Verbindung” den Menüpunkt “PDA-Installation”. Bitte achten Sie darauf, dass der Dialog “Software” von ActiveSync nicht geöffnet ist, wenn Sie das Programm PDA-Installation ausführen!

Damit wird ActiveSync aufgefordert den NCP Secure Entry CE Client auf dem mobilen Gerät zu installieren.

Als Installationsverzeichnis auf dem PDA wählen Sie das Standardverzeichnis. Klicken Sie deshalb in nebenstehendem Bild auf “Ja”.

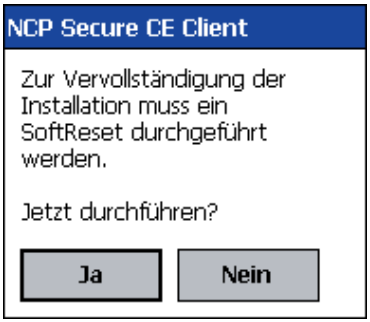
Anschließend werden die Daten für den NCP Secure Entry CE Client übertragen.



Nachdem die Datenübertragung abgeschlossen ist, überprüfen Sie den Bildschirm des mobilen Geräts:

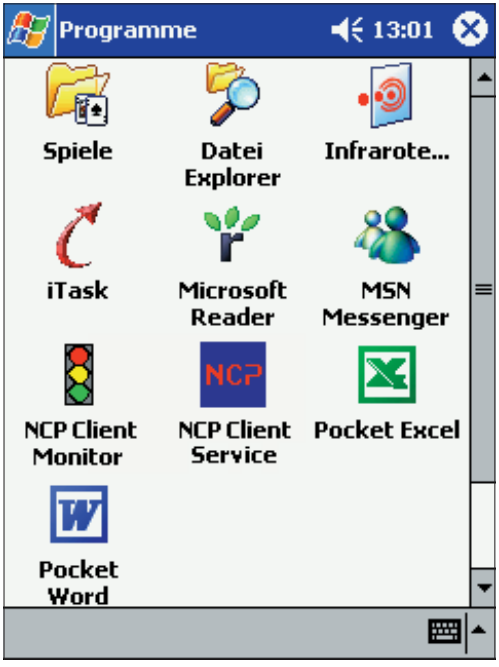
Auf dem PDA erfolgt die Installation mit dem Entpacken der übertragenen Daten.

→ *weiter nächste Seite*



Nach dem Entpacken werden Sie vom PDA zu einem Soft-Reset aufgefordert.

Damit ist die Installation der PDA-Komponente abgeschlossen.



Nach dem Soft-Reset finden Sie im Ordner der Programme die beiden Icons zu
– NCP Client Monitor
– NCP Client Service

(Vor dem Start des Monitors muss der Driver gestartet worden sein! Siehe → “Eine Verbindung herstellen” und “PDA-Monitor”.)

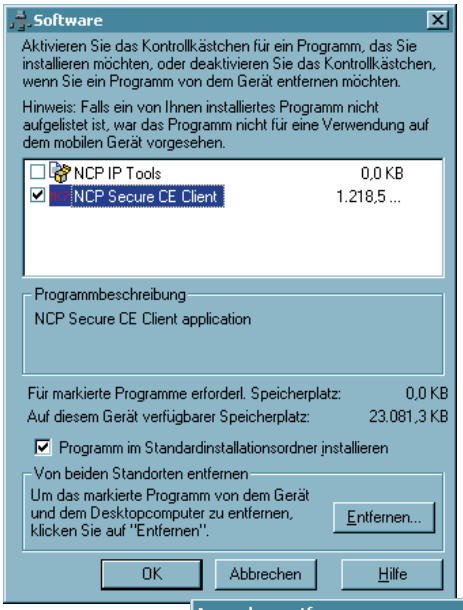
Bevor eine Verbindung aufgebaut werden kann, müssen die Profil-Einstellungen mit den konfigurierten Zielsystemen und gegebenenfalls die Zertifikats-Daten auf den PDA übertragen werden! Siehe dazu oben

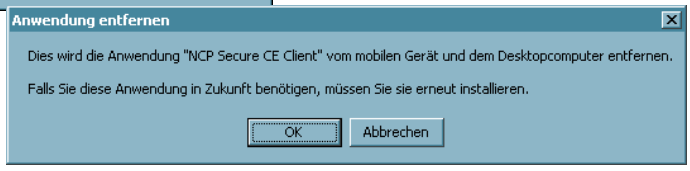
→
2.4 Übertragen der Profile und der Zertifikate

2.5 Deinstallation der PDA-Komponente

Die PDA-Komponente kann vom PC aus über ActiveSync entfernt werden, aber auch direkt am PDA.

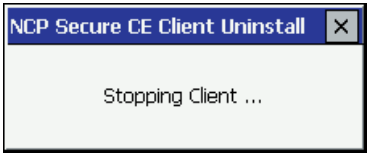
2.5.1 Deinstallation vom PC aus

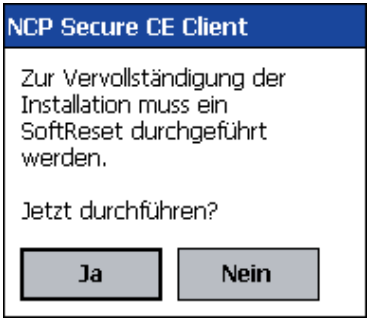




Nach dem Start von ActiveSync wählen Sie “Software”, markieren den NCP Secure CE Client wie in nebenstehendem Bild und klicken auf “Entfernen”.

Im darauf folgenden, unten stehenden Fenster klicken Sie auf OK.



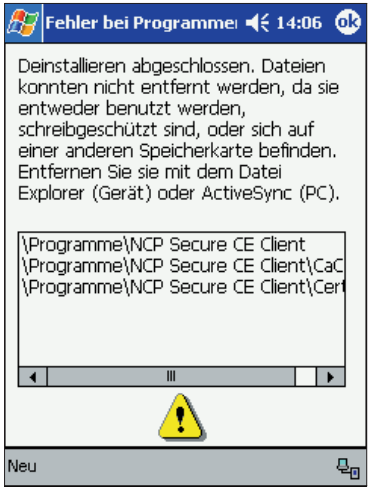


Am PDA erscheint kurzzeitig nebenstehende Meldung...

... und anschließend die Aufforderung einen Soft-Reset durchzuführen.

Klicken Sie OK, führen Sie einen Soft-Reset durch und führen danach die Deinstallation erneut durch, wie bis hierher beschrieben!

→ *weiter nächste Seite*

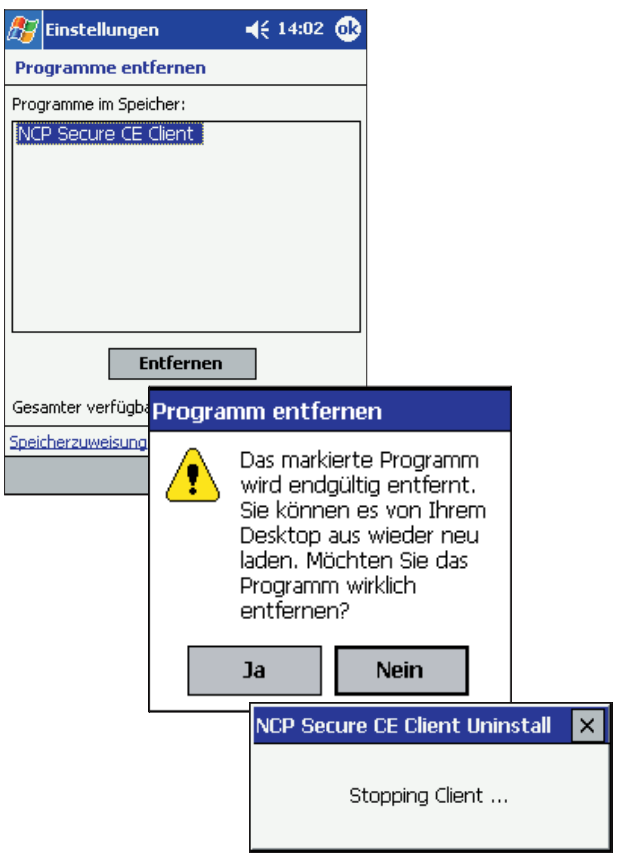


Nach dem erneuten Durchlauf ist die Deinstallation abgeschlossen.

Sollten noch Zertifikate auf dem PDA vorhanden sein (siehe nebenstehendes Bild), so müssen diese per Hand aus den angegebenen Verzeichnissen entfernt werden.

Die Profil-Einstellungen werden automatisch gelöscht.

2.5.2 Deinstallation am PDA

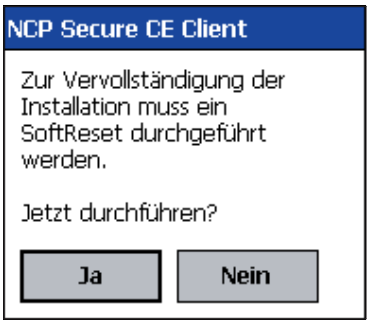


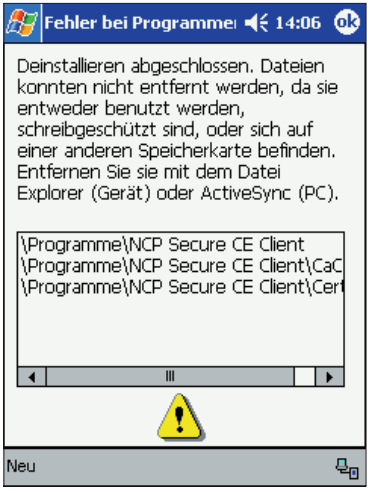
Wählen Sie im Startmenü des PDAs “Einstellungen – System – Programme entfernen”, selektieren Sie das Programm NCP Secure CE Client und betätigen Sie den Entfernen-Button.

Die Sicherheitsabfrage bestätigen Sie mit “Ja”.

Der Client wird gestoppt und ...

→ *weiter nächste Seite*





... und anschließend erscheint die Aufforderung einen Soft-Reset durchzuführen.

Klicken Sie OK, führen Sie einen Soft-Reset durch und führen danach die Deinstallation erneut durch, wie bis hierher beschrieben!

Nach dem erneuten Durchlauf ist die Deinstallation abgeschlossen.

Sollten noch Zertifikate auf dem PDA vorhanden sein (siehe nebenstehendes Bild), so müssen diese per Hand aus den angegebenen Verzeichnissen entfernt werden.

Die Profil-Einstellungen werden automatisch gelöscht.

2.6 Erweiterte Installation

Eine erweiterte Installation und Konfigurationsänderungen können mit den Programmen AUTOINSTALL.EXE am PC und NCPCONFIG.EXE am PDA vorgenommen werden.

2.6.1 Funktionen von AUTOINSTALL.EXE

Im Installationsverzeichnis der PC-Komponente befindet sich unter \ncp\ceclient\bin\ die Datei AUTOINSTALL.RTF. Diese Datei beschreibt den Einsatz des Programms AUTOINSTALL.EXE, das sich ebenfalls in diesem Verzeichnis befindet.

Mit AUTOINSTALL.EXE können folgende Funktionen ausgeführt werden:

- ☐ Installation
- ☐ Deinstallation
- ☐ Profilübertragung
- ☐ Lizenzänderungen
- ☐ Einstellungsänderungen

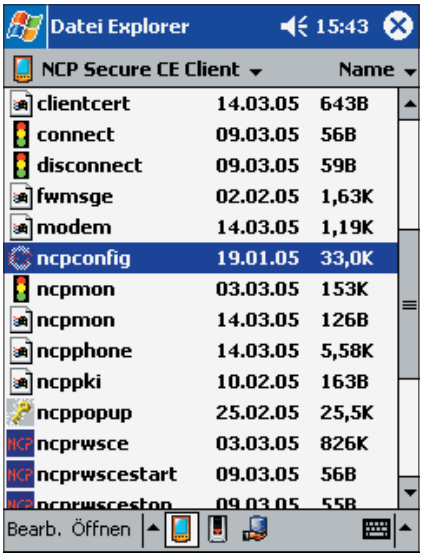
2.6.2 Autostart des NCP-Diensts am PDA

Der NCP-Dienst muss nach der Installation und nach einem Softreset nicht unbedingt manuell aus dem Programmordner gestartet werden. Der Treiber wird automatisch gestartet, wenn das Programm ncprwscestart aus dem Installationsverzeichnis am PDA in das (anzulegende) Autostart-Verzeichnis unter Windows kopiert wurde. Dies ist mit AUTOINSTALL.EXE einstellbar.

2.7 Konfigurationsprogramme am PDA

Die Basiskonfiguration erfolgt über die Profil-Einstellungen am Configurator der PC-Komponente. Am PDA können jedoch darüber hinaus weitere Einstellungen vorgenommen werden, die gerätespezifisch von Bedeutung sind. Dafür steht das Konfigurationsprogramm NCPCONFIG.EXE und ein Popup-Menü zur Verfügung.

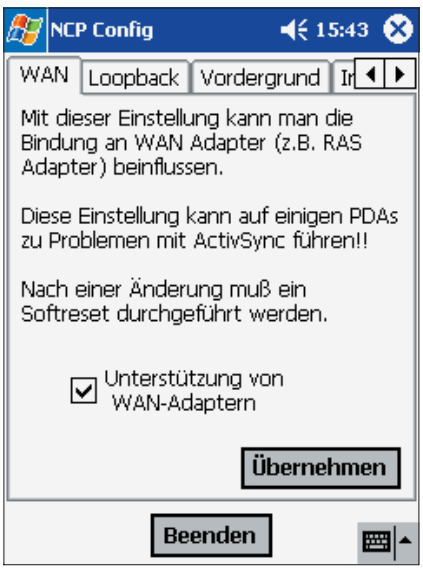
2.7.1 Funktionen von NCPCONFIG.EXE



Das Programm NCPCONFIG.EXE steht im Installationsverzeichnis (normalerweise: \Programme\NCP Secure CE Client\) auf dem PDA und kann dort von Hand gestartet werden.

Nach Aufruf des Programms werden am PDA fünf Karteikarten eingeblendet, die Informationen zu Einstellungsmöglichkeiten und Gerätekonfigurationen zeigen.

■ **WAN**



Mit NCPCONFIG.EXE kann die Unterstützung von WAN-Adaptern am PDA konfiguriert werden. Im Auslieferungszustand ist der WAN-Support eingeschaltet.

Nur bei aktivem WAN-Support ist auch die Firewall-Funktionalität für den RAS-Adapter gegeben. WAN-Support wird außerdem benötigt, um IPSec-Tunneling über RAS-Verbindungen nutzen zu können. Alle anderen Verbindungsarten über den RAS-Adapter benötigen keinen WAN-Support.

Voraussetzung für den WAN-Support ist Pocket PC 2002 mit EUU3 oder ein neueres System auf dem PDA. Nach der Aktivierung und einem anschließenden Softreset muss eine

ActivSync-Verbindung (über USB oder seriell) zum PC weiterhin möglich sein. Ist dies nicht der Fall, so funktioniert der WAN-Support nicht und muss mit NCPCONFIG.EXE abgeschaltet werden. Nach einem erneuten Softreset sollte ActiveSync wieder funktionsfähig sein. NCP empfiehlt den WAN-Support nur dann zu deaktivieren, wenn Probleme auftreten.

■ Loopback (Betrieb ohne virtuellen Netzwerkadapter)

Auf Windows CE-Geräten der PocketPC Platform wird der virtuelle Netzwerkadapter "NCP Loopback" bei der Neuinstallation standardmäßig deaktiviert. Dadurch sind Profil-Einstellungen mit NCP Dialer und teilweise auch automatischem Modus nicht einsetzbar. Diese Profile werden am PDA nach einem Upload vom Configurator automatisch ausgeblendet. Dazu erscheint im Log-Fenster ein Text, der darauf hinweist, dass die Profile nicht kompatibel zur aktuellen Einstellung am PDA sind.

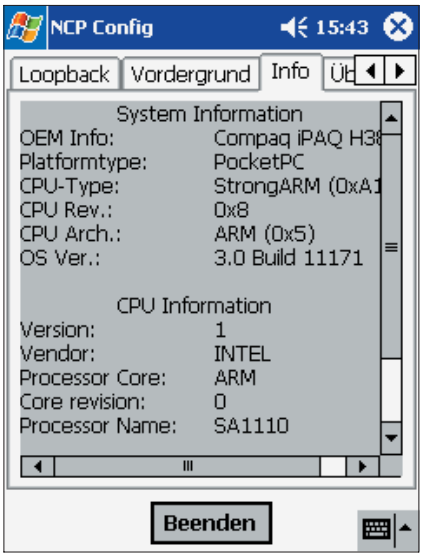
Der Betrieb ohne virtuellen Netzwerkadapter ist auf Geräten mit PocketPC 2003 Phone Edition zu empfehlen.

■ Vordergrund

Bei einer Änderung des Verbindungsstatus erscheint der Monitor im Vordergrund, wenn dies über die Benutzeroberfläche in NCPCONFIG.EXE am PDA eingeschaltet wurde. Dies kann dann sinnvoll sein, wenn zum Beispiel schnell auf einen Verbindungsabbruch reagiert werden soll.

Der Monitor muss nach dem Ändern dieser Einstellung neu gestartet werden.

Info



Das Info-Feld zeigt schnell und übersichtlich die wichtigsten Informationen zum System und zur CPU.

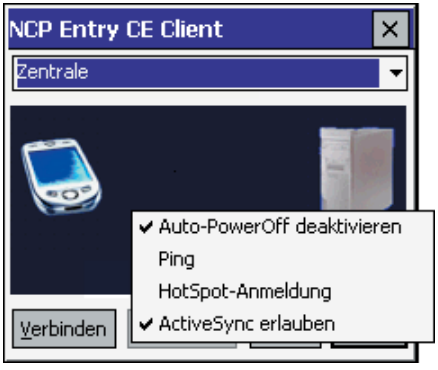
Über

In diesem Feld werden Informationen zum Konfigurationsprogramm NCPCONFIG gezeigt.

2.7.2 Popup-Menü

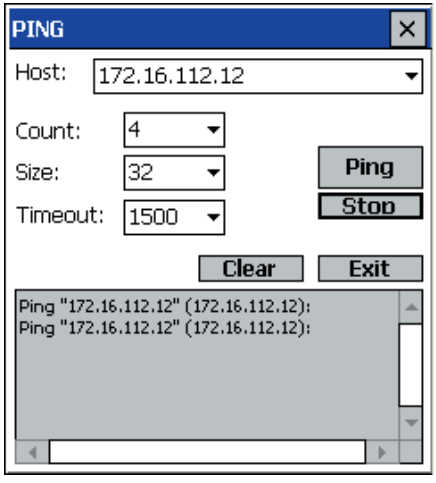
Das Popup-Menü wird aktiviert, indem im grafischen Feld des Monitors mit dem Pen ein Tab-and-Hold ausgeführt wird.

- **Auto-PowerOff**



Standardmäßig ist die Auto-PowerOff-Funktion deaktiviert, d.h. der PDA versetzt sich nicht automatisch in den Stromsparmodus, wenn eine VPN-Verbindung steht und kein Datenverkehr stattafindet.

- **Ping**



Der CE Client enthält ein integriertes Ping-Utilty-Programm um ICMP-Echo_Requests (Ping) abzusenden. Der Aufruf erfolgt mit Klick auf den Menüpunkt im Popup-Programm. Das Programm PING.EXE befindet sich im Installationsverzeichnis der Client Software und ist auch stand-alone verwendbar.

HotSpot-Anmeldung

Mit Klick auf diesen Menüpunkt erfolgt eine automatische HotSpot-Anmeldung. Damit der remote Client in jeder Phase des Verbindungsaufbaus auch in WLANs mit HotSpots ohne Zutun des Benutzers gegenüber jeglichen Attacken geschützt ist, wurde die Firewall fest in die Client Software integriert. Sie verfügt über intelligente Automatismen für eine sichere HotSpot-Anmeldung.

Voraussetzungen:

Der PDA muss sich mit aktivierter WLAN-Karte im Empfangsbereich eines HotSpots befinden. Die Verbindung zum HotSpot muss hergestellt und eine IP-Adresse für den Wireless-Adapater muss zugewiesen sein.

Die Firewall des NCP Secure Clients sorgt dafür, dass lediglich die IP-Adresszuweisung per DHCP erfolgen darf, weitere Zugriffe ins WLAN bzw. vom WLAN werden unterbunden. Die Firewall gibt dynamisch die Ports für http bzw. https für die Anmeldung bzw. Abmeldung am HotSpot frei. Dabei ist nur Datenverkehr mit dem HotSpot Server des Betreibers möglich. Ein öffentliches WLAN wird auf diese Weise ausschließlich für die VPN-Verbindung zum zentralen Datennetz genutzt. Direkter Internet-Zugriff ist ausgeschlossen. Damit die Anmeldeseite des HotSpots im Browser geöffnet werden kann, muss eine eventuelle Proxy-Konfiguration deaktiviert werden.

Derzeit unterstützt die HotSpot-Anmeldung des Clients ausschließlich HotSpots, die mit einer Umleitung (Redirect) einer Anfrage mit einem Browser auf die Anmeldeseite des öffentlichen WLAN-Betreibers arbeiten (z.B. T-Mobile oder Eurospot).

Funktionsbeschreibung:

Sind obige Voraussetzungen erfüllt, kann der Benutzer im Hauptmenü “Verbindung” den Menüpunkt “HotSpot-Anmeldung” aktivieren. Der Client sucht daraufhin automatisch den HotSpot und öffnet die Website zur Anmeldung im Standard-Browser. Nach erfolgreicher Eingabe der Zugangsdaten und Freischaltung durch den Betreiber, kann die VPN-Verbindung z.B. zur Firmenzentrale aufgebaut und sicher wie an einem Büroarbeitsplatz kommuniziert werden.

Dabei ist nur Datenverkehr mit dem HotSpot-Server des Betreibers möglich. Nicht angeforderte Datenpakete werden abgewiesen. Die direkte Kommunikation zum Internet unter Umgehung des VPN-Tunnels ist ausgeschlossen, aufgrund der bereits beschriebenen dynamischen Firewall-Regeln, die von der integrierten Personal Firewall des Clients selbständig gesetzt werden.

Sollte vom Client keine HotSpot-Anmeldung durchgeführt werden, wird dies durch die Meldung “HotSpot konnte nicht gefunden werden” mitgeteilt. Für einen solchen Fall ist zu klären, ob über diesen HotSpot-Betreiber ein generelles Problem in Verbindung mit den von NCP implementierten Mechanismen besteht.

■ ActiveSync erlauben

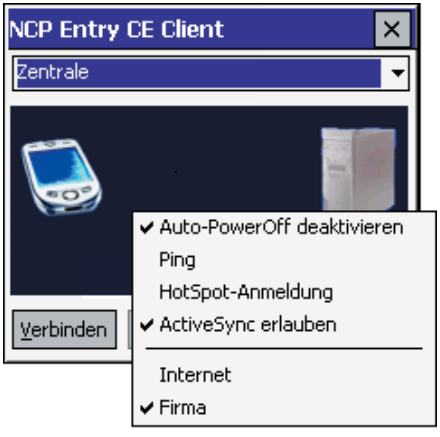
Die (globale) Firewall muss bei einer Direktverbindung (über USB, seriell oder Infrarot) für ActiveSync freigeschaltet werden. Dies erfolgt in den Firewall-Einstellungen des Configurators unter “Optionen – ActiveSync-Verbindungen (TCP 990, 999, 5678, 5679) zulassen”. Diese Einstellung kann auch am PDA über den Menüpunkt “ActiveSync erlauben” im Popup-Programm vorgenommen werden, wenn die (globale) Firewall aktiv ist.

Wird ActiveSync über Netzwerk betrieben (LAN oder WLAN), so muss zusätzlich manuell eine eigene Firewall-Regel für die Namensauflösung (DNS/WINS) erstellt werden.

ActiveSync-Verbindungen werden als normale TCP-Verbindungen von der Link Firewall behandelt. Obwohl ActiveSync die TCP-Verbindung in beide Richtungen (PC ⟷ PDA) etabliert, wird bei aktiviertem Stateful Inspection-Filter in der Link Firewall zugelassen. Die Verbindung wird gesperrt, wenn “Ausschließlich Kommunikation im Tunnel zulassen” aktiviert ist.

Auch komprimierte Verbindungen des RAS-Dialers können vom Client als normaler IP-Verkehr überwacht werden, da sowohl die Kompression (CCP) als auch die VanJacobson-IP-Header-Kompression (im IPCP) nicht mehr ausgehandelt werden.

■ PocketPC Connection Manager



In den Profil-Einstellungen kann im Parameterfeld “Grundeinstellungen” das Verbindungsmedium “PocketPC Connection Manager” für PocketPC Plattformen eingestellt werden. Dieses Verbindungsmedium ist ideal für Geräte mit integriertem Telefon (MDA). Während eine GPRS-Verbindung besteht, kann gleichzeitig telefoniert werden. Der PocketPC Connection Manager übernimmt dabei automatisch das Parken der GPRS-Verbindung. Bei der Konfiguration eines Profils für diese Anwendung ist darauf zu achten, dass die Timeout-Spanne genügend groß gewählt wird, bzw. der Timeout deaktiviert ist und Dead Peer Detection (DPD) in den IPSec-Einstellungen deaktiviert ist.

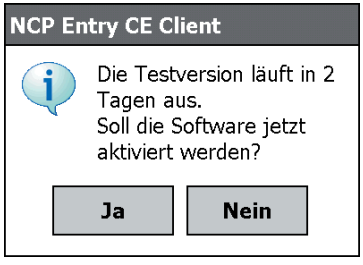
Bei Einsatz dieses Verbindungsmediums, nur sinnvoll bei deaktiviertem Loopback-Adapter, kann man das Zielnetzwerk auswählen: Internet oder Firmennetz. Diese Einstellung kann auch am PDA über das Popup-Menü geändert werden.

Bei Verwendung dieses Medientyps wird der PocketPC Connection Manager dazu veranlasst eine Verbindung (ins Internet oder Firmennetz) aufzubauen. D.h. der ConnectionManager wird automatisch eine RAS-Verbindung auswählen und aufbauen, oder er erkennt eine schon vorhandene LAN-Karte und baut keine weitere Verbindung auf.

Unter “Start / Einstellungen / Verbindungen / Verbindungen”, kann mit Bordmitteln die entsprechende Internet- und Firmenverbindung konfiguriert werden. Ist der virtuelle Adapter aktiv, so ist für den sinnvollen Einsatz des Connection Managers genauere projektspezifische Kenntnis der Umgebung nötig.

2.8 Lizenzierung über den Aktivierungs-Dialog

Die Client-Software wird zunächst immer als Testversion installiert, sofern noch keine Client-Software installiert wurde oder aber mit einer bereits installierten älteren Version noch keine Software-Aktivierung stattgefunden hat. Dies gilt auch dann, wenn die ältere Version bereits lizenziert wurde. In diesem Fall wird die ältere Version auf den Status einer Testversion zurückgesetzt, und die Lizenzdaten der neueren Version (Aktivierungs- bzw. Lizenzschlüssel und Seriennummer) müssen innerhalb von 30 Tagen nochmals über den Aktivierungs-Dialog eingegeben werden.



Der Aktivierung-Dialog wird geöffnet über das Popup-Menü “Aktivierung” (Bild links) oder mit Druck auf “Ja”, sobald die Meldung (links mitte) nach Start des Dienstes NCP Client Service erscheint.

Die verbliebene Zeitdauer bis zur Software-Aktivierung, d.h. die Gültigkeitsdauer der Testversion, wird in der Lizenz-Information (Bild links unten) angezeigt. Um eine zeitlich unbegrenzt gültige Vollversion nutzen zu können, muss die Software mit dem erhaltenen Lizenzschlüssel und der Seriennummer im freigeschaltet werden.

Dies kann erfolgen nach Druck auf den Pfeil-Button rechts oben in der Lizenz-Information (Bild links unten).

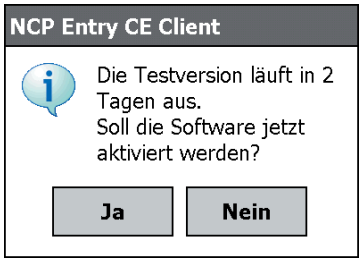
Im folgenden können die Lizenzdaten wahlweise online oder offline über einen Assistenten eingegeben werden.

In der Offline-Variante muss eine Datei, die nach Eingabe von Lizenzschlüssel und Seriennummer erzeugt wird, an den NCP Web Server geschickt werden und der daraufhin auf der Website angezeigte Aktivierungsschlüssel notiert werden. Dieser Aktivierungsschlüssel kann zu einem späteren Zeitpunkt im Lizenzierungsfenster des Monitormenüs eingegeben werden.

In der Online-Variante werden die Lizenzierungsdaten über einen Assistenten unmittelbar nach Eingabe an den Web Server weitergegeben und die Software damit unverzüglich freigeschaltet.

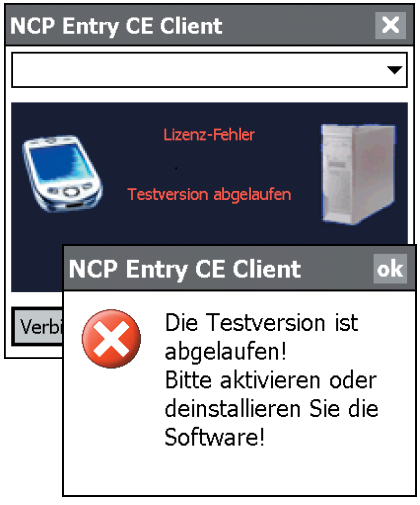
2.8.1 Gültigkeitsdauer der Testversion

Die Gültigkeitsdauer der Testversion beträgt 30 Tage. Ohne Software-Aktivierung bzw. Lizenzierung ist nach dieser Zeitspanne kein Verbindungsaufbau mehr möglich.



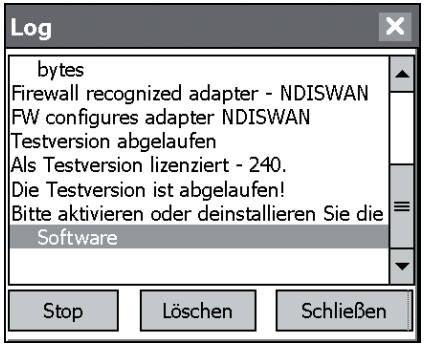
Ab dem Zeitpunkt der Installation wird bei jedem Start des Dienstes NCP Secure Service oder jedem Verbindungsaufbau die verbliebene Gültigkeitsdauer der Test-Software ausgegeben.

Die Software kann während der Testphase genutzt werden, nachdem der automatisch eingeblendete Aktivierungsdialog mit “Nein” beendet wird.



Ist die Testphase abgelaufen, können mit der Entry Client Software nur noch Verbindungen innerhalb von vier Minuten (240 s, siehe unten Log-Fenster) zu Zielsystemen aufgebaut werden, die der Software-Aktivierung/-Lizenzierung dienen. So kann eines der Profile des Entry Clients dazu verwendet werden, eine Internet-Verbindung zum Zweck der Lizenzierung aufzubauen.

Bei einer abgelaufenen Testversion können Sie den Aktivierungs-Dialog mit Druck auf den ok-Button starten (siehe folgende Seite).

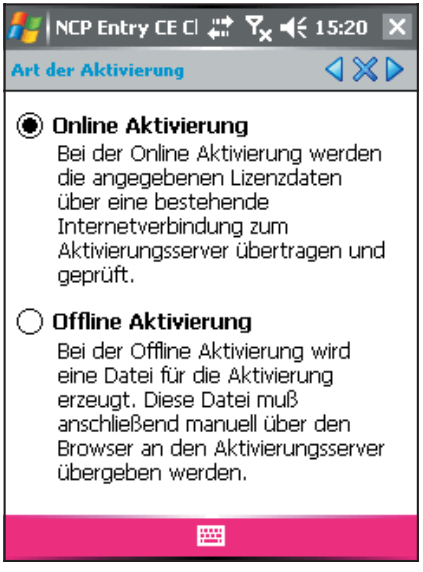


2.8.2 Software-Aktivierung

Spätestens wenn die Testphase abgelaufen ist, muss die Software aktiviert oder deinstlliert werden. Zur Aktivierung selektieren Sie im Popup-Menü den Menüpunkt “Aktivierung”.

Sie können hier ablesen um welche Software-Version es sich handelt und wie die Software lizenziert ist, d.h. dass die Testversion abgelaufen und die Software noch nicht aktiviert/lizenziert ist.

Zur Aktivierung der Software drücken Sie auf den Pfeil-Button rechts oben.



Im folgenden Fenster können Sie zwischen einer Online- und einer Offline-Variante wählen.

In der Offline-Variante muss eine Datei, die nach Eingabe von Lizenzschlüssel und Seriennummer erzeugt wird, an den NCP Web Server geschickt werden und der daraufhin auf der Website angezeigte Aktivierungsschlüssel notiert werden. In der Online-Variante werden die Lizenzierungsdaten über einen Assistenten unmittelbar nach Eingabe an den Web Server weitergegeben und die Software damit unverzüglich freigeschaltet.

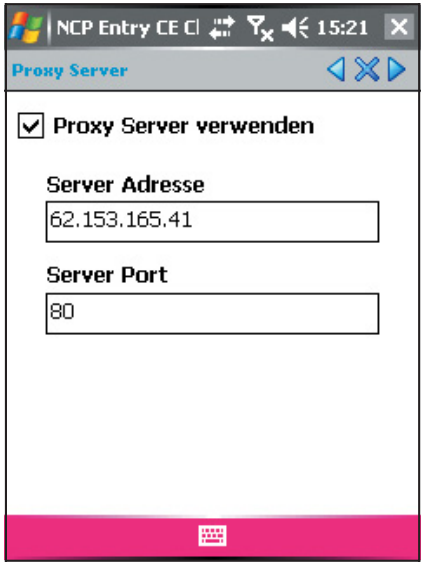
Nach der Wahl der Aktivierungsart können die Lizenzdaten in die dafür vorgesehenen Felder eingetragen werden.

Drücken Sie anschließend die rechte Pfeil-Button.

Online-Variante

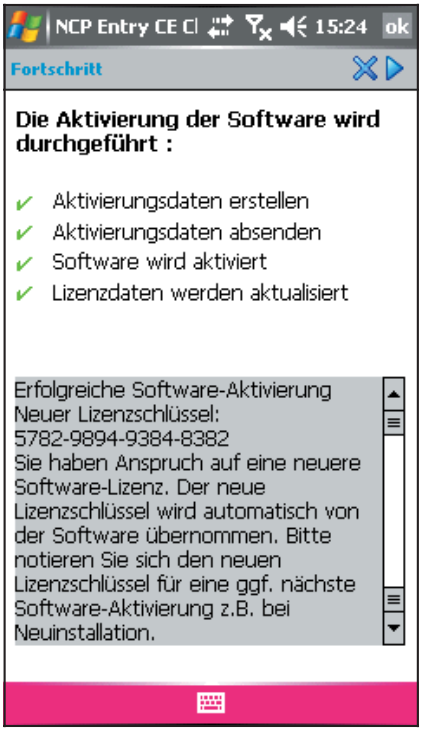
Bei der Online-Aktivierung werden die Lizenzdaten über eine Internetverbindung zum NCP Aktivierungs-Server übertragen. Diese Internetverbindung kann über den DFÜ-Dialer hergestellt (via PocketPC Connection Manager oder Modem/Handy) werden.

Zunächst wird die Verbindung hergestellt, um anschließend über den Aktivierungsdialog den Assistenten zu starten.



Dabei ist darauf zu achten, dass bei aktivierter Firewall der Port 80 (für HTTP) freigeschaltet ist. (Sollte ein Proxy Server im Betriebssystem konfiguriert sein, kann dessen Adresse übernommen werden.)

Drücken Sie anschließend die rechte Pfeil-Button.



Die Software-Aktivierung erfolgt automatisch in der angegebenen Reihenfolge.

Sobald der Aktivierungs-Server erkennt, dass Ihnen eine neuere Software-Lizenz zusteht und der Lizenzschlüssel zur installierten Software passt, wird mit der Online-Aktivierung automatisch der neue Lizenzschlüssel übertragen (Lizenz-Update) und damit die neuen Features der Software freigeschaltet.

Notieren Sie sich den neuen Schlüssel für eine eventuelle Neuinstallation.

Nach Abschluss der Aktivierung kann im Fenster für die Lizenz-Informationen abgelesen werden, dass es sich bei der eingesetzten Software um eine korrekt aktivierte Vollversion handelt.

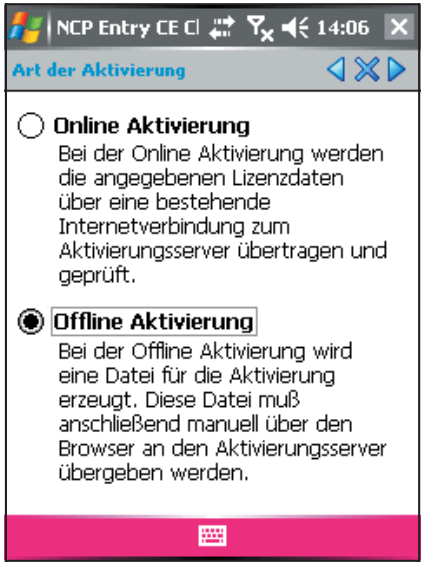
Schließen Sie hier den Dialog! Nur so ist gewährleistet, dass der Lizenzschlüssel korrekt übernommen wird.

Offline-Variante

Die Offline-Variante wird in zwei Schritten durchgeführt. Im ersten Schritt muss eine Datei, die nach Eingabe von Lizenzschlüssel und Seriennummer erzeugt wird, an den NCP Web Server geschickt werden. Die URL lautet:

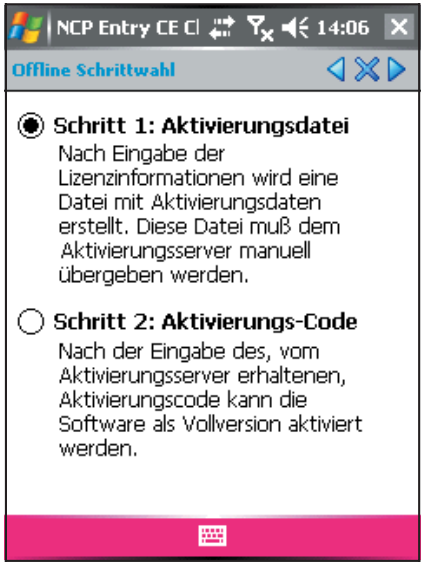
`http://www.ncp.de/deutsch/services/license`

Auf der Website wird daraufhin ein Aktivierungsschlüssel angezeigt, der notiert werden muss, um im zweiten Schritt, der auch zu einem späteren Zeitpunkt vorgenommen werden kann, im Lizenzierungsfenster des Monitormenüs eingegeben werden zu können.



Die Offline-Variante wird über den Aktivierungs-Dialog gestartet und im ersten Fenster selektiert.

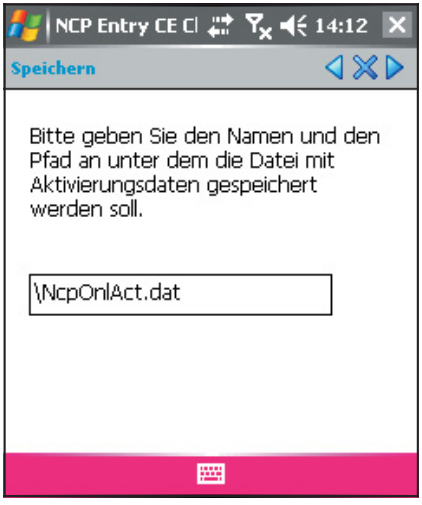
Drücken Sie anschließend die rechte Pfeil-Button.



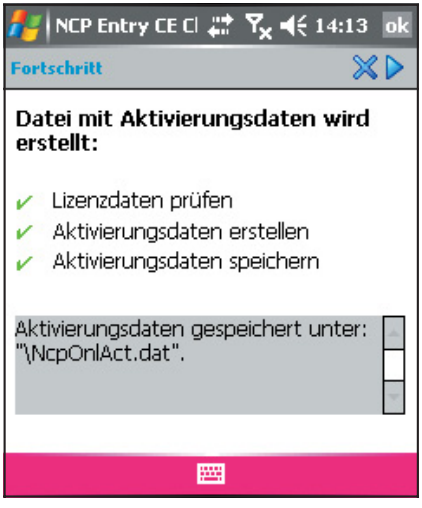
Im zweiten Fenster werden die beiden Schritte der Offline-Aktivierung erklärt. Der erste Schritt, die Erstellung der Aktivierungsdatei, ist automatisch selektiert.

Drücken Sie anschließend die rechte Pfeil-Button.

Im folgenden Fenster geben Sie die Lizenzdaten ein und klicken auf “Weiter” ...



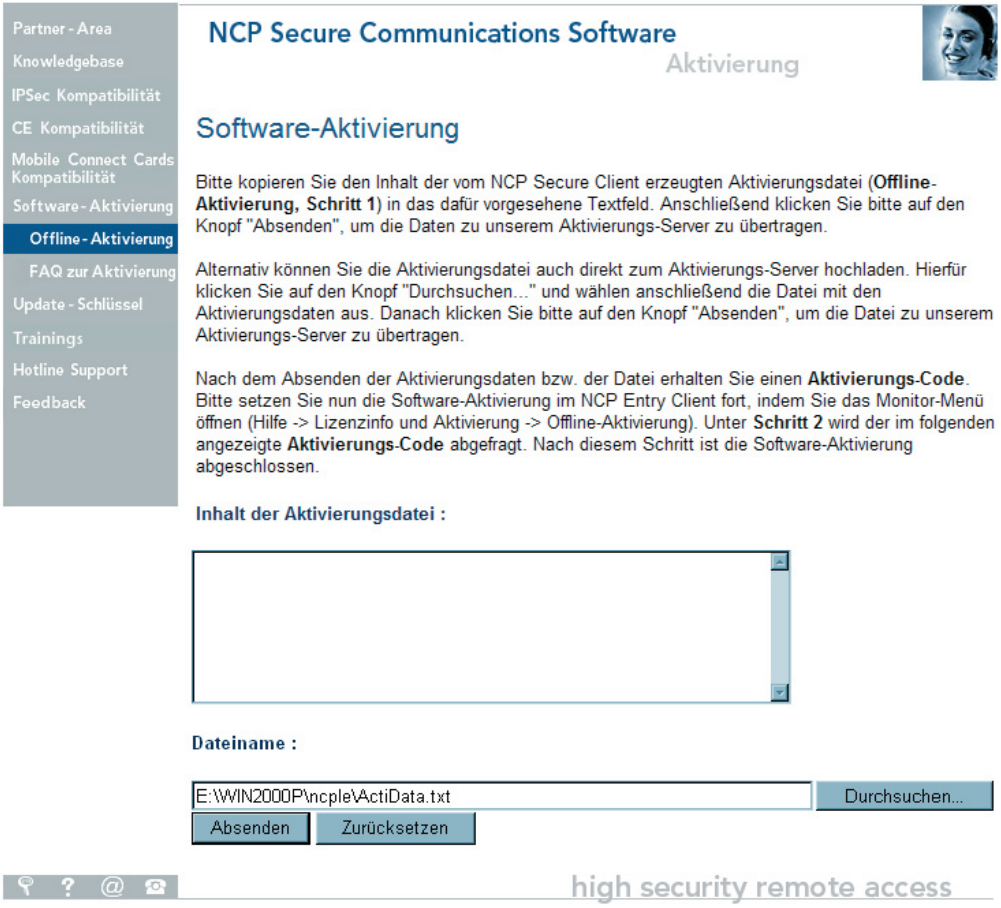
Geben Sie nun Name und Pfad für die Aktivierungsdatei ein (z.B. auf dem Desktop). Standardmäßig wird das Installationsverzeichnis der Software und der Name Act.dat (mit Seriennummer) eingesetzt.



Nun wird die Aktivierungsdatei erstellt, die an den Aktivierungs-Server übergeben werden muss.

Dazu muss die NCP Website aufgerufen werden:

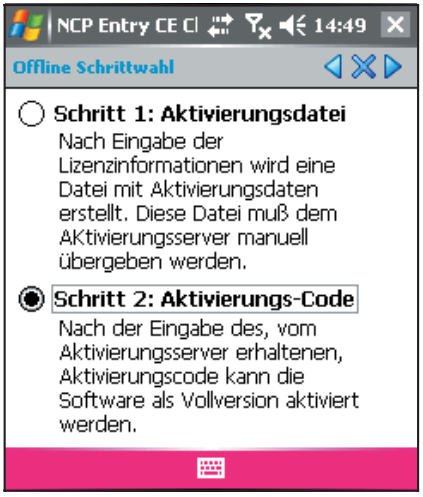
http://www.ncp.de/deutsch/services/license



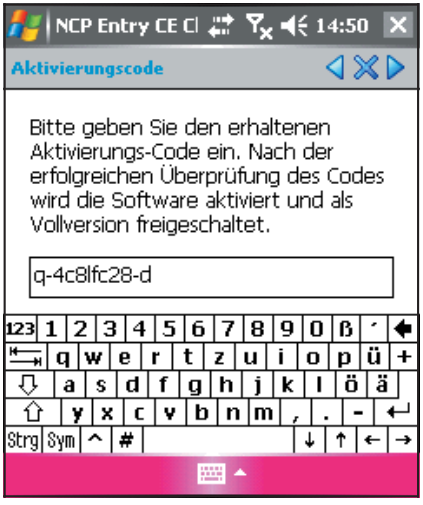
Die Datenübergabe von der Aktivierungsdatei an den Aktivierungs-Server kann auf zweierlei Weise erfolgen. Entweder kopieren Sie den Inhalt der Aktivierungsdatei mit Copy&Paste, nachdem Sie die Aktivierungsdatei mit dem Notepad (ASCII-Editor) geöffnet haben, in das auf der Website geöffnete Fenster “Inhalt der Aktivierungsdatei” oder Sie klicken auf den Button “Durchsuchen” und selektieren die Aktivierungsdatei. Anschließend klicken Sie auf “Absenden”.

Daraufhin wird der Aktivierungs-Code generiert und auf der Website angezeigt. Notieren Sie sich den Aktivierungs-Code und setzen Sie die Aktivierung fort unter dem Menüpunkt “Hilfe / Lizenzinfo und Aktivierung”, indem Sie in der Offline-Variante den zweiten Schritt der Aktivierung ausführen.

Sollte der Aktivierungs-Server erkennen, dass Ihnen eine neuere Software-Lizenz zusteht und der Lizenzschlüssel zur installierten Software passt, wird mit der Online-Aktivierung automatisch der neue Lizenzschlüssel angezeigt. Wenn Sie die neuen Features aktivieren möchten, notieren Sie sich den neuen Lizenzschlüssel, führen Sie die Aktivierung zu Ende und verwenden anschließend den neuen Lizenzschlüssel. (Bitte beachten Sie dazu den Abschnitt “Szenarien” am Ende dieses Kapitels.)

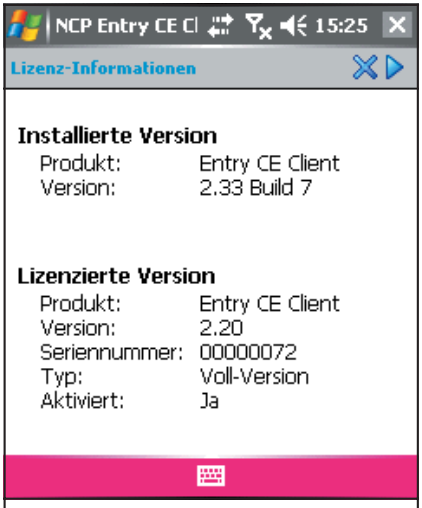


Der zweite Schritt der Offline-Variante wird erneut über den Aktivierungs-Dialog angestoßen. Nachdem die Offline-Variante gewählt wurde, selektieren Sie den zweiten Schritt.



Daraufhin öffnet sich ein Fenster zur Eingabe des Aktivierungs-Codes. Wenn Sie ihn eingetragen haben, drücken Sie den rechten Pfeil-Button.

Mit diesem Fenster wird die Offline-Aktivierung abgeschlossen.



Nach Abschluss der Aktivierung kann im Fenster für die Lizenzdaten abgelesen werden, dass es sich bei der eingesetzten Software um eine korrekt aktivierte Vollversion handelt.

Die Nummer der Software-Version und der lizenzierten Version können sich unterscheiden, sofern die Lizenzierung nur für eine ältere Version gültig ist.

Sollten Sie vom Aktivierungs-Server während der Offline-Aktivierung einen neuen Lizenzschlüssel erhalten haben (siehe oben bei Anzeige des Aktivierungs-Codes), so geben Sie diesen Lizenzschlüssel für ein Lizenz-Update ein, nachdem Sie den Pfeil-Button gedrückt haben.

In diesem Fenster (links) geben Sie den neuen Lizenzschlüssel ein und klicken auf den rechten Pfeil-Button.

Die Lizenzdaten werden geprüft und übernommen.

Klicken Sie “Fertigstellen” wenn die Prüfung abgeschlossen ist.

2.8.3. Betriebssystem des mobilen Geräts

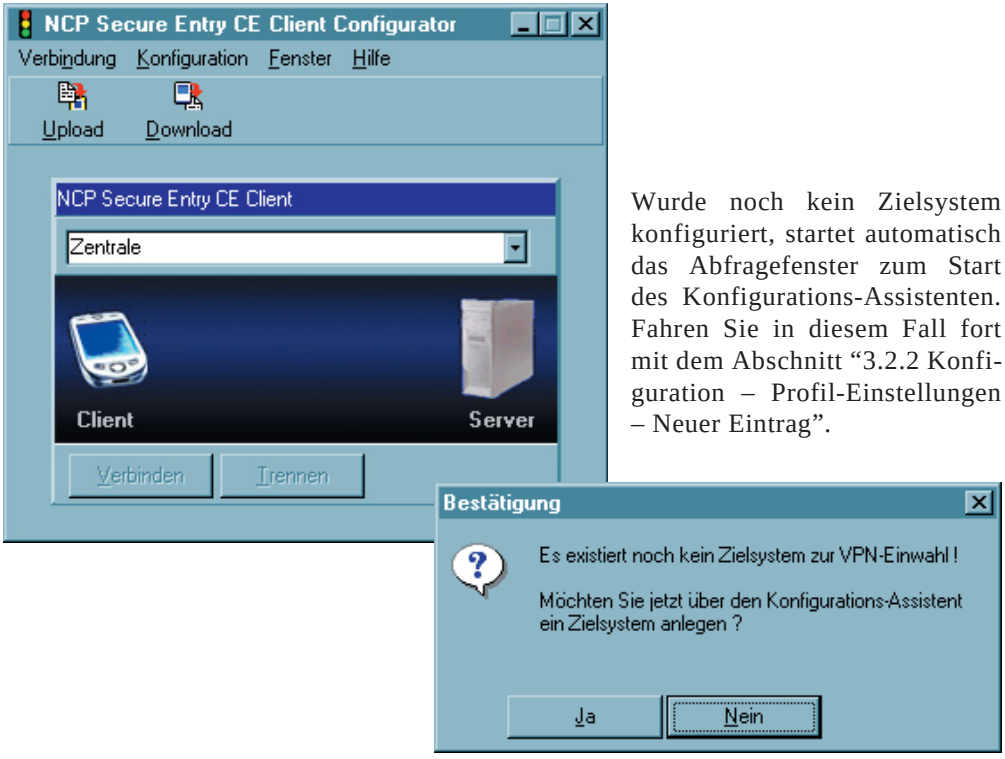
Mit der Version 2.33 des NCP Secure Entry CE Clients wird neben den bereits zuvor verfügbaren Windows Mobile Betriebssystemen auch Windows Mobile 6 unterstützt.

Die Installation der Client Software 2.33 unter Microsoft Windows Mobile 6 erfordert einen Lizenzschlüssel für diese Version. Unter einem älteren Lizenzschlüssel kann diese Software nicht betrieben werden. Die Eingabe eines älteren Lizenzschlüssels verursacht eine Fehlermeldung.

Die Aktivierung der Client Software unter Windows Mobile 6 setzt voraus, dass Sie über einen Lizenzschlüssel verfügen, der mindestens der Version 2.3 entspricht. Sofern Ihnen ein kostenfreies Update auf die Version 2.3 zur Verfügung steht, erhalten Sie den zugehörigen Lizenzschlüssel, wenn Sie eine Software-Aktivierung durchführen. Für ein kostenpflichtiges Update auf die Version 2.3 wenden Sie sich bitte an Ihren Reseller.

3. Client Configurator

Wenn die Software nach den Standardvorgaben installiert wurde, kann der Configurator der PC-Komponente über das Start-Menü “Programme / NCP Secure Client / Secure Entry CE Client Configurator” aktiviert werden. Damit öffnet sich das Fenster des Configurators auf dem Bildschirm, sofern bereits ein Zielsystem konfiguriert wurde (siehe oben → 2.3 Vor der Inbetriebnahme).



Wurde noch kein Zielsystem konfiguriert, startet automatisch das Abfragefenster zum Start des Konfigurations-Assistenten. Fahren Sie in diesem Fall fort mit dem Abschnitt “3.2.2 Konfiguration – Profil-Einstellungen – Neuer Eintrag”.

Hinweis: Wenn der Configurator zum Icon verkleinert wird, erscheint er als Ampellicht in der Taskleiste.

Der Configurator hat 4 wichtige Funktionen:

☑ die Definition und Konfiguration der Profile zur Anwahl an ein Zielsystem.

☑ die Erstellung der IPSec- und der Zertifikats-Konfiguration.

☑ das Kopieren der Profil-Einstellungen auf das PDA-Gerät.

☑ das Herunterladen der Profil-Einstellungen vom PDA, um Modifizierungen vornehmen zu können.

3.1 Die Oberfläche des Client Configurators

Der Client Configurator besteht aus:

- einer Titelzeile mit Produktbezeichnung,

- der Hauptmenüleiste,

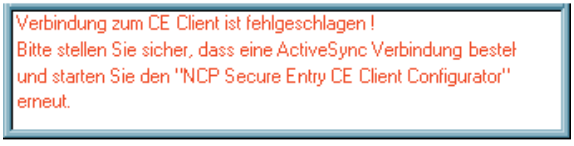
- einer Buttonleiste für “Upload” und “Download” des Telefonbuchs

- der Profilauswahl für bereits erstellte Profile,

- dem grafischen Statusfeld zur Anzeige des Verbindungsstatus (derzeit noch ohne Funktion),

- der Buttonleiste mit “Verbinden” und “Trennen” (derzeit noch ohne Funktion)

- und dem Log-Fenster für Meldungen. Die Texte in diesem Log-Fenster, betreffen die Kommunikation zwischen PDA und PC-Komponente bzw. die Kompatibilität der Profil-Einstellungen des Configurators mit den aktuellen Einstellungen des PDAs. So wird zum Beispiel geprüft, ob der virtuelle Adapter (Loopback-Adapter) am PDA ausgeschaltet ist und beim Kopieren der Profile auf den PDA darauf hingewiesen, dass in diesem Fall der NCP Dialer nicht verwendet werden kann. Das entsprechende Profil wird am PDA dann nicht angezeigt.



rote Meldungen: Fehler und missglückte Verbindungen
grüne Meldungen: OK-Meldungen bei Upload von Profil-Einstellung und Zertifikat
blaue Meldungen: Hinweise und Warnungen wegen inkompatibler Profile (WAN Support, virtueller Adapter am PDA - Upload auf den PDA)

Die Benutzeroberfäche ist Windows-konform gestaltet und der Bedienung anderer Windows-Anwendungen angepasst.

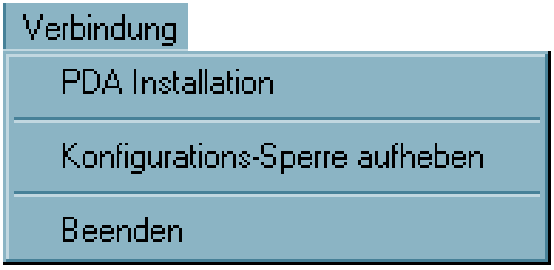
4. Das Configurator-Menü

Die Beschreibung folgt den Menüpunkten in der Menüleiste.

Die Hauptmenüpunkte in der Menüleiste von links nach rechts sind:

- ☐ Verbindung |Menü
- ☐ Konfiguration |Menü
- ☐ Fenster |Menü
- ☐ Hilfe |Menü

4.1 Verbindung



Unter diesem Menüpunkt wird die Installation der PDA-Komponente angestoßen (siehe dazu oben → 2.6 Installation der PDA-Komponente), die Konfigurations-Sperre aufgehoben und der Configurator beendet.

PDA-Installation

Unter diesem Menüpunkt wird die Installation der PDA-Komponente angestoßen. Bitte beachten Sie dabei, dass zur Installation der PDA-Komponente eine ActiveSync-Verbindung bestehen muss.

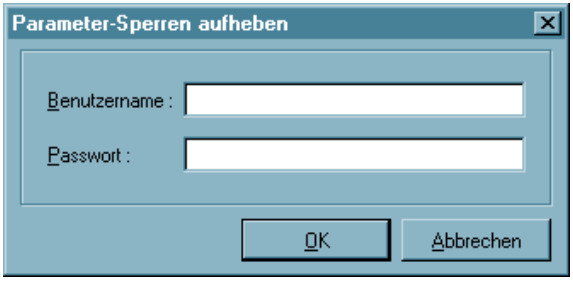
Bitte achten Sie darauf, dass der Dialog “Software” von ActiveSync nicht geöffnet ist, wenn sie das PDA-Installationsprogramm ausführen.

Konfigurations-Sperren aufheben/wiederherstellen

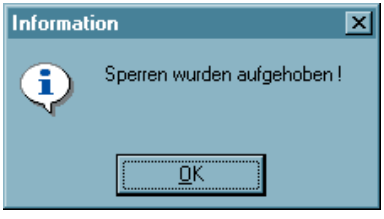
Dieser Menüpunkt erscheint nur, wenn Konfiguration-Sperren durch den Administrator vergegeben wurden.

Diverse Parameterfelder und Menüpunkte, die für Ihren Anschluss nicht von Bedeutung sind, können vom Systemadministrator ausgeblendet werden. Sie sind dann in den Profil-Einstellungen bzw. Menü nicht mehr sichtbar.

Um die Parameter wieder einzublenden, wählen Sie diesen Menüpunkt.

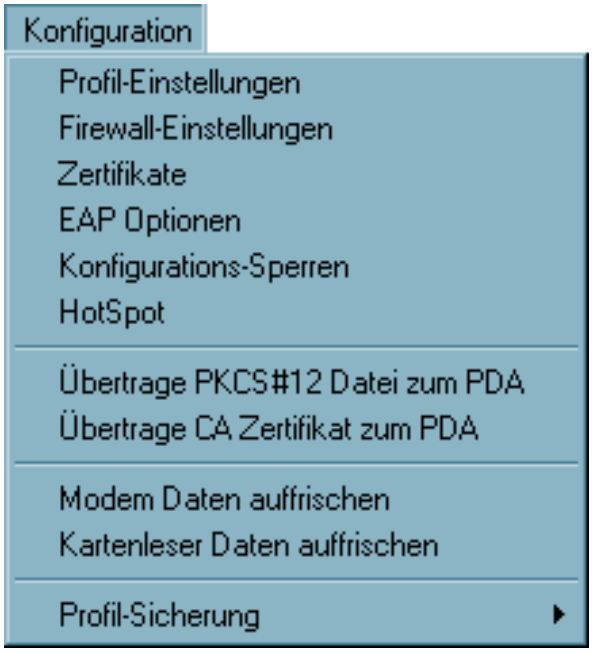


Nach Eingabe von User ID und Passwort des Administrators werden die Sperren aufgehoben.



Nach dem Informationsfenster (links) erscheint der Menüpunkt “Konfigurations-Sperre wiederherstellen”.

4.2 Konfiguration



Unter diesem Menüpunkt können sämtliche Einstellungen für die Arbeit mit dem IPSec Client vorgenommen werden, die länger als eine Session bestehen sollen. Dies betrifft das Anlegen der Profile, die Konfiguration der IPSec-Verbindungen und die Firewall-Einstellungen.

Darüber hinaus kann eigens konfiguriert werden, wie Zertifikate genutzt werden sollen, welche IP-Pakete von der Personal Firewall gefiltert werden sollen und welche Konfigurations-Rechte der Benutzer erhält.

Der Menüpunkt "Übertrage PKCS#12-Datei zum PDA" dient der Kopie des Soft-Zertifikats auf das PDA-Gerät.

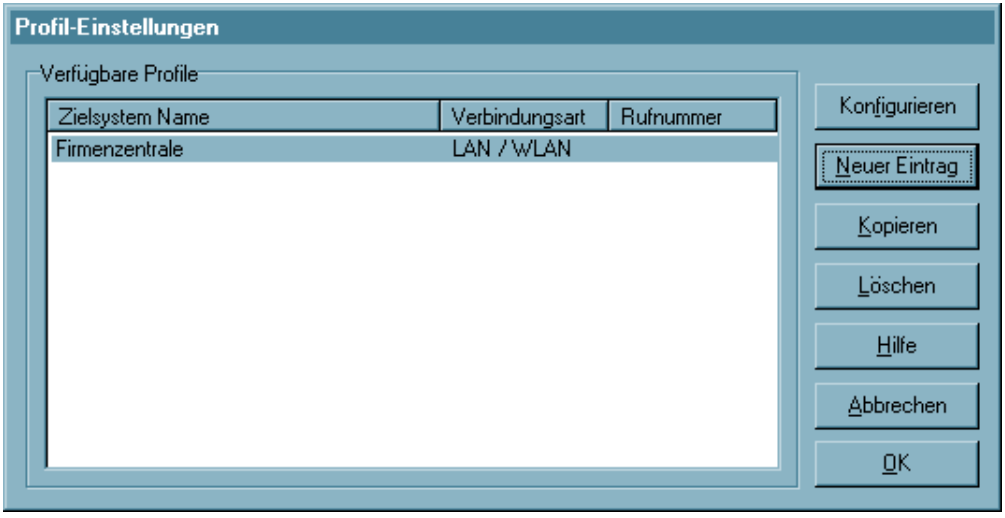
4.2.1 Profil-Einstellungen

Die Einträge der Profil-Einstellungen

Bei einer Erstinstallation der IPSec Client Software ist noch kein Profil vorhanden. In diesem Fall wird automatisch ein Konfiguartions-Assistent eingeblendet, der Ihnen hilft, eine Konfiguration anzulegen. Damit wird zugleich das erste Profil der IPSec Client Software angelegt. Dieser Assistent wird auch gestartet bei Klick auf “Neuer Eintrag” (siehe unten, “Neuer Eintrag – Profil”).

Mit den Profil-Einstellungen kann die Parametrisierung für die Zielsysteme (Profil) durchgeführt und die Übertragungsart, den Benutzeranforderungen entsprechend, bis ins Detail konfiguriert werden.

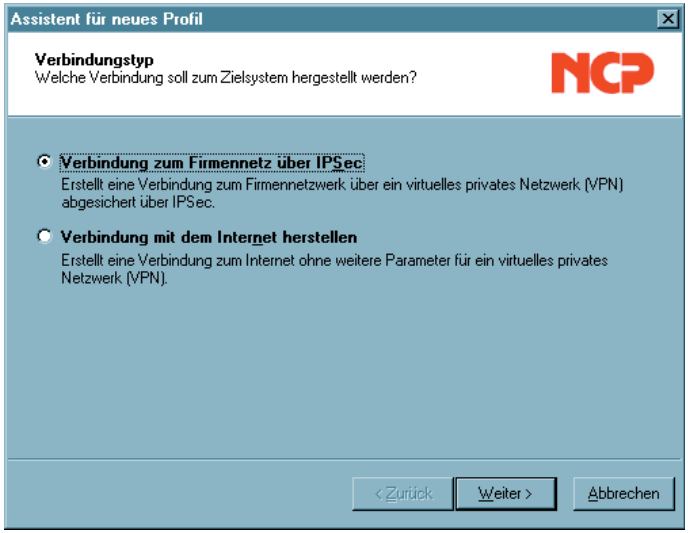
Nachdem Sie auf “Profil-Einstellungen” im Monitor-Menü “Konfiguration” geklickt haben, öffnet sich das Menü und zeigt in einer Liste der bereits verfügbaren Profile deren Namen und die Rufnummern der zugehörigen Zielsysteme.



Auf der rechten Seite der Profil-Einstellungen sind Buttons angebracht zu folgenden Funktionen: Konfigurieren, Neuer Eintrag, Kopieren, Löschen, OK, Hilfe und Abbrechen.

Neuer Eintrag – Profil

Um ein neues Profil zu definieren, klicken Sie auf “Profil-Einstellungen”. Wenn sich das Fenster des Menüs öffnet klicken Sie auf “Neuer Eintrag”. Jetzt legt der “Assistent für ein neues Profil” mit Ihrer Hilfe ein neues Profil an. Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Profil angelegt. Für alle weiteren Parameterfelder des Profils werden Standardwerte eingetragen.



Mit dem Konfigurations-Assistenten können Verbindungen mit dem Internet oder zum Firmennetz rasch hergestellt werden. Je nach Auswahl des gewünschten Verbindungstyps wird das Profil nach wenigen Konfigurationsabfragen angelegt.

Im folgenden die jeweils notigen Daten zur Konfiguration:

Verbindung zum Firmennetz über IPSec:

→ Profil-Name
→ Verbindungsmedium
→ Zugangsdaten fur Internet-Dienstanbeiter (Benutzername, Passwort, Rufnummer)
→ VPN-Gateway-Parameter (Tunnelendpunkt IP-Adresse)
→ Zugangsdaten fur VPN-Gateway (XAUTH, Benutzername, Passwort)
→ IPSec-Konfiguration (Exch. Mode, PFS-Gruppe, Kompression)
→ Statischer Schlüssel (Preshared Key), ohne Zertifikat (IKE ID-Typ, IKE ID)
→ IP-Adressen-Konfiguration (IP-Adresse des Clients, DNS/WINS-Server)
→ Firewall-Einstellungen

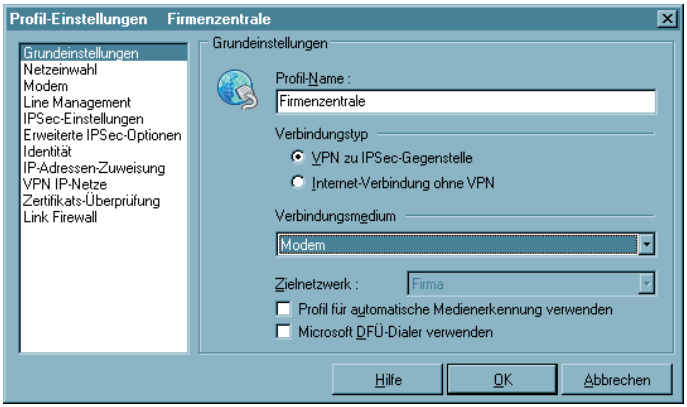
Verbindung mit dem Internet herstellen:

→ Profil-Name
→ Verbindungsmedium
→ Zugangsdaten fur Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)

Das neue Zielsystem erscheint nun in der Liste der Zielsysteme im Telefonbuch mit dem von Ihnen vergebenen Namen. Wenn keine weiteren Parameter-Einstellungen nötig sind, können Sie das Telefonbuch mit Ok schließen. Das neue Zielsystem ist nach einem Upload des Telefonbuchs auf das PDA-Gerät sofort verfügbar. Es kann über den Verbinden-Button unter Windows CE sofort angewählt werden.

Konfigurieren – Profil

Um die (Standard-)Werte eines Profils zu editieren, wählen Sie mit der Maus das Profil, dessen Werte Sie ändern möchten, und klicken anschließend auf “Konfigurieren”. Die Profil-Einstellungen zeigen nun in ihrem linken Fenster eine Liste von Begriffen, denen jeweils ein Parameterfeld zugeordnet ist:



Grundeinstellungen
Netzeinwahl
Modem
Line Management
IPSec-Einstellungen
Erweiterte IPSec-Optionen
Identität
IP-Adressen-Zuweisung
VPN IP-Netze
Zertifikats-Überprüfung
Firewall-Einstellungen

Je nachdem, welcher Begriff markiert wird, zeigt sich das entsprechende Feld mit den zugehörigen Parametern (siehe → 5. Konfigurationsparameter).

Ok – Profil

Die Konfiguration eines Profils ist abgeschlossen, wenn Sie das Konfigurationsfenster mit “OK” schließen. Das neue oder geänderte Profil ist im Monitor sofort verfügbar. Es kann im Monitor über die Profilauswahl selektiert werden und über das Menü “Verbindung / Verbinden” sofort zur Anwahl an das Zielsystem verwendet werden.

Kopieren – Profil

Um die Parameter-Einstellungen eines bereits definierten Profils zu kopieren, markieren sie das zu kopierende Profil in der Liste und klicken Sie auf den Kopieren-Button. Daraufhin wird das Grundeinstellungen-Parameterfeld geöffnet. Ändern Sie nun den Eintrag in “Profil-Name” und klicken Sie anschließend Ok. Nur wenn Sie den Namen des Profils ändern, kann es auch als neuer Eintrag in der Liste der Profile vermerkt werden.

Ein kopiertes Profil muss einen neuen, noch nicht vergebenen, Namen erhalten. Nur so kann es in der Liste der Profile abgelegt werden.

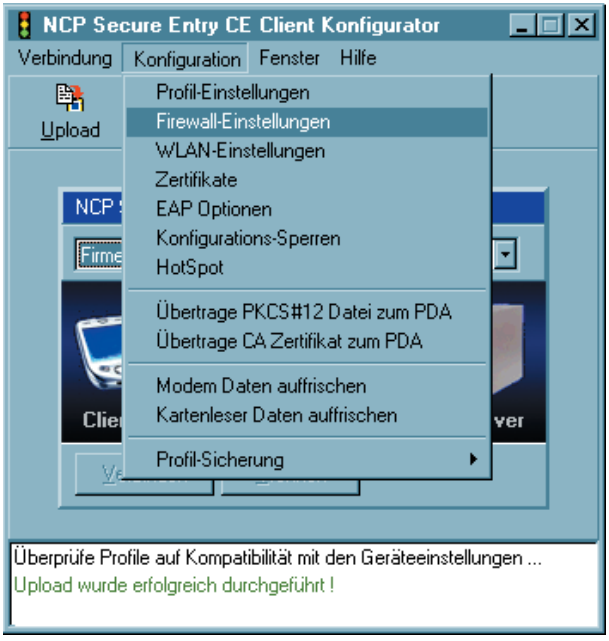
Löschen – Profil

Um ein Profil zu löschen, wählen Sie es aus und klicken den Löschen-Button.

4.2.2 Firewall-Einstellungen

Alle Firewall-Mechanismen sind optimiert für Remote Access-Anwendungen und werden bereits beim Start des Rechners aktiviert. D.h. im Gegensatz zu VPN-Lösungen mit eigenständiger Firewall ist der Telearbeitsplatz bereits vor der eigentlichen VPN-Nutzung gegen Angriffe geschützt.

Die Firewall bietet auch im Fall einer Deaktivierung der Client-Software vollen Schutz des Endgerätes. Alle Firewall-Regeln können zentral vom Administrator vorgegeben und deren Einhaltung erzwungen werden. Voraussetzung hierfür ist das zentrale NCP Secure Enterprise Management, mit dessen Hilfe die Konfiguration des Clients fest, für den Anwender nicht änderbar, vorgegeben werden kann.



Bitte beachten Sie, dass die Firewall-Einstellungen global, d.h. für alle Profil-Einstellungen gültig sind.

Dagegen ist die Einstellung der Link Firewall, die im Telefonbuch vorgenommen werden kann, nur für den dazu gehörenden Telefonbuch-Eintrag (Zielsystem) und die Verbindung zu diesem Zielsystem wirksam.

Eigenschaften der Firewall

Die Firewall arbeitet nach dem Prinzip der Paketfilterung in Verbindung mit Stateful Packet Inspection (SPI). Die Firewall prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis des konfigurierten Regelwerks, ob ein Datenpaket weitergeleitet oder verworfen wird.

Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen wird der unbefugte Zugriff auf Daten und Ressourcen im zentralen Datennetz verhindert. Zum anderen wird mittels Stateful Inspection der jeweilige Status bestehender Verbindungen überwacht. Die Firewall kann darüber hinaus erkennen, ob eine Verbindung "Tochterverbindungen" geöffnet hat – wie beispielsweise bei FTP oder Netmeeting – deren Pakete ebenfalls weitergeleitet werden müssen. Wird eine Regel für eine ausgehende Verbindung definiert, die einen Zugriff erlaubt, so gilt die Regel automatisch für entsprechende Rückpakete. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf.

Die Firewall-Regeln können dynamisch konfiguriert werden, d.h. ein Anhalten der Software oder ein Reboot ist nicht nötig.

Die Firewall-Einstellungen im Konfigurationsmenü des Client-Monitors gestatten eine genauere Spezifikation von Firewall-Filterregeln. Sie wirken global. D.h. unabhängig vom aktuell gewählten Zielsystem werden immer zuerst die Regeln der erweiterten Firewall-Einstellungen abgearbeitet, bevor die Regeln der Firewall aus dem Telefonbuch angewendet werden.

Eine Kombination der globalen und link-bezogenen Firewall kann in bestimmten Szenarien durchaus sinnvoll sein. Im Allgemeinen sollten jedoch nahezu alle Anforderungen über die globalen Einstellungmöglichkeiten abzudecken sein.

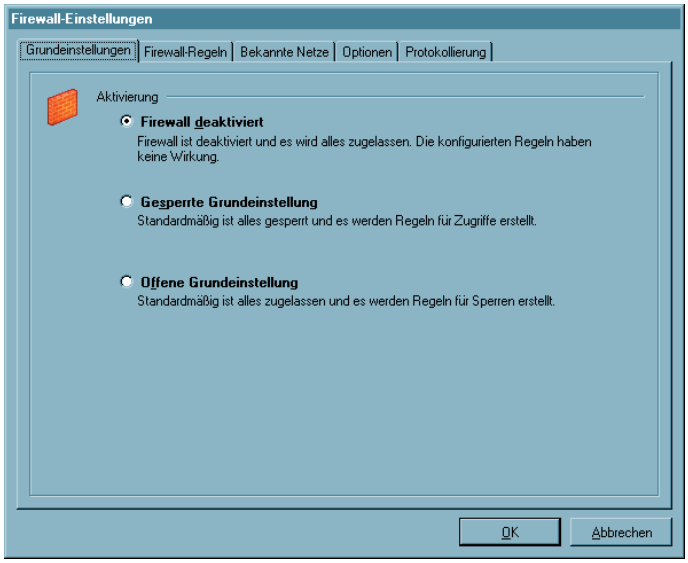
Bitte beachten Sie, dass die link-bezogenen Firewall-Einstellungen bei Aktivierung Vorrang den globalen haben. Ist z.B. die Link-Firewall auf "immer" und "Ausschließlich Kommunikation im Tunnel zulassen" eingestellt, kann trotz evtl. anders lautender Regeln der globalen Konfiguration nur ein Tunnel aufgebaut und darüber kommuniziert werden. Jeglicher anderer Verkehr wird von der Link-Firewall verworfen.

Konfiguration der Firewall-Einstellungen

Die Filterregeln der erweiterten Firewall können sowohl anwendungsbezogen als auch (zusätzlich) adressorientiert, bezüglich bekannter/unbekannter Netze, definiert werden.

Um Konflikte zwischen den Regeln der verbindungsorientierten Firewall des Telefonbuchs und der erweiterten Firewall zu vermeiden, wird empfohlen, die Firewall des Telefonbuchs auf "inaktiv" zu schalten, wenn die erweiterte Firewall eingesetzt wird. Die IP-Adressen der jeweiligen Verbindung (zum Ziel-Gateway) können stattdessen in den Filterregeln der erweiterten Firewall eingesetzt werden.

Konfigurationsfeld Grundeinstellungen



In den Grundeinstellungen wird festgelegt, mit welcher Basis-Policy die Firewall arbeiten soll.

Firewall deaktiviert

Wird die erweiterte Firewall deaktiviert, so wird in diesem Kompatibilitätsmodus nur die im Telefonbuch konfigurierte Firewall genutzt. Dies bedeutet, dass alle Datenpakete nur über die Sicherheitsmechanismen dieser verbindungsorientierten Firewall abgearbeitet werden.

Gesperrte Grundeinstellung (empfohlen)

Wird diese Einstellung gewählt, so sind die Sicherheitsmechanismen der Firewall immer aktiv. D.h. ohne zusätzlich konfigurierte Regeln wird jeglicher IP-Datenverkehr unterbunden. Ausgenommen sind die Datenpakete, die durch eigens erstellte, aktive Firewall-Regeln gestattet (durchgelassen) werden (Permit Filter).

Trifft eine der Eigenschaften eines Datenpakets auf die Definition einer Firewall-Regel zu, wird an dieser Stelle die Abarbeitung der Filterregeln beendet und das IP-Paket weitergeleitet.

Im Modus der gesperrten Grundeinstellung kann auf komfortable Weise eine L2Sec/IPSec-Tunnelkommunikation freigeschaltet werden.

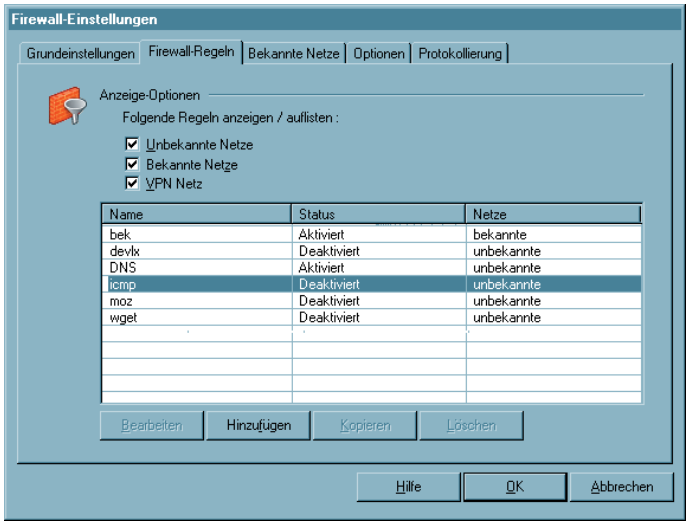
Dazu kann im Konfigurationsfeld “Optionen” der Datenverkehr über VPN-Protokolle (L2Sec, IPSec) global zugelassen werden.

Offene Grundeinstellung

In der offenen Grundeinstellung sind zunächst alle IP-Pakete zugelassen. Ohne weitere Filterregeln werden alle IP-Pakete weitergeleitet.

Ausgenommen sind die Datenpakete, die durch eigens erstellte, aktive Firewall-Regeln ausgefiltert (nicht durchgelassen) werden (Deny Filter). Trifft eine der Eigenschaften eines beim Server/Client ankommenden IP-Pakets auf die Definition eines Deny-Filters zu, wird an dieser Stelle die sequentielle Abarbeitung der Filterregeln beendet und das IP-Paket von der Weiterleitung ausgeschlossen. Daten-Pakete, die auf keinen passenden Deny-Filter treffen, werden weitergeleitet.

Konfigurationsfeld Firewall-Regeln



In diesem Konfigurationsfenster werden die Regeln für die Firewall zusammengestellt. Die Anzeige-Optionen sind standardmäßig alle aktiv. Mittels dieser wird eingestellt, welche Regeln in Abhängigkeit ihrer Zuordnung in der Übersicht angezeigt werden:

– unbekannte Netze
– bekannte Netze
– VPN-Netze

Diese Auswahlfelder für die Anzeigen der Regeln dienen nur der Übersichtlichkeit und haben keine Auswirkung auf die Anwendung einer Filterregel. Für jede definierte Regel werden die wichtigsten Eigenschaften gezeigt:
– Name
– Status
– Netz

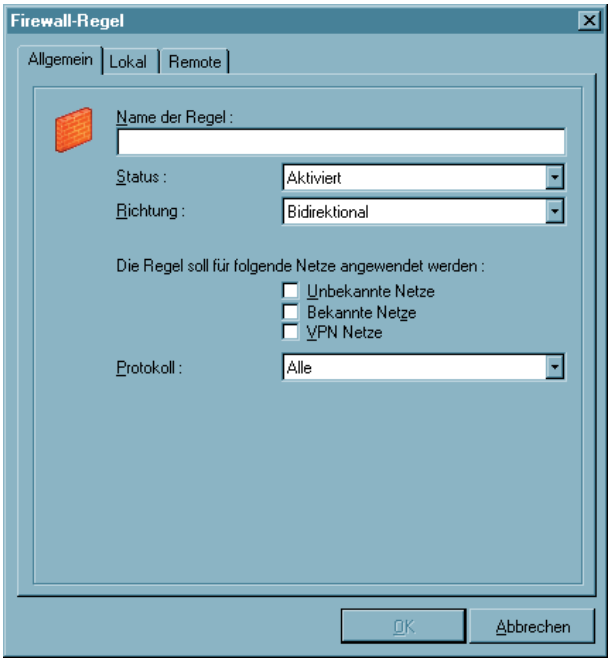
Durch Klick auf diese Eigenschafts-Buttons können die eingeblendeten Regeln sortiert werden.

Erstellen einer Firewall-Regel

Über die Buttons unterhalb der Anzeigezeilen werden die Regeln erzeugt oder bearbeitet. Um eine Firewall-Regel zu erstellen, klicken Sie auf “Hinzufügen”. Die Erstellung einer Filterregel erfolgt über drei Konfigurationsschritte bzw. Registerkarten:

– Allgemein: In diesem Konfigurationsfeld wird festgelegt für welche Netze und welches Protokoll die Regel gelten soll.
– Lokal: In diesem Konfigurationsfeld werden die Werte der lokalen Ports und IP-Adressen eingetragen.
– Remote: Im Remote-Feld werden die Port- und Adress-Werte der Gegenseite eingetragen.

■ Firewall-Regel / Allgemein



Einzelregeln stellen immer Ausnahmen von der Grundeinstellung dar (siehe → Grundeinstellung).

Name der Regel

Mit diesem Namen erscheint die Regel in der Anzeigeliste.

Status

Die Regel wird nur dann auf Datenpakete angewendet, wenn der Status “aktiv” ist.

Richtung

Mit der Richtung geben Sie an, ob diese Regel für eingehende oder ausgehende Datenpakete gelten soll. Wird die Richtung auf ausgehend gesetzt, wird nach dem Prinzip von Stateful Inspectiongearbeitet (siehe → Eigenschaften der Firewall). Stateful Inspection wird jedoch nur für die Protokolle UDP und TCP angewendet.
Auf “eingehend” kann z.B. dann geschaltet werden, wenn von Remote-Seite eine Verbindung aufgebaut werden soll (z.B. für “eingehende Rufe” oder Administrator-Zugriffe).
Die Einstellung “bidirektional” ist nur sinnvoll, wenn Stateful Inspection nicht zur Verfügung steht, z.B. für das ICMP-Protokoll (bei einem Ping).

Die Regel soll für folgende Netze angewendet werden

Beim Neuanlegen einer Regel ist diese zunächst keinem Netz zugeordnet. Eine Regel kann erst dann gespeichert werden, wenn die gewünschte Zuordnung erfolgt ist und ein Name vorgegeben wurde.
Unbekannte Netze
– sind alle Netze (IP-Netzwerkschnittstellen), die weder einem bekannten noch einem VPN-Netz zugeordnet werden können. Darunter fallen z.B. Verbindungen über das DFÜ-Netzwerk von Microsoft oder auch direkte und unverschlüsselte Verbindungen mit dem integrierten Dialer des Clients, wie auch HotSpot WLAN-Verbindungen. Soll eine Regel für unbekannte Netze gelten, so muss diese Option aktiviert werden.

Bekannte Netze
– werden im gleichnamigen Register im Fenster “Firewall-Einstellungen” definiert. Solle eine Regel für bekannte Netze gelten, muss diese Option aktiviert werden.
VPN-Netze
– sind alle L2Sec- oder IPSec-Verbindungen in aufgebautem Zustand. Darüber hinaus fallen unter diese Gruppe auch alle verschlüsselten Direkteinwahlverbindungen über den integrierten Dialer des Clients. Solle eine Regel für VPN-Netze gelten, so muss diese Option aktiviert werden.

Protokoll

Je nach Anwendung oder Art der Verbindung ist das entsprechende Protokoll zu wählen:

TCP, UDP, ICMP, GRE, ESP, AH, IGRP, RSVP, IPv6 oder IPv4, Alle

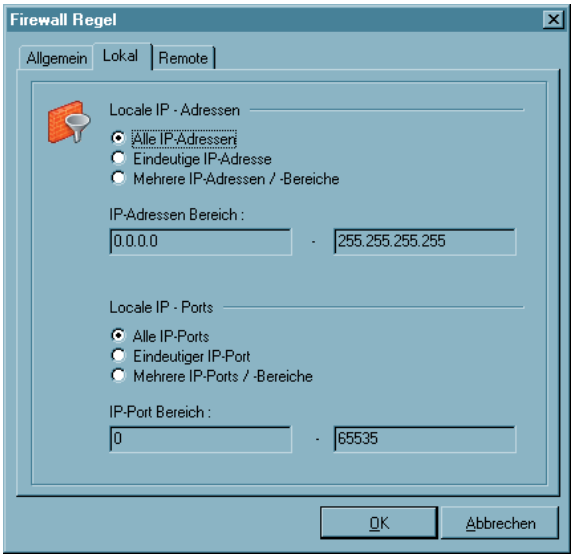
Verbindungssteuerung

Über diese Parameter wird die Art der Verbindung beeinflusst.

Sie wählen z.B. die Option, dass die hier konfigurierte Regel “nur gültig bei inaktiver VPN-Verbindung” ist, wenn Sie wünschen, dass z.B. eine Internet-Verbindung bei gleichzeitig bestehender VPN-Verbindung ausgeschlossen wird, ansonsten aber Internet-Verbindungen zu unbekannten Netzen zugelassen sein sollen. Dazu muss diese Regel für “unbekannte Netze” angewendet werden, d.h. diese Regel muss den Zugang zu unbekannten Netzen zulassen.

Die Option “kein automatischer Verbindungsaufbau” steht nur bei gesperrter Grundeinstellung zur Verfügung. Sie ist nur sinnvoll, wenn im Telefonbuch im Parameterfeld “Verbindungssteuerung” der Verbindungsaufbau auf “automatisch” gestellt wurde. Für die über diese Regel definierten Datenpakete findet bei Aktivierung dieser Funktion kein automatischer Verbindungsaufbau statt, für andere Datenpakete schon.

■ Firewall-Regel / Lokal



Auf dieser Registerkarte werden die Filter für die lokalen IP-Adressen und IP-Ports eingestellt.

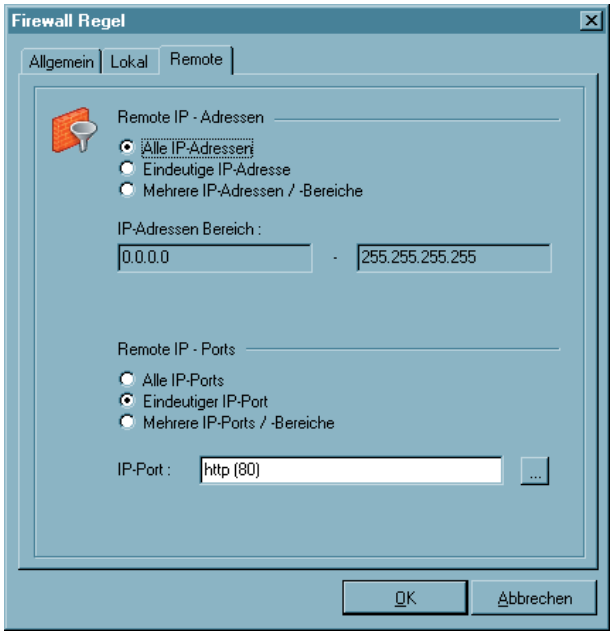
Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall nach außen durchgelassen, deren Quelladresse (Source Address) mit der unter “Lokale IP-Adressen” übereinstimmt oder im Gültigkeitsbereich liegt. Von den eingehenden Datenpaketen werden diejenigen durchgelassen, deren Zieladresse (Destination Address) mit der unter “Lokale IP-Adressen” übereinstimmt oder im Gültigkeitsbereich liegt.

Ebenso verhält es sich bei gesperrter Grundeinstellung mit den IP-Ports. Diejenigen Datenpakete werden nach außen gelassen, deren Quell-Port (Source Port) unter die Definition der lokalen Ports fällt. Von den eingehenden Datenpaketen werden die durchgelassen, deren Ziel-Port (Destination Port) unter die Definition der lokalen Ports fällt.

Alle IP-Adressen
– umfasst alle Quell-IP-Adressen abgehender bzw. Ziel-IP-Adressen eingehender Pakete, unabhängig vom lokalen Netzwerkadapter.
Eindeutige IP-Adresse
– ist die für den lokalen Netzwerkadapter definierte IP-Adresse. Sie kann je nach Verbindung z.B. der Adresse der Ethernet-Karte, der WLAN-Karte oder auch dem VPN-Adapter zugeordnet sein.
Mehrere IP-Adressen
– bezeichnet einen Adressbereich oder Pool. Z.B. kann dies der IP-Adress-Pool sein, aus dem die vom DHCP Server an den Client zugewiesene Adresse stammt.

Alle Ports
– erlaubt Kommunikation über alle Quellports bei ausgehenden und Ziel-Ports bei eingehenden Paketen.
Eindeutiger Port
– Diese Einstellung sollte nur dann verwendet werden, wenn dieses System einen Server-Dienst zur Verfügung stellt (z.B. Remote Desktop auf Port 3389).
Mehrere Ports
– Diese Einstellung sollte nur dann verwendet werden, wenn sich die lokalen Ports zu einem Bereich zusammenfassen lassen, die von einemDienst benötigt werden, der auf diesem System zur Verfügung gestellt wird (z.B. FTP Ports 20/21).

Firewall-Regel / Remote



Auf dieser Registerkarte werden die Filter für die remote IP-Adressen und IP-Ports eingestellt.

Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall nach außen durchgelassen, deren Zieladresse (Destination Address) mit der unter “Lokale IP-Adressen” übereinstimmt oder im Gültigkeitsbereich liegt. Von den eingehenden Datenpaketen werden diejenigen durchgelassen, deren Quelladresse (Source Address) mit der unter “Lokale IP-Adressen” übereinstimmt oder im Gültigkeitsbereich liegt.

Ebenso verhält es sich bei gesperrter Grundeinstellung mit den IP-Ports. Diejenigen Datenpakete werden von der Firewall nach außen gelassen, deren Ziel-Port (Destination Port) unter die Definition der lokalen Ports fällt. Von den eingehenden Datenpaketen werden die durchgelassen, deren Quell-Port (Source Port) unter die Definition der lokalen Ports fällt.

Mit den Einstellungen unter Remote-IP-Adressen lässt sich festlegen, mit welchen entfernten IP-Adressen das system kommunizieren darf.

Alle IP-Adressen
– erlaubt die Kommunikation mit beliebigen IP-Adressen der Gegenseite, ohne Einschränkung.
Eindeutige IP-Adresse
– lässt nur Kommunikation mit der hier angegebenen IP-Adresse auf der Gegenseite zu.
Mehrere IP-Adressen /-Bereiche
– gestattet die Kommunikation mit verschiedenen IP-Adressen auf der Gegenseite entsprechend der Einträge.

Mit den Einstellungen unter Remote Ports lässt sich festlegen, über welche Ports mit entfernten Systemen kommuniziert werden darf.

Alle Ports
– setzt keinerlei Beschränkungen hinsichtlich Ziel-Port bei abgehenden bzw. Quell-Port bei eingehenden Paketen.

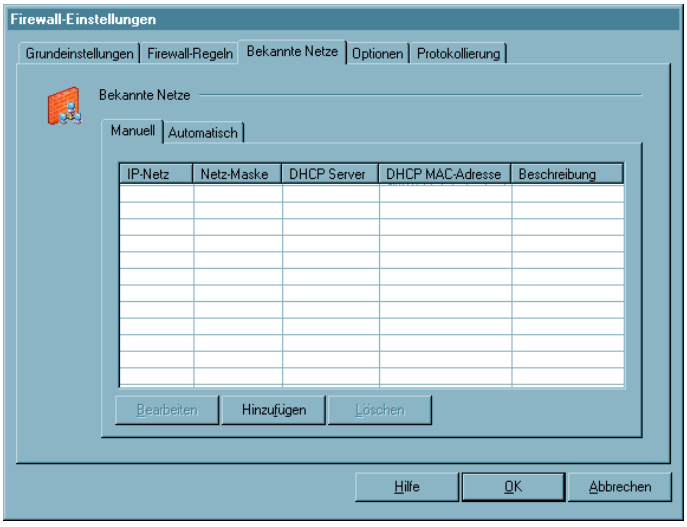
Eindeutiger Port
– lässt nur eine Kommunikation über den angegebenen Port zu, wenn dieser als Ziel-Port im abgehenden bzw. als Quell-Port im eingehenden Paket vorkommt. Soll z.B. eine Regel nur Telnet zu einem anderen System zulassen, ist hier Port 23 einzutragen.
Mehrere Ports / Bereiche
– können verwendet werden, wenn mehrere Ports für eine Regel verwendet werden sollen (z.B. FTP Port 20/21).

Konfigurationsfeld Bekannte Netze

Die bekannten Netze können unter den Rubriken “Manuell”, “Automatisch” und “Optionen” konfiguriert werden.

Die manuelle Definition eines bekannten Netzes durch den Administrator und die automatische Erkennung eines bekannten Netzes mittels Friendly Net Detection schließen sich nicht aus, sondern können gleichzeitig eingesetzt und über die Registerkarten “Manuell” und “Automatisch” konfiguriert werden.

Manuell



Wurde im Konfigurationsfeld “Firewall-Regeln” definiert, dass eine Regel auf Verbindungen mit bekannten Netzen (Friendly Nets) anzuwenden ist, so wird diese Regel immer angewendet, wenn ein Netz nach den hier anzugebenden Kriterien als Friendly Net identifiziert werden kann, bzw. der LAN-Adapter sich in einem Friendly Net befindet.

Der LAN-Adapter des Clients befindet sich dann in einem Friendly Net wenn:

[IP-Netze und Netzmaske]

– die IP-Adresse des LAN-Adapters aus dem angegebenen Netzbereich stammt. Ist z.B. das IP-Netz 192.168.254.0 mit der Maske 255.255.255.0 angegeben, so würde die Adresse 192.168.254.10 auf dem LAN-Adapter eine Zuordnung zum bekannten Netz bewirken.

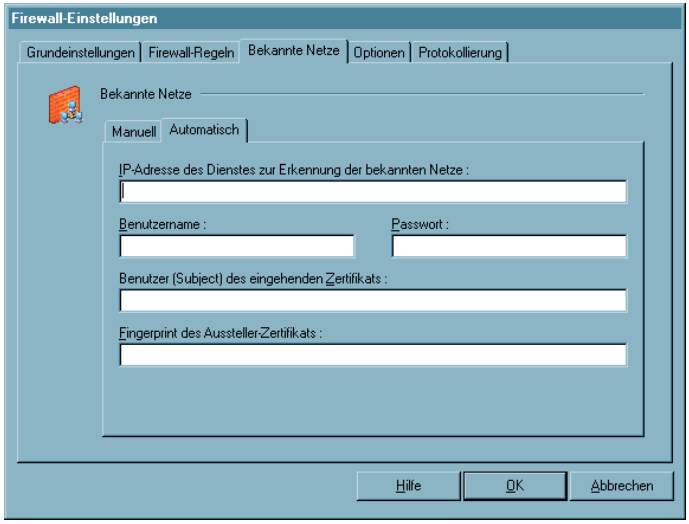
[DHCP Server]

– diese IP-Adresse von dem DHCP Server zugewiesen wurde, der die hier angegebene IP-Adresse besitzt;

[DHCP MAC-Adresse]

– wenn dieser DHCP Server die hier angegebene MAC-Adresse besitzt. Diese Option kann nur dann verwendet werden, wenn sich der DHCP Server im selben IP-Subnet befindet wie der DHCP Client.
Je mehr dieser Bedingungen erfüllt werden, desto präziser ist der Nachweis, dass es sich um ein vertrautes Netz handelt.
Die Zuordnung eines Adapters zu unbekannten oder bekannten Netzen wird automatisch protokolliert im Log-Fenster des Client-Monitors und in der Log-Datei der Firewall (siehe → Protokollierung).wenn dieser DHCP Server die hier angegebene MAC-Adresse besitzt.

Automatisch



Was ein Friendly Net ist, wird vom Administrator zentral verbindlich festgelegt. Die Signalisierung eines Friendly Net erfolgt im Monitor durch das Firewall-Symbol, das sich grün färbt, sobald sich der Client in ein Friendly Net eingewählt hat.

IP-Adresse des Dienstes zur Erkennung der bekannten Netze

Erforderlich ist ein Friendly Net Detection Server (FNDS), d.h. eine Softwarekomponente von NCP, die in einem als “Friendly Net” definierten Netz installiert werden muss. Dieser Friendly Net Detection Server muss über IP erreichbar sein und seine IPAdresse hier eingetragen werden.

Benutzername, Passwort (FNDS)

Die Authentisierung des FND Servers erfolgt über MD5 oder TLS. Hier einzutragender Benutzername und Passwort müssen mit jenen am FNDS hinterlegten übereinstimmen.

Benutzer (Subject) des eingehenden Zertifikats

Das eingehende Zertifikat des FNDS wird auf diesen String hin geprüft. Nur bei Gleichheit handelt es sich um ein Friendly Net.

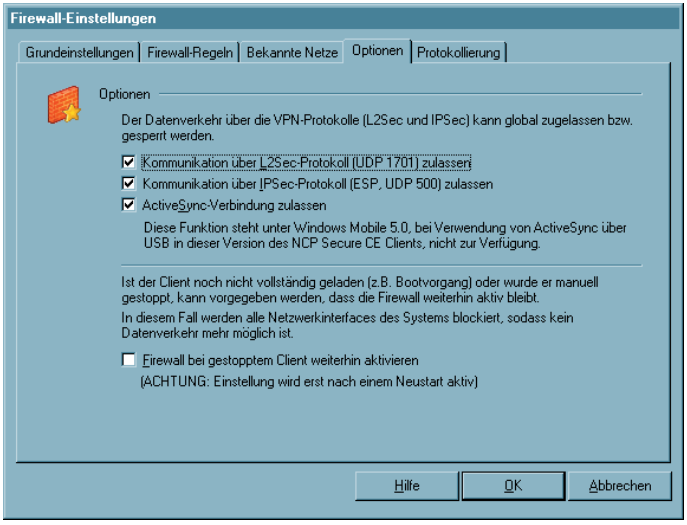
Fingerprint des Aussteller-Zertifikats

Um ein Höchstmaß an Fälschungssicherheit bieten zu können, muss der Fingerprint des Aussteller-Zertifikats überprüft werden können. Er muss mit dem hier eingegebenen Hash-Wert übereinstimmen.

Friendly Net Detection mittels TLS

Soll die Friendly Net Detection mittels TLS erfolgen (einschließlich einer Authentisierung über den Fingerprint des Aussteller-Zertifikats), so muss sich im Programmverzeichnis “CaCerts” dieses Aussteller-Zertifikat befinden und dessen Fingerprint muss mit dem hier konfigurierten übereinstimmen.

Konfigurationsfeld Optionen



Bei gesperrter Grundeinstellung kann der Aufbau von VPN-Verbindungen über das Register “Optionen” global zugelassen werden.

Es werden die folgenden für den Tunnelaufbau benötigten Protokolle und Ports per automatisch generierter Filter freigegeben:

Für L2Sec: UDP 1701 (L2TP), UDP 67 (DHCPS), UDP 68 (DHCPC)
Für IPSec: UDP 500 (IKE ISAKMP), IP-Protokoll 50 (ESP), UDP 4500 (NAT-T), UDP 67 (DHCPS), UDP 68 (DHCPC)
Für ActiveSync: TCP 990, 999, 5678, 5679

Die (globale) Firwall muss bei einer Direktverbindung (über USB, seriell oder Infrarot) für ActiveSync freigeschaltet werden. Diese Einstellung kann auch am PDA über das Popup-Menü vorgenommen werden, wenn die (globale) Firewall aktiv ist. Wird ActiveSync über Netzwerk betrieben (LAN oder WLAN), so muss zusätzlich manuell eine eigene Firewall-Regel für die Namensauflösung (DNS/WINS) erstellt werden.

Die globale Definition erspart die Einrichtung dedizierter Einzelregeln für die jeweilige VPN-Variante.

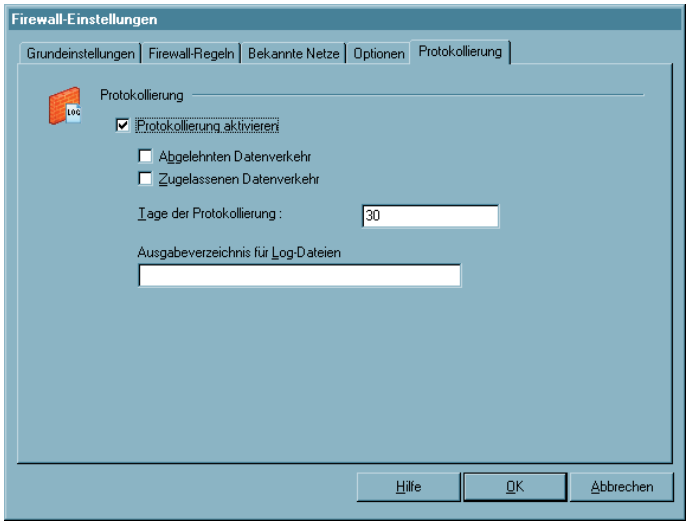
Bitte beachten Sie, dass dadurch lediglich der Tunnelaufbau ermöglicht wird. Existieren keine weiteren Regeln für VPN-Netze, die eine Kommunikation im Tunnel zulassen, kann über die VPN-Verbindung kein Datenaustausch erfolgen.

Firewall bei gestopptem Client weiterhin aktivieren

Die Firewall kann auch bei gestopptem Client aktiv sein, wenn diese Funktion selektiert wird. In diesem Zustand wird jedoch jede ein- und ausgehende Kommunikation unterbunden, so dass keinerlei Datenverkehr möglich ist, solange der Client deaktiviert ist.

Wird oben genannte Funktion nicht genutzt und der Client gestoppt, so wird auch die Firewall deaktiviert.

Konfigurationsfeld Protokollierung



Die Aktivitäten der Firewall werden je nach Einstellung in eine Log-Datei geschrieben. Das "Ausgabeverzeichnis für Log-Dateien" befindet sich standardmäßig im Installationsverzeichnis unter \log.

Die Log-Dateien für die Firewall sind im reinen Textformat geschrieben und benannt als Firewallyymmdd.log. Sie beinhalten eine Beschreibung vom "abgelehnten Datenverkehr" und/oder "zugelassenen Datenverkehr". Wurde keine dieser Optionen selektiert, so werden nur Statusinformationen zur Firewall hinterlegt.

Die Log-Dateien werden bei jedem Start der Firewall geschrieben. Maximal werden davon so viele im Log-Verzeichnis gehalten, wie als Anzahl der "Tage der Protokollierung" eingegeben wurde.

4.2.3 Zertifikate

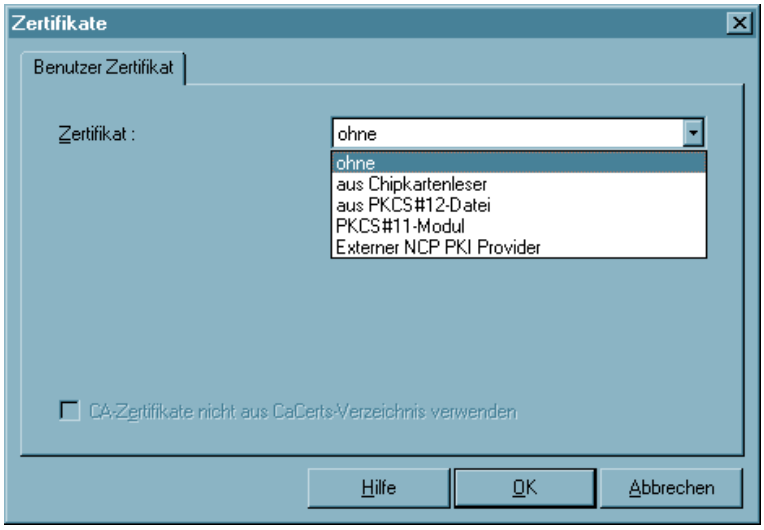
Unter diesem Menüpunkt wird konfiguriert welche Art von Zertifikaten eingesetzt werden – ob Soft-Zertifikate oder Zertifikate auf Chipkarten (Smart Cards) – und wo diese Zertifikate auf dem Rechnersystem zu finden sind. Deweiteren wird die Dauer der Gültigkeit eines Zertifikats festgelegt und können die Richtlinien für die PIN definiert werden.

Zertifikate (Certificates) werden von einer CA (Certification Authority) mittels PKI-Manager (Software) ausgestellt. Sie können als Soft-Zertifikat in Dateiform ausgeliefert werden oder auf eine Smart Card (Chipkarte) gebrannt werden. Diese Smart Card enthält u.a. mit den Zertifikaten digitale Signaturen, die ihr den Status eines digitalen Personalausweises verleihen. Es können Zertifikate eingesetzt werden, die einen privaten Schlüssel bis zu einer Länge von 2048 Bits haben. Als Gegenstelle muss der NCP Secure Server 5.21 oder höher eingesetzt werden.

Die Client Software überwacht, ob eine PKCS#12-Datei vorhanden ist. Wird eine PKCS#12-Datei (Soft-Zertifikat) eingesetzt, z.B. auf einem USB-Stick oder einer SD-Karte gespeichert, so wird nach dem Ziehen der SD-Karte die PIN zurückgesetzt und eine bestehende Verbindung abgebaut. Dieser Vorgang entspricht dem “Verbindungsabbau bei gezogener Chipkarte”, der bei Verwendung einer Chipkarte im Monitormenü unter “Konfiguration / Benutzer-Zertifikat” eingestellt werden kann. Wird später die SD-Karte wieder gesteckt, kann nach der erneuten PIN-Eingabe die Verbindung wieder hergestellt werden.

In der Zertifikats-Konfiguration können für die Pfad-Angaben die Umgebungsvariablen (Benutzer) des Betriebssystems eingesetzt werden. Die Variablen werden beim Schießen des Dialogs und beim Einlesen des Telefonbuches umgewandelt und in die Konfiguration zurück geschrieben. Existiert eine Umgebungsvariable nicht, wird sie aus dem Pfad beim Umwandeln entfernt und ein Log-Eintrag ins Logbuch geschrieben. Fehlt ein %-Zeichen (Syntax), bleibt die Variable stehen und es wird ebenfalls ein Log-Eintrag geschrieben.

Benutzer-Zertifikat

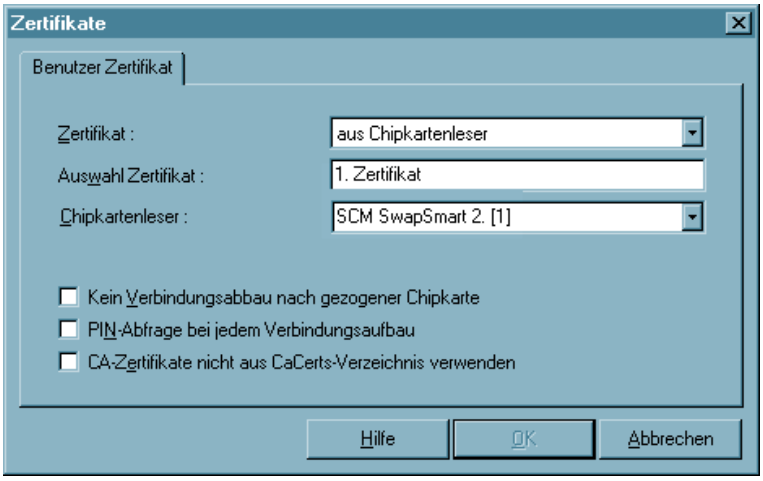


Zertifikat

Klicken Sie auf das Untermenü “Zertifikate”, so können Sie zunächst bestimmen, ob Sie die Zertifikate und damit die “Erweiterte Authentisierung” nutzen wollen – oder nicht.

ohne :		Wählen Sie in der Listbox “Zertifikat” die Einstellung “ohne”, so wird kein Zertifikat ausgewertet und die “Erweiterte Authentisierung” findet nicht statt.
aus Chipkartenleser	:	Wählen sie “aus Chipkartenleser” in der Listbox, so werden bei der “Erweiterten Authentisierung” die Zertifikate von der Smart Card in ihrem Chipkartenleser ausgelesen.
aus PKCS#12-Datei	:	Wählen Sie “aus PKCS#12 Datei” aus der Listbox, so werden bei der “Erweiterten Authentisierung” die Zertifikate aus einer Datei auf der Festplatte Ihres Rechners gelesen.
aus PKCS#11-Modul	:	Diese Schnittstelle können Sie auswählen, wenn bei der “Erweiterten Authentisierung” die relevanten Zertifikate von einem auf dem PDA installierten PKCS#11-Modul gelesen werden sollen.
Externer NCP PKI Provider:		Ein externer NCP PKI Provider bezeichnet eine NCP-spezifische Schnittstelle für besondere Anforderungen.

Chipkartenleser



Die Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind. Wenn Sie die Zertifikate von der Smart Card mit Ihrem Lesegerät nutzen wollen, wählen Sie Ihren Chipkartenleser aus der Listbox.

Bitte beachten Sie, dass der Chipkartenleser nur ausgewählt werden kann, wenn er am PDA installiert wurde und der NCP Client Service am PDA mindestens einmal gestartet wurde. (Siehe → Voraussetzungen für die Strong Security-Version)

Der Name eines Chipkarten-Lesers kann hier selektiert oder editiert werden. Verwendet man nun am PDA einen anderen Leser so unterscheidet sich der Name und der Leser wird nicht gefunden. Bei zwei Lesern, die sich lediglich in der Firmware unterscheiden, deswegen jedoch einen anderen Namen haben, kann das evtl. nicht erwünscht sein. z.B.:
SpringCard GCR-R1.44-GI slot A
SpringCard GCR-R1.44-GH slot A
für obiges Beispiel kann mit einem Stern “*” als Wildcard z.B. folgender Lesernamen angegeben werden: SpringCard*

■ Auswahl Zertifikat

1. Zertifikat ... (Standard = 1) Aus der Listbox kann aus bis zu drei verschiedenen Zertifikaten gewählt werden, die sich auf der Chipkarte befinden. Die Anzahl der Zertifikate auf der Chipkarte ist abhängig von der Registration Authority, die diese Karte brennt. Wenden Sie sich zu weiteren Fragen bitte an Ihren Systemadministrator.

Beispiel:

Auf den Chipkarten von Signtrust und NetKey 2000 befinden sich drei Zertifikate:
(1) zum Siginieren
(2) zum Ver- und Entschlüsseln
(3) zum Authentisieren (optional bei NetKey 2000)

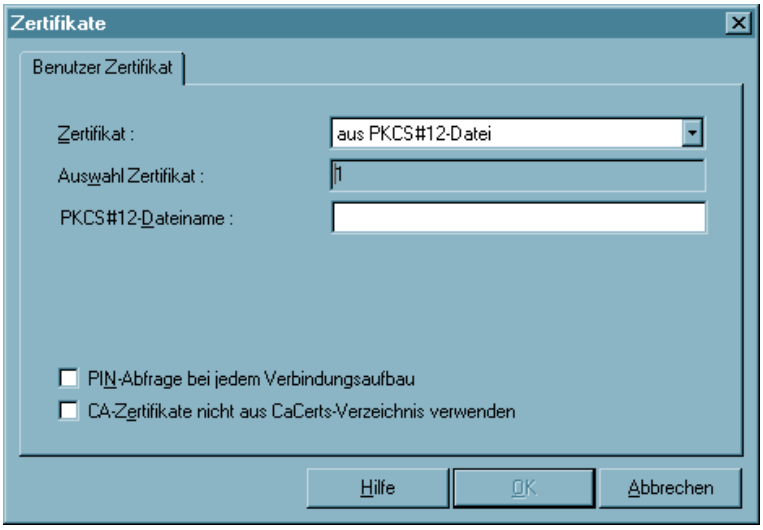
■ Kein Verbindungsabbau bei gezogener Chipkarte

Beim Ziehen der Chipkarte wird nicht unbedingt die Verbindung abgebaut. Damit "Kein Verbindungsabbau bei gezogener Chipkarte" erfolgt, muss diese Funktion aktiviert werden.

■ PIN-Abfrage bei jedem Verbindungsaufbau

Hier kann eingestellt werden, dass die PIN nicht nur nach jedem ersten Verbindungsaufbau nach einem Reboot des PDAs sondern vor jedem Verbindungsaufbau korrekt eingegeben werden muss. Diese Funktionalität kann für alle Verbindungsmodi (manuell, automatisch, wechselnd) genutzt werden.

PKCS#12-Datei



Nutzen Sie das PKCS#12-Format, so erhalten Sie von Ihrem Systemadministrator eine Datei, die auf dem PDA eingespielt werden muss (siehe → Übertrage PKCS#12-Datei auf PDA). In diesem Fall muss Pfad und Dateiname der PKCS#12 Datei eingegeben werden.

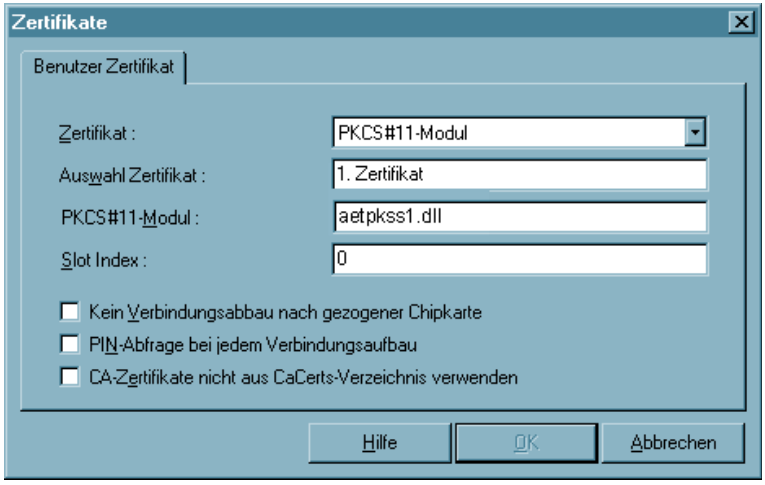
■ PKCS#12-Dateiname

Bitte beachten Sie: Pfad und Name der für die Konfiguration erforderlichen PKCS#12-Datei muss zu dem Ort der Datei auf dem PDA passen!

Zur Übertragung der PKCS#12-Datei kann im Configurator der PC-Komponente der Menüpunkt “Konfiguration - Übertrage PKCS#12-Datei zum PDA” verwendet werden. Wird diese Funktion genutzt, so kann der Pfad folgendermaßen angegeben werden:

```
%INSTALLDIR%\certs\<PKCS#12-Dateiname>
```

PKCS#11-Modul



Der Smart Card oder dem Token wird ein Treiber in Form einer PKCS#11-Bibliothek (DLL) mitgegeben. Diese Treiber-Software muss zunächst am PDA installiert werden. Dabei wird, je nach Hersteller, die DLL in einem Verzeichnis auf dem PDA abgelegt. Dieses Verzeichnis ist für gewöhnlich das Windows-Verzeichnis. Wird die DLL dort abgelegt, so genügt es im Feld zum PKCS#11-Modul den Namen der DLL einzutragen (siehe das Beispiel in obiger Abbildung “aetpkss1.dll”). Wird die DLL bei der Installation in ein anderes Verzeichnis gespielt, so muss der komplette Pfadname angegeben werden.

Alternativ kann die Datei NCPPKI.CONF editiert werden. Sie befindet sich im Installationsverzeichnis auf dem PDA (\programme\ncp secure ce client). Zum Editieren muss die Datei von Hand auf den PC kopiert werden. Unter “Interfaces” wird “PKCS11=1" gesetzt, als Modulname wird eine Bezeichnung für den angeschlossenen Leser angegeben und als PKCS11-DLL der Name der zugehörigen Treiberdatei (im Beispiel unten ”aetpkss1.dll").

```
[General]
LogLevel=
LogFile=

[Interfaces]
CTAPI=0
PCSC=1
PKCS11=1

[PKCS11 1]
ModulName        = A.E.T. SafeSign (PKCS11)
PKCS11-DLL       = aetpkss1.dll

Slotindex        = 1
```

Nach dem Editieren muss die Datei NCPPKI.CONF auf den PDA zurück kopiert werden. Anschließend muss ein Softreset am PDA erfolgen und der NCP Client Driver neu

gestartet werden. Nachdem die Kartenleserdaten aufgefrischt wurden (siehe unten) steht das PKCS#11-Modul im Configurator als “Chipkartenleser” (siehe oben) zur Verfügung.

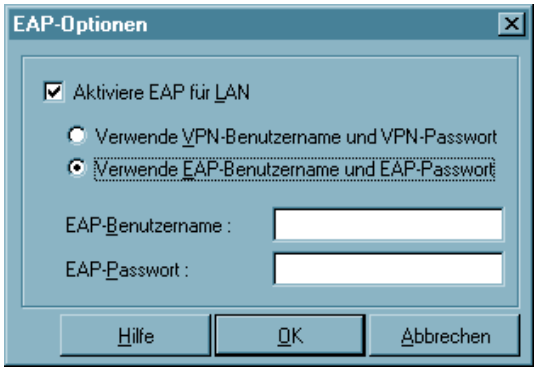
Slotindex

Der Slotindex ist im Normalfall “0". Weicht dieser Wert in der zugehörigen Beschreibung davon ab, so kann er nur bei der Konfiguration über die Datei NCPPKI.CONF geändert werden.

CA-Zertifikate nicht aus CACerts-Verzeichnis verwenden

Ist dies Funktion aktiv, so wird nicht das CA-Zertifikat aus dem lokalen Verzeichnis am PDA zur Verifizierung verwendet, sondern ein alternatives, das sich zum Beispiel auf einer Chipkarte befindet. Dieses CA-Zertifikat muss dasjenige sein, gegen das das eingehende Server-Zertifikat verifiziert wird.

4.2.4 EAP-Optionen



Hier kann der Einsatz des Extensible Authentication Protocols Message Digest5 (EAP MP5) eingestellt werden. Dieses Protokoll kann dann zum Einsatz kommen, wenn für den Zugang zum LAN ein Switch oder für das wireless LAN ein Access Point verwendet werden, die 802.1x-fähig sind und eine entsprechende Authentisierung unterstützen.

Mit dem Extensible Authentication Protocol (EAP MP5) kann verhindert werden, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.

Zur Authentisierung kann wahlweise “VPN-Benutzername” mit “VPN-Passwort” verwendet werden oder ein eigener “EAP-Benutzername” mit einem “EAP-Passwort”.

Zertifikatsinhalte können dergestalt automatisch übernommen werden, indem im Telefonbuch unter “Tunnel-Parameter” VPN-Benutzername und VPN-Passwort vom Zertifikat übernommen werden und in den EAP-Optionen “Verwende VPN-Benutzername und VPN-Passwort” aktiviert wird.

Bei EAP-TLS (mit Zertifikat) kann der EAP-Benutzername direkt aus der Zertifikats-Konfiguration bezogen werden. Folgende Inhalte des konfigurierten Zertifikats können genutzt werden, indem in die EAP-Konfiguration die entsprechenden Platzhalter eingegeben werden:

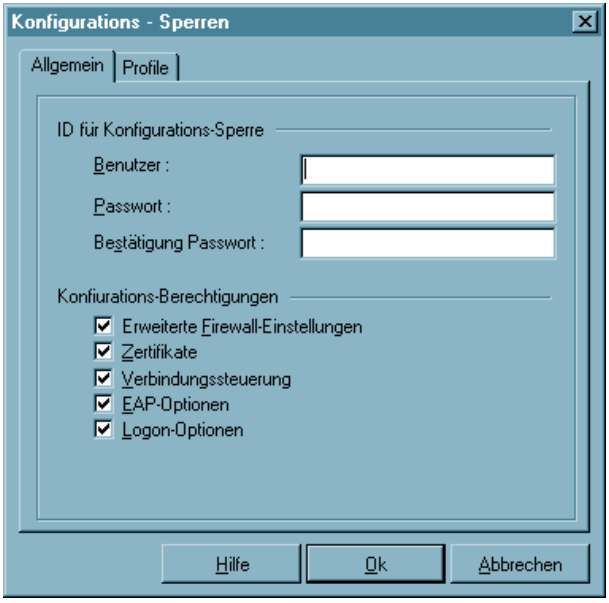
```
Commonname : %CERT_CN%
E-Mail : %CERT_EMAIL%
```

4.2.5 Konfigurations-Sperren

Über die Konfigurations-Sperren kann das Konfigurations-Hauptmenü im Monitor so modifiziert werden, dass der Benutzer die voreingestellten Konfigurationen nicht mehr abändern kann, bzw. ausgewählte Parameterfelder für den Benutzer nicht sichtbar sind.

Die Konfigurations-Sperren werden in der definierten Form erst wirksam, wenn die Einstellungen mit “OK” übernommen werden. Wird der “Abbrechen”-Button gedrückt, wird auf die Standard-Einstellung zurückgesetzt.

- **Allgemein | Konfigurations-Sperren**



Um die Konfigurations-Sperren wirksam festlegen zu können, muss eine ID eingegeben werden, die sich aus “Benutzer” und “Passwort” zusammensetzt. Das Passwort muss anschließend bestätigt werden.

Bitte beachten Sie, dass die ID für die Konfigurations-Sperre unbedingt nötig ist, die Sperren wirksam werden zu lassen oder die Konfigurations-Sperren auch wieder aufzuheben. Wird die ID vergessen, besteht keine Möglichkeit mehr, die Sperren wieder aufzuheben!

Anschließend kann die Berechtigung, die Menüpunkte unter dem Hauptmenüpunkt “Konfiguration” zu öffnen, für den Benutzer eingeschränkt werden. Standardmäßig kann der Benutzer alle Menüpunkte öffnen und die Konfigurationen bearbeiten. Wird zu einem Menüpunkt der zugehörige Haken mit einem Mausklick entfernt, so kann der Benutzer diesen Menüpunkt nicht mehr öffnen.

Profile | Konfigurations-Sperren

Die Bearbeitungsrechte für die Parameter in den Profil-Einstellungen sind in zwei Sparten unterteilt:

– Allgemeine Rechte
– Sichtbare Parameterfelder der Profile

Allgemeine Rechte

Die allgemeinen Rechte beziehen sich nur auf die (Konfiguration der) Profile. Wird festgelegt “Profile dürfen neu angelegt werden”, “Profile dürfen konfiguriert werden” bleibt jedoch ausgeschlossen, so können zwar mit dem Assistenten neue Profile definiert werden, eine nachfolgende Änderung einzelner Parameter ist dann jedoch nicht mehr möglich.

Sichtbare Parameterfelder der Profile

Die Parameterfelder der Profil-Einstellungen können für den Benutzer ausgeblendet werden.

Beachten Sie, dass Parameter eines nicht sichtbaren Feldes auch nicht konfiguriert werden können.

4.2.6 HotSpot

In der Konfiguration zur HotSpot-Anmeldung sind folgende Einstellungen möglich:

- **Standard-Browser für HotSpot-Anmeldung verwenden**

  Standardeinstellung. Wird der Haken in der Checkbox entfernt, kann ein anderer Browser unter Angabe des kompletten Pfads am PDA angegeben werden.

  Ein alternativer Browser (nicht Bestandteil der Software) kann speziell für die Anforderungen am Hotspot konfiguriert werden. D. h. es wird kein Proxy Server konfiguriert und alle aktiven Elemente (Java, Javascript, ActiveX) werden deaktiviert. (Der alternative Browser ist nicht Bestandteil der Client Software!)

- **MD5-Hash**

  In das Feld für “MD5-Hash” kann der MD5-Hash-Wert der Browser-Exe-Datei eingetragen werden, nachdem er ermittelt wurde. Auf diese Weise wird sichergestellt, dass nur mit diesem Browser eine HotSpot-Verbindung zustande kommt.

- **Startseite / Adresse**

  Unter “Startseite / Adresse” wird die oben beschriebene Startseite eingegeben in der Form: http://www.mycompagnie.de/error.html.

4.2.7 Übertrage PKCS#12-Datei zum PDA

Nach Klick auf diesen Menüpunkt kann die PKCS#12-Datei vom PC auf das PDA-Gerät übertragen werden.

Dazu öffnet sich zunächst ein Auswahlfenster, worin die gewünschte PKCS#12-Datei selektiert werden muss.

Achten Sie darauf, dass die physikalische Verbindung zwischen PDA und PC hergestellt und ActiveSync gestartet ist.

4.2.8 Übertrage CA-Zertifikat zum PDA

Nach Klick auf diesen Menüpunkt kann die PKCS#12-Datei vom PC auf das PDA-Gerät übertragen werden.

Dazu öffnet sich zunächst ein Auswahlfenster, worin die gewünschte PKCS#12-Datei selektiert werden muss.

Achten Sie darauf, dass die physikalische Verbindung zwischen PDA und PC hergestellt und ActiveSync gestartet ist.

4.2.9 Modem-Daten auffrischen

Nach Klick auf diesen Menüpunkt wird die Datei für die Modem-Daten (MODEM.INI) neu generiert und vom PC auf das PDA-Gerät übertragen.

Achten Sie darauf, dass die physikalische Verbindung zwischen PDA und PC hergestellt und ActiveSync gestartet ist.

4.2.10 Kartenleser-Daten auffrischen

Nach Klick auf diesen Menüpunkt wird die Datei für den Kartenleser (READER.INI) vom PC auf das PDA-Gerät übertragen.

Achten Sie darauf, dass die physikalische Verbindung zwischen PDA und PC hergestellt und ActiveSync gestartet ist.

4.2.11 Telefonbuch-Sicherung

Existiert noch kein gesichertes Telefonbuch, zum Beispiel bei einer Erstinstallation, so wird automatisch ein erstes angelegt (NCPPHONE.SAV).

- **Erstellen [Telefonbuch-Sicherung]**

  Nach jedem Klick auf den Menüpunkt “Erstellen” wird nach einer Sicherheitsabfrage eine Telefonbuch-Sicherung angelegt, das die Konfiguration zu diesem Zeitpunkt enthält.

- **Wiederherstellen [Telefonbuch-Sicherung]**

  Nach jedem Klick auf “Wiederherstellen” wird die letzte Telefonbuch-Sicherung eingelesen. Änderungen in der Konfiguration, die seit der letzten Telefonbuch-Sicherung vorgenommen wurden gehen damit verloren.

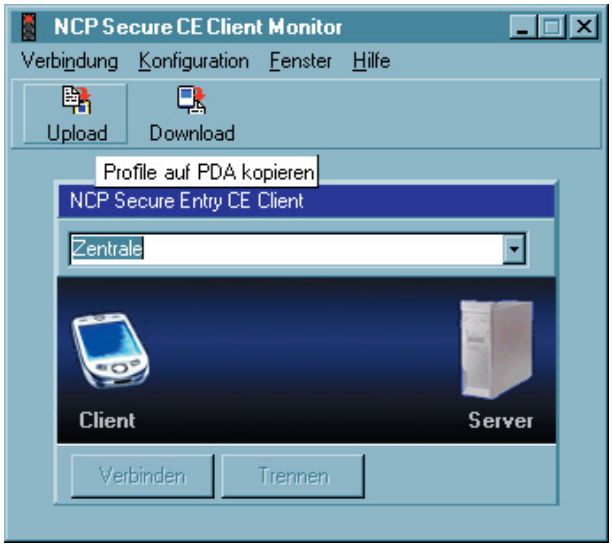
4.3 Fenster – Sprache

Unter dem Menüpunkt “Fenster” können Sie mit Klick auf Sprache von Deutsch auf Englisch umschalten und umgekehrt. Die Standardsprache bei Auslieferung ist Deutsch.

4.4 Hilfe – Info

Unter dem Menüpunkt Hilfe finden Sie mit Klick auf “Info” die Versionsnummer Ihrer eingesetzten Software.

4.5 Upload der Profil-Einstellungen



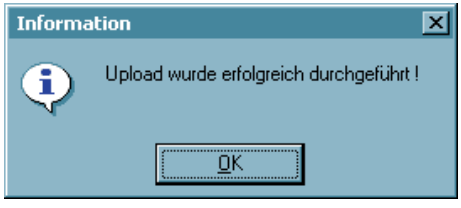
Nachdem die Konfiguration eines Zielsystems abgeschlossen wurde und die Profil-Einstellungen komplettiert wurden, müssen sie auf den PDA kopiert werden.

Dazu betätigen Sie den Upload-Button.

Bitte achten Sie darauf, dass ActiveSync die Verbindung zum PDA korrekt herstellt.

Der NCP Client Driver und der NCP Client Configurator auf dem PDA müssen nicht gestartet sein.

Beachten Sie jedoch, dass eine eventuell bestehende VPN-Verbindung durch den Upload ohne Vorwarnung getrennt wird.

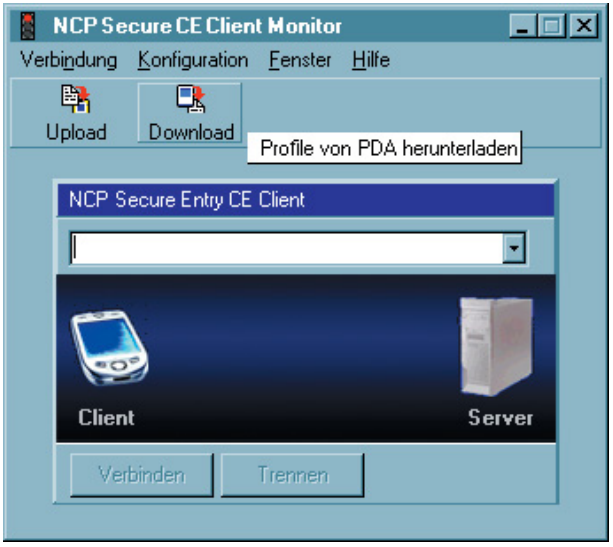


Nachdem der Upload erfolgreich durchgeführt wurde, ...

... muss im PDA-Monitor (Bild links) der gleiche Name in der Zielauswahl stehen wie im PC-Configurator (Bild oben).

Bitte beachten Sie dass eventuell bereits vorhandene Profil-Einstellungen auf dem PDA ohne Rückfrage überschrieben werden.

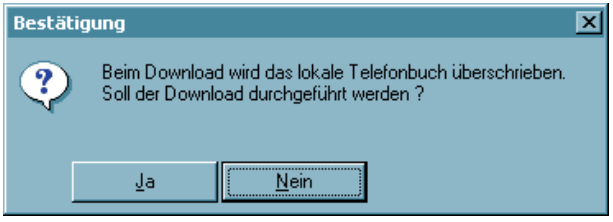
4.6 Download der Profil-Einstellungen



Ein Download der Profil-Einstellungen vom PDA auf den PC ist immer dann nötig, wenn Änderungen in der Konfiguration eines Profils bzw. Zielsystems vorgenommen werden müssen.

Dazu betätigen Sie den Download-Button.

Bitte achten Sie darauf, dass ActiveSync die Verbindung zum PDA korrekt herstellt.



Bei einem Download der Profil-Einstellungen vom PDA werden die Profil-Einstellungen auf dem PC überschrieben.

Um vorhandene Profil-Einstellungen auf dem PC zu erhalten, müssen Sie eigens gesichert werden. Sie befinden sich in dem Verzeichnis:

```
Programme\ncp\ceclient\bin\ncpphone.cfg
```

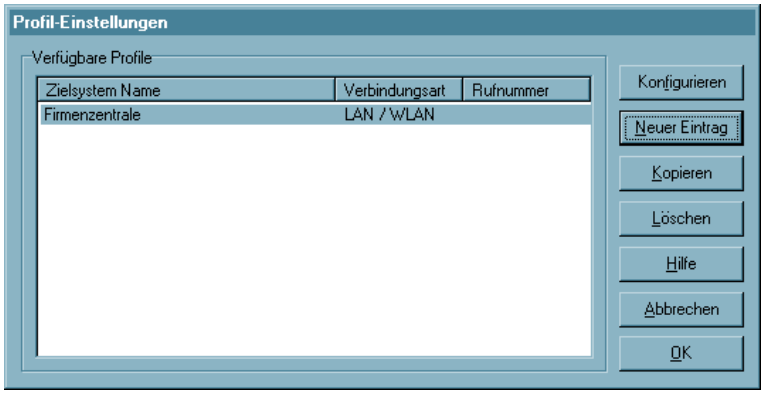
5. Konfigurationsparameter

Die IPSec Client Software gestattet die Einrichtung individueller Profile für entsprechende Zielsysteme, die nach den Benutzeranforderungen konfiguriert werden können.

Im folgenden sind alle Parameterbeschreibungen aufgeführt, und sie sind so angeordnet, wie sie auf der Oberfläche des Client Monitors erscheinen.

5.1 Profil-Einstellungen

Nachdem Sie “Profil-Einstellungen” im Menü des Monitors angeklickt haben, öffnet sich das Menü und zeigt eine Übersicht über die bereits definierten Profile und die Rufnummern der zugehörigen Ziele.



Seitlich finden Sie Buttons, über die Sie die Einstellungen für die Profile (Zielsysteme) modifizieren können.

Um ein neues Profil zu definieren, klicken Sie in der Menüleiste des Monitors auf “Profil-Einstellungen”. Das Menü öffnet sich nun und zeigt die bereits definierten Profile. Klicken Sie jetzt auf “Neuer Eintrag”. Jetzt legt der “Assistent für ein neues Profil” mit Ihrer Hilfe ein neues an. Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Profil angelegt. Für alle weiteren Parameterfelder werden Standardwerte eingetragen.

Um diese Standardwerte zu editieren, d.h. weitere Parameter so einzustellen, wie es den Verbindungsanforderungen zum zugehörigen Zielsystem entspricht, wählen Sie mit der Maus das Profil aus, dessen Werte Sie ändern möchten und klicken anschließend auf “Konfigurieren”.

Um die Definitionen eines bereits definierten Profils zu kopieren, klicken Sie “Kopieren”.

Um ein Profil zu löschen, wählen Sie es aus und klicken “Löschen”.

Parameterfelder:

Die Parameter, die die jeweilige Verbindung über das Profil zu den Zielen spezifizieren, sind in verschiedenen Parameterfeldern gesammelt. In der Kopfzeile steht der Name des Profils (siehe auch → Profil-Einstellungen, Konfigurieren). Seitlich sind die Titel der Parameterfelder angeordnet:

1 ***Grundeinstellungen***

2 ***Netzeinwahl***

3 ***HTTP-Anmeldung***

4 ***Modem***

5 ***Line Management***

6 ***IPSec-Einstellungen***

7 ***Erweiterte IPSec-Optionen***

8 ***Identität***

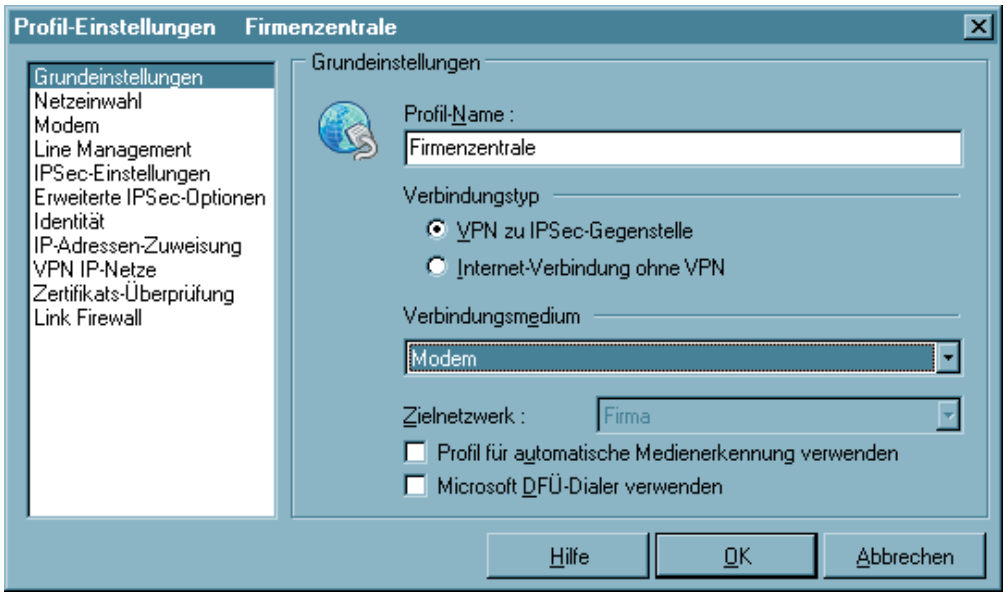
9 ***IP-Adressen-Zuweisung***

10 ***VPN IP-Netze***

11 ***Zertifikats-Überprüfung***

12 ***Link Firewall***

5.1.1 Grundeinstellungen



Im Parameterfeld "Grundeinstellungen" wird der "Profil-Name", den "Verbindungstyp" und das "Verbindungsmedium" zu einem Profil eingegeben.

Parameter:

- ☐ Profil-Name
- ☐ Verbindungstyp
- ☐ Verbindungsmedium
- ☐ Zielnetzwerk
- ☐ Profil für automatische Medienerkennung verwenden
- ☐ Microsoft DFÜ-Dialer verwenden

- **Profil-Name**

Wenn Sie ein neues Profil definieren, sollten Sie zunächst einen unverwechselbaren Namen für dieses System eintragen (z.B. IBM London). Der Name des Profils darf jeden gewünschten Buchstaben wie auch Ziffern beinhalten und darf, Leerzeichen mitgezählt, bis zu 39 Zeichen lang sein.

- **Verbindungstyp**

Alternativ stehen mit dem IPSec Client zwei Verbindungstypen zur Wahl:

VPN zu IPSec-Gegenstelle:

In diesem Fall wählen Sie sich mit dem IPSec Client in das Firmennetz ein (bzw. an das Gateway an). Dazu wird ein VPN-Tunnel aufgebaut.

Internet-Verbindung ohne VPN:

In diesem Fall nutzen Sie den IPSec Client nur zur Einwahl in das Internet. Dabei wird Network Address Translation (IPNAT) weiterhin im Hintergrund genutzt, sodass nur Datenpakete akzeptiert werden, die angefordert wurden.

- **Verbindungsmedium**

Die Verbindungsart kann für jedes Profil eigens eingestellt werden, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem (Windows-)System installiert.

Modem:

Angeschlossene Hardware: Asynchrone Modems (PCMCIA-Modem, GSM-Karte) mit Com Port-Unterstützung;
Netze: Analoges Fernsprechnetz (PSTN) (auch GSM);
Gegenstellen: Modem oder ISDN-Karte mit digitalem Modem;

LAN / WLAN (over IP):

Angeschlossene Hardware: LAN-Adapter, WLAN-Adapter;
Netze: Local Area Network mit Ethernet oder Token Ring, WLAN;
Gegenstellen: Die Gegenstellen des lokalen Multiprotokoll-Routers im LAN oder Access Point;

PocketPC Connection Manager:

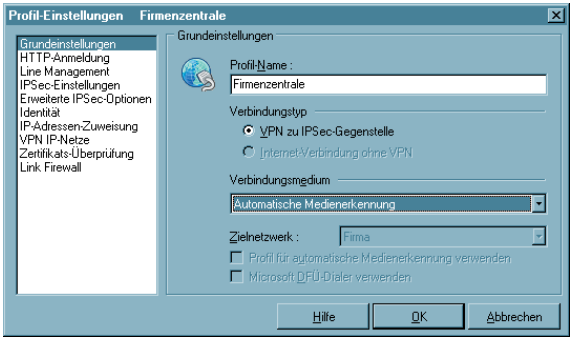
Dieses Verbindungsmedium kann für PocketPC Plattformen eingestellt werden. Es ist ideal für Geräte mit integriertem Telefon (MDA). Während eine GPRS-Verbindung besteht, kann gleichzeitig telefoniert werden. Der PocketPC Connection Manager übernimmt dabei automatisch das Parken der GPRS-Verbindung. Bei der Konfiguration eines Profils für diese Anwendung ist darauf zu achten, dass die Timeout-Spanne genü-

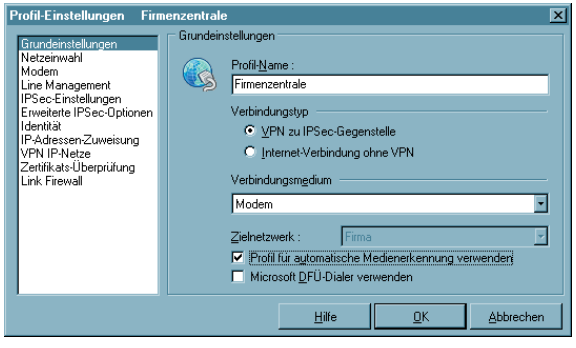
gend groß gewählt wird, bzw. der Timeout deaktiviert ist und Dead Peer Detection (DPD) in den IPSec-Einstellungen deaktiviert ist.

Bei Verwendung dieses Medientyps wird der PocketPC Connection Manager dazu veranlasst eine Verbindung (ins Internet oder Firmennetz) aufzubauen. D.h. der ConnectionManager wird automatisch eine RAS-Verbindung auswählen und aufbauen, oder er erkennt eine schon vorhandene LAN-Karte und baut keine weitere Verbindung auf. Unter “Start / Einstellungen / Verbindungen / Verbindungen”, kann mit Bordmitteln die entsprechende Internet- und Firmenverbindung konfiguriert werden. Ist der virtuelle Adapter aktiv so ist für den sinnvollen Einsatz des Connection Managers genauere projektspezifische Kenntnis der Umgebung nötig.

Automatische Medienerkennung

Werden wechselweise unterschiedliche Verbindungsarten genutzt, wie zum Beispiel Modem und ISDN, so kann die manuelle Auswahl des Zielsystems mit dem jeweils zur Verfügung stehenden Verbindungsmedium entfallen, wenn ein Zielsystem für “Automatische Medienerkennung” konfiguriert wurde und je ein Zielsystem mit den alternativ verfügbaren Verbindungsarten, wie zum Beispiel Modem und ISDN.





Dabei ist zu beachten, dass das Zielsystem mit automatischer Medienerkennung mit allen für die Verbindung zum VPN Gateway nötigen Parametern konfiguriert ist (Bild links oben), wohingegen die Zielsysteme mit den alternativen Verbindungsarten so konfiguriert sein müssen, dass die jeweils gewünschte Verbindungsart (evtl. auch die Modemparameter) eingestellt ist und die Funktion “Eintrag für automatische Medienerkennung” aktiviert ist (Bild links unten). Außerdem müssen für das jeweilige Verbindungsmedium die Eingangsdaten zum ISP im Parameterfeld “Netzeinwahl” gesetzt sein.

Bei einem Verbindungsaufbau erkennt der Client automatisch, welche Verbindungsarten aktuell zur Verfügung stehen und wählt davon die schnellste aus, wobei bei mehreren alternativen Übertragungswegen automatisch der schnellste gewählt wird. In einer Suchroutine ist die Priorisierung der Verbindungsarten in folgender Reihenfolge festgelegt: 1. LAN, 2. WLAN, 3. DSL, 4. UMTS/GPRS, 5. ISDN, 6. MODEM. Die Eingangsdaten für die Verbindung zum ISP werden aus den Telefonbucheinträgen übernommen, die für die automatische Medienerkennung konfiguriert wurden.

■ Profil für automatische Medienerkennung verwenden

Mit Aktivierung dieser Funktion wird dieses Zielsystem an den Telefonbucheintrag für automatische Medienerkennung gebunden und bei Verfügbarkeit des entsprechenden Mediums automatisch für einen potentiellen Verbindungsaufbau herangezogen. Beachten Sie dazu die Beschreibung zur “Verbindungsart”.

Dieses Zielsystem kann auch manuell selektiert werden, um eine Verbindung herzustellen, sofern die Tunnel-Parameter für den Zugang zum VPN Gateway korrekt eingetragen sind.

■ Zielnetzwerk

Bei Einsatz des Verbindungsmediums “PocketPC Connection Manager” kann das Zielnetzwerk ausgewählt werden: Internet oder Firmennetz. Diese Einstellung kann auch nachträglich am PDA über das Popup-Menü geändert werden.

■ Microsoft DFÜ-Dialer verwenden

Zur Einwahl am ISP (Internet Service Provider) kann der Microsoft DFÜ-Dialer genutzt werden. Dies ist immer dann nötig, wenn der Einwahlpunkt ein Einwahl-Script benötigt. Der DFÜ-Dialer unterstützt dieses Script. Im Parameterfenster “Netzeinwahl” wird anschließend die Script-Datei unter Eingabe von Pfad und Namen zur eingespielten Script-Datei eingetragen (siehe → Script-Datei).

NCP-Dialer und Microsoft DFÜ-Dialer

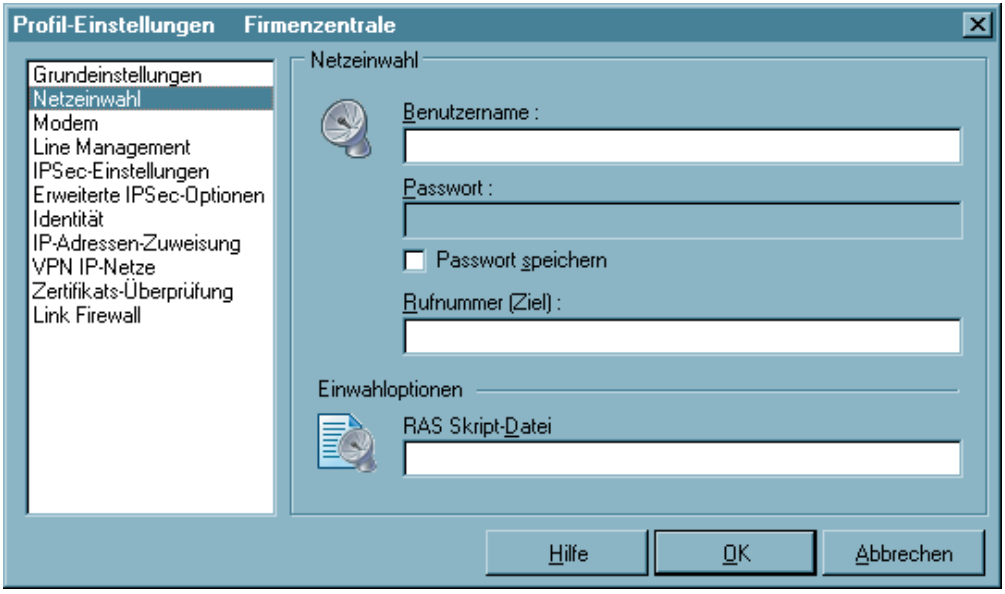
Der CE Client kann sowohl den Microsoft DFÜ-Dialer als auch den NCP-Dialer nutzen. Mit dem NCP-Dialer können Initialisierungs-Strings an Handys (Modems) gesendet werden, sodass GPRS-Verbindungen mit jedem dafür geeigneten Handy aufgebaut werden können (auch V.110).

Der NCP-Dialer ist standardmäßig voreingestellt und muss nicht eigens im Profil unter “Zielsystem” eingestellt werden. Wird für das Zielsystem die Verbindungsart “Modem” gewählt, so kann die Option “Microsoft DFÜ-Dialer verwenden” aktiviert werden. Wird diese Option nicht selektiert, so ist der NCP-Dialer aktiv.

Welcher Dialer genutzt werden soll, hängt davon ab, welche Hardware-Komponente bzw. welches Handy oder Modem für den Verbindungsaufbau eingesetzt wird und ob der Einwahlpunkt (ISP) ein Einwahl-Script benötigt.

Für die Kommunikation über Modem (bzw. Handy) muss das Modem korrekt von Windows CE erkannt worden sein. Treiber für Modems, die den Hayes-Befehlssatz unterstützen, sind in Windows CE integriert. Ebenso unterstützt Windows CE die meisten Handys mit IR-Schnittstelle und eingebautem Modem. Auch Datenverbindungen, zu deren Aufbau ein Initialisierungs-String nötig ist (meist GPRS) sind möglich.

5.1.2 Netzeinwahl



Dieses Parameterfeld beinhaltet den Benutzernamen und das Passwort, die bei der Anwahl an das Zielsystem zur Identifizierung benötigt werden. Diese beiden Größen werden auch für die PPP-Verhandlung zum ISP (Internet Service Provider) benötigt. Das Parameterfeld erscheint überhaupt nicht, wenn der IPSec Client mit dem Verbindungsmedium "LAN over IP" betrieben wird.

Parameter:

- ☐ Benutzername
- ☐ Passwort
- ☐ Passwort speichern
- ☐ Rufnummer (Ziel)
- ☐ Alternative Rufnummern
- ☐ Script-Datei

Benutzername

Mit dem “Benutzernamen” weisen Sie sich gegenüber dem Network Access Server (NAS) aus, wenn Sie eine Verbindung zum Zielsystem aufbauen wollen. Bei Kommunikation über das Internet benötigen Sie den Benutzernamen zur Identifikation am ISP (Internet Service Provider). Der Name für den Benutzer kann bis zu 254 Zeichen lang sein. Für gewöhnlich wird Ihnen ein “Benutzername” vom Zielsystem zugewiesen, da Sie vom Zielsystem (auch Radius- oder LDAP-Server) erkannt werden müssen. Sie erhalten ihn von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Passwort

Das Passwort benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 254 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie vom Zielsystem auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.

Wird der Parameter “Passwort speichern” nicht aktiviert, so muss er bei jedem Verbindungsaufbau das Passwort per Hand eingeben.

Passwort speichern

Dieser Parameter muss aktiviert (angeklickt) werden, wenn gewünscht wird, dass das Passwort und das Passwort Ziel (sofern es eingegeben ist) gespeichert wird. Andernfalls werden die Passwörter gelöscht, sobald der PC gebootet wird oder ein Zielsystem gewechselt wird. Standard ist die aktivierte Funktion.

Wichtig: Bitte beachten Sie, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Client Software arbeiten kann – auch wenn er die Passwörter nicht kennt.

Rufnummer (Ziel)

Für jedes Ziel muss eine Rufnummer definiert sein, da der Client sonst keine Verbindung herstellen kann. Diese Rufnummer muss genauso eingetragen werden, als würden Sie diese Telefonnummer per Hand wählen. D.h. Sie müssen alle notwendigen Vorwahlziffern berücksichtigen: Landesvorwahl, Ortsvorwahl, Durchwahlziffern, etc. etc.
Beispiel: Sie wollen eine Verbindung von Deutschland nach England herstellen
00 (für die internationale Verbindung, wenn Sie von Deutschland aus wählen)
44 (dies ist die landesspezifische Vorwahl für England)
171 (Vorwahl für London)
1234567 (die Nummer, die Sie zu erreichen wünschen)

Insgesamt wird nach diesem Beispiel folgende Nummer im Profil gespeichert und für die Anwahl verwendet: 00441711234567
Die Rufnummer des Ziels kann bis zu 128 Ziffern beinhalten.

Hinweis: Wenn ein Zielsystem eine Verbindung zum PDA über Rückruf aufbauen will, benötigt der Client diese Rufnummer in diesem Feld, um den Rückruf, entsprechend des gewählten Rückrufmodus annehmen zu können.

Amtsholung

Eine eventuell notwendige Amtsholung muss bei Verwendung des NCP-Dialers der "Rufnummer Ziel", im Profil unter "Netzeinwahl", vorangestellt werden. Dies muss bei der Erstellung des Profils mit der PC-Komponente erfolgen und kann nicht nachträglich am PDA geändert werden!

Wird das Microsoft RAS-Dialer verwendet, so kann die Amtsholung nachträglich am PDA geändert werden. Siehe dazu den Abschnitt "Anpassen der Wahlparameter".

■ Alternative Rufnummern

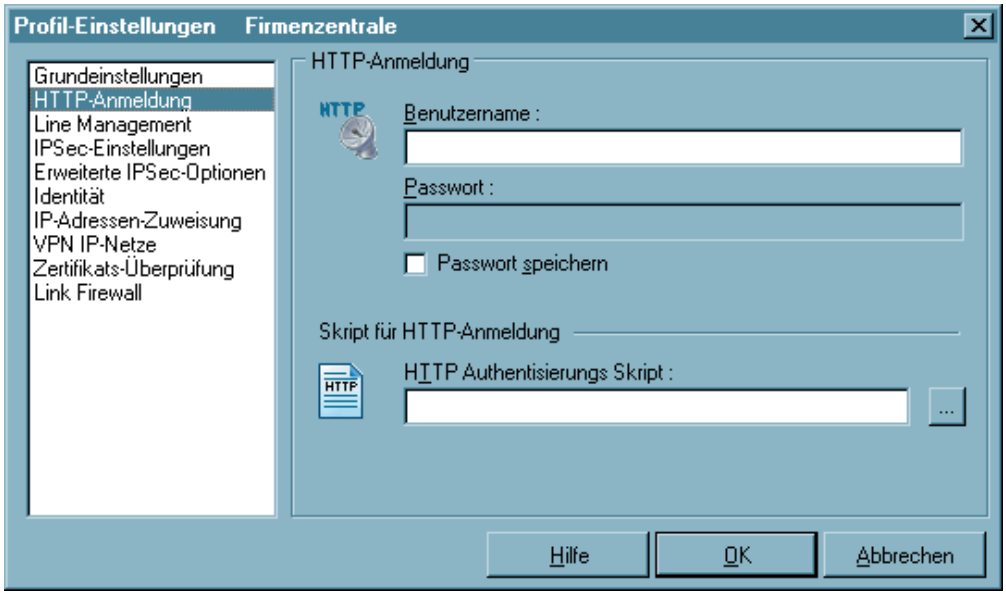
Möglicherweise ist das Zielsystem ein Network Access Server (NAS), der mit mehreren S0-Anschlüssen für verschiedene Rufnummern ausgestattet ist. In diesen Fall empfiehlt es sich, alternative Rufnummern einzugeben – falls zum Beispiel die erste Nummer besetzt ist. Die alternativen Rufnummern werden der ersten Nummer angehängt, nur mit einem Doppelpunkt (:) oder einem Semikolon (;) getrennt. Maximal werden 8 alternative Rufnummern unterstützt.
Beispiel : 00044171123456 7:00044171123456 8
Die erste Nummer ist die Standard-Rufnummer und wird immer zuerst gewählt. Kann keine Verbindung hergestellt werden, weil besetzt ist, wird die zweite Nummer gewählt, usw.

Wichtig: Bitte beachten Sie, dass der Verbindungsaufbau nur funktionieren kann, wenn die Protokoll-Eigenschaften für die Anschlüsse der alternativen Rufnummern die gleichen sind.

■ Script-Datei

Wenn Sie den Microsoft DFÜ-Dialer benutzen, tragen Sie hier die Script-Datei unter Eingabe von Pfad und Namen ein. (Siehe → Grundeinstellungen, Micosoft DFÜ-Dialer verwenden)

5.1.3 HTTP-Anmeldung



Mit den Einstellungen in diesem Parameterfeld kann die automatische HTTP-Anmeldung vorgenommen werden. Zentral erstellte Anmelde-Scripts und die hinterlegten Anmeldedaten können vom Access Point (HotSpot) übernommen werden, ohne dass ein Browserfenster geöffnet wird.

Bitte beachten Sie, dass die Verbindung über einen HotSpot-Betreiber gebührenpflichtig ist. Sie müssen den Geschäftsbedingungen des HotSpot-Betreibers zustimmen, wenn die Verbindung aufgebaut werden soll.

Parameter:

☐ Benutzername | HTTP-Anmeldung

☐ Passwort | HTTP-Anmeldung

☐ Passwort speichern | HTTP-Anmeldung

☐ HTTP Authentisierungs-Script | HTTP-Anmeldung

Mit diesen Daten wird die Anmeldung am HotSpot automatisiert. Dies geschieht in der Weise, dass bei einem Verbindungsaufbau zum Access Point von dort ein HTTP Redirect an den Client mit einer Website zur Anmeldung erfolgt. Anstatt eines Browser-Starts zur HTTP-Authentisierung, erfolgt mit den hier gemachten Eingaben die Authentisierung automatisch im Hintergrund.

Für die script-gesteuerte Anmeldung kann ein Script aus dem Installationsverzeichnis
`<install>\scripts\samples`
für weitere HotSpots entsprechend angepasst werden.

Bei der Verbindungsart WLAN werden die Authentisierungsdaten für den Hotspot aus den WLAN-Einstellungen übernommen, bzw. wenn diese deaktiviert sind, aus dem Management Tool der WLAN-Karte.

- **Benutzername | HTTP-Anmeldung**

  Dies ist der Benutzername, den Sie von Ihrem HotSpot-Betreiber erhalten haben.

- **Passwort | HTTP-Anmeldung**

  Dies ist das Passwort, das Sie von Ihrem HotSpot-Betreiber erhalten haben. Das Passwort wird mit verdeckter Schreibweise (mit *) eingegeben.

- **Passwort speichern | HTTP-Anmeldung**

  Nachdem das Passwort eingegeben wurde, kann es gespeichert werden

- **HTTP Authentisierungs-Script | HTTP-Anmeldung**

  Hier kann nach Klick auf den Suchen-Button [...] das hinterlegte Anmelde-Script selektiert werden.

  Um eingehende Zertifikate bei der HTTP-Authentisierung überprüfen zu können, muss im Script die Variable CACERTDIR gesetzt worden sein. Desweiteren können auch Inhalte des WEB Server-Zertifikats überprüft werden. Hierzu stehen weitere Variablen zur Verfügung:

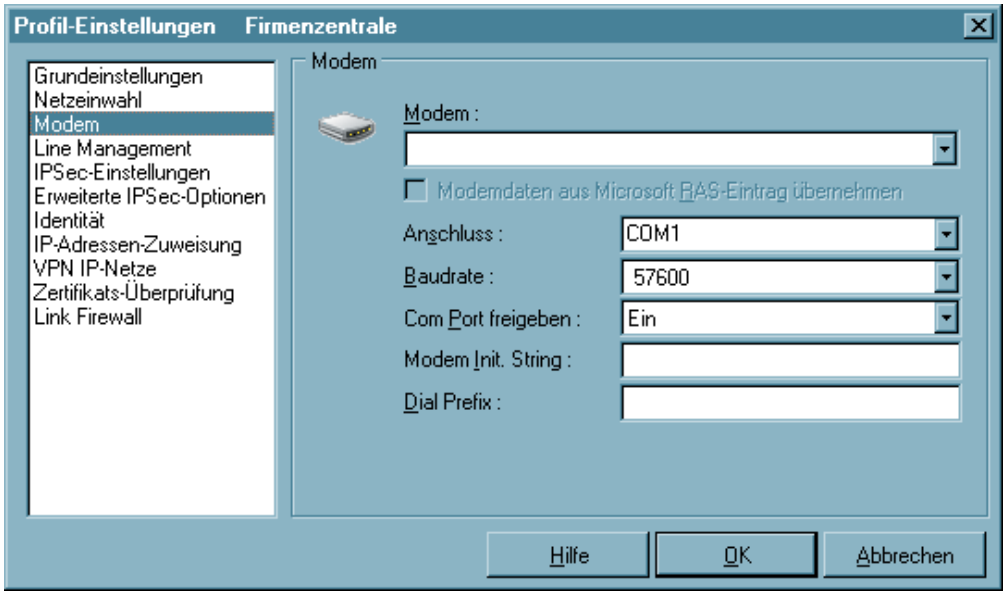
  `CACERTVERIFY_SUBJECT`
  überprüft den Inhalt des Subjects (z.B. cn=WEB Server 1)

  `CACERTVERIFY_ISSUER`
  Überprüft den Inhalt der Issuers

  `CACERTVERIFY_FINGERPRINT`
  überprüft den MD5 Fingerprint des Aussteller-Zertifiats

  Stimmt der Inhalt der Variable mit dem eingegebenen Zertifikat nicht überein, wird die SSL-Verbindung nicht hergestellt und eine Log-Meldung im Monitor ausgegeben.

5.1.4 Modem



Dieses Parameterfeld erscheint ausschließlich, wenn Sie als "Verbindungmedium" "Modem" gewählt haben. Alle nötigen Parameter zu dieser Verbindungsart sind hier gesammelt.

Beachten Sie unbedingt die Absätze zu "NCP-Dialer und Microsoft RAS-Dialer" und zu "Amtsholung" im Abschnitt "Zielsystem", sowie die hier angehängte Beschreibung zu einem neuen Telefonbucheintrag.

Parameter:

☐ Modem

☐ Anschluss

☐ Baudrate

☐ Com Port freigeben

☐ Modem Init. String

☐ Dial Prefix

☐ Modemdaten aus RAS-Eintrag übernehmen

■ Modem

Dieses Parameterfeld zeigt die auf dem PC installierten Modems. Wählen Sie aus der Liste das gewünschte Modem aus.

Je nachdem, welches Modem Sie wählen, werden die zugehörigen Parameter “Com Port” und “Modem Init. String” automatisch in die Konfigurationsfelder des Profils aus der Treiberdatenbank des Systems übernommen.

(Weitere Parameter für dieses Kommunikationsmedium können auch über die Systemsteuerung des PCs konfiguriert werden.)

Hinweis: Bitte beachten Sie, dass Sie das Modem vor der Konfiguration der Verbindung im Profil installiert haben müssen, um es korrekt für Kommunikationsverbindungen nutzen zu können.

■ Anschluss

An dieser Stelle bestimmen Sie, welcher Com Port von Ihrem Modem genutzt werden soll. Wenn Sie bereits Modems unter Windows installiert haben, wird der während dieser Installation festgesetzte Com Port automatisch übernommen, sobald Sie das entsprechende Gerät unter “Modem” auswählen.

Hinweis: Wenn Sie ein bereits unter Ihrem System installiertes Modem nutzen möchten, so wählen Sie vor der Einstellung des Com Ports zuerst das gewünschte Gerät unter “Modem” aus – der entsprechend konfigurierte Com Port wird dann automatisch gesetzt.

■ Baudrate

Die Baudrate beschreibt die Übertragungsgeschwindigkeit zwischen Com Port und Modem. Wenn Ihr Modem z.b. mit 14.4 Kbits übertragen kann, sollten sie die nächsthöhere Baudrate 19200 wählen.

Folgende Baudraten können gewählt werden:
1200, 2400, 4800, 9600, 19200, 38400, 57600 und 115200

Hinweis: Der Microsoft RAS-Dialer unterstützt nicht alle Baudraten bei allen Modems und nicht alle Modems. Wird die gewünschte Rate nicht unterstützt, so wird die vom Treiber vorgegebene Standardrate verwendet. Dieser Vorgang ist für den Benutzer leider nicht einsehbar.

Com Port freigeben

Wenn Sie für Ihren Client ein analoges Modem verwenden, kann es wünschenswert sein, dass der Com Port nach Beendigung der Kommunikation für andere Applikationen freigegeben wird (z.B. Fax). In diesem Fall stellen Sie den Parameter auf “Ein”.

Modem Init. String

Jeder AT-Befehl innerhalb des Initialisierungs-Strings muss mit <cr> abgeschlossen werden, da ansonsten das Kommando nicht abgesetzt wird. Dies bedeutet, dass in jedem Fall der Init-String mit <cr> abgeschlossen werden muss. Beachten Sie außerdem die Anführungszeichen “ innerhalb des Strings und dass keine Leerzeic hen zwischen den Kommandos stehen.

Beispiel zu einem InitString für GPRS über E-Plus:
`AT+cgdcont=1,"IP","internet.eplus.de"<cr>`

Bei Störungen mit einem zusätzlichen ATZ<cr> (bewirkt einen Modem-Reset) vor dem InitString testen.

Dial Prefix

Dieses Feld ist optional. Ist das Modem korrekt installiert und steht der Software als Standardtreiber zur Verfügung, so muss hier kein Eintrag vorgenommen werden. Der Dial Prefix ist nur in seltenen Ausnahmefällen nötig. Ziehen Sie dazu das Modem-Handbuch zu Rate.

Im folgenden einige Beispiele für Dial Prefix:

ATDT
ATDP
ATDI
ATDX

Modemdaten aus RAS-Eintrag übernehmen

Wählt man als Verbindungsart “Modem” und den Microsoft RAS-Dialer so besteht bei der Modem-Konfiguration die zusätzliche Option “Modemdaten aus RAS-Eintrag übernehmen”. Wird diese Option selektiert, so werden unter “Modem” alle im PDA gefundenen RAS-Einträge angezeigt. Aus dem gewählten Eintrag wird die Modemkonfiguration incl. gerätespezifischer Einstellungen für den vom NCP-Client neu angelegten RAS-Eintrag übernommen.

Zu den gerätespezifischen Einstellungen gehört z.B. die Baudrate und der Init-String, nicht jedoch die Telefonnummer. Somit ist es möglich einen Modem Init-String über den Ras-Dialer zu verwenden.

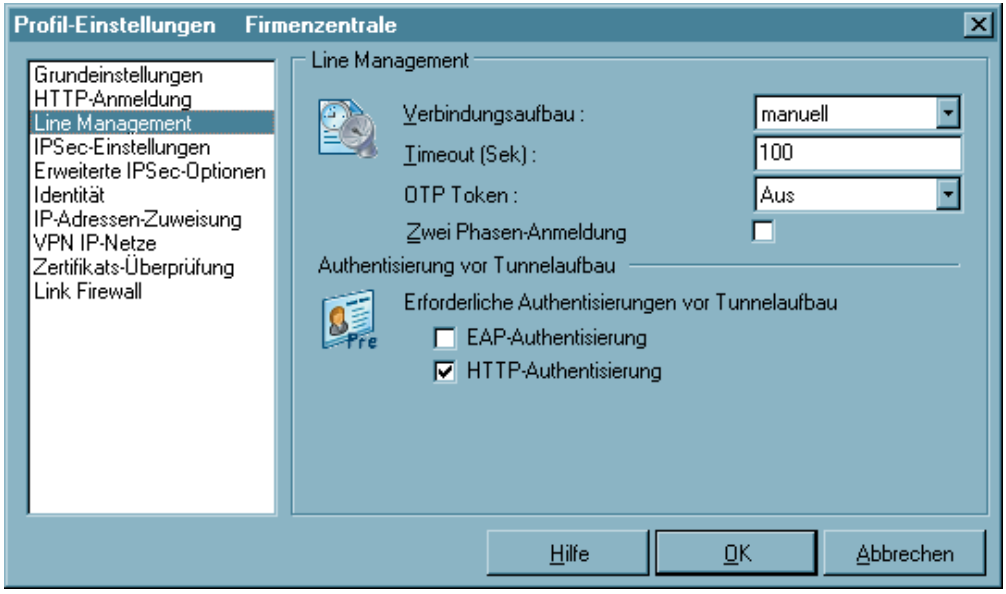
Neuer Telefonbucheintrag mit Modem-Verbindung

Wird ein neues Profil mit Modem-Verbindung erzeugt indem der Button “Neuer Eintrag” gedrückt wird, so wird der Konfigurations-Assistent gestartet. Dieser Assistent unterscheidet nicht zwischen NCP-Dialer und Microsoft RAS-Dialer, sodass alle am PDA vorhandenen Modemtreiber mit Namen aufgeführt werden, bzw. ein Gerät auch unter zwei Namen geführt werden kann, den für RAS und den für den seriellen Com Port (NCP-Dialer). Zudem werden die Namen vom PDAHersteller vorgegeben und können irreführend sein. Z.B. muss beim Compaq iPAQ für eine Infrarot-Verbindung “Com3" und nicht etwa ”IRDA Connection" gewählt werden.

Je nach gewähltem Treibernamen im Assitenten, wird auch der zugehörige Dialer in der Konfiguration des Telefonbuchs automatisch gesetzt.

Ist der Treibername nicht bekannt, muss der Eintrag zur Unterscheidung zwischen NCP- und Microsoft RAS-Dialer eventuell nachkonfiguriert werden, indem im Parameterfenster “Zielsystem” die Funktion entsprechend aktiviert oder deaktiviert wird. Entsprechend werden dann im Parameterfenster “Modem” auch nur die zugehörigen Treibernamen gezeigt.

5.1.5 Line Management



In diesem Parameterfeld bestimmen Sie, wie der "Verbindungsaufbau" erfolgen soll und stellen die Timeout-Werte ein.

Welche Authentisierung vor dem Tunnelaufbau erforderlich ist, wird vom Zielnetzwerk oder vom HotSpot-Betreiber vorgegeben.

Parameter:

☐ Verbindungsaufbau

☐ Timeout

☐ Zwei-Phasen-Anmeldung

☐ EAP-Authentisierung

☐ HTTP-Authentisierung

■ Verbindungsaufbau

Hier definieren Sie, wie die Verbindung zu einem Zielsystem aufgebaut werden soll:

automatisch: (default) Dies bedeutet, dass die Client Software die Verbindung zum Zielsystem automatisch herstellt. Das Trennen der Verbindung erfolgt je nach Protokoll Ihres Systems, entsprechend den Anforderungen der Anwendung und den Einstellungen im Profil.

manuell: In diesem Fall müssen Sie die Verbindung zum Zielsystem manuell herstellen. Ein Trennen der Verbindung erfolgt je nach eingestelltem Wert für den Timeout.

wechselnd: Wird dieser Modus gewählt, muss zunächst die Verbindung “manuell” aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau:
– Wird die Verbindung nun mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung “automatisch” hergestellt,
– wird die Verbindung manuell abgebaut, muss sie auch wieder manuell aufgebaut werden.

Wichtig: Sollten Sie den Verbindungsaufbau auf “manuell” setzen, so sollten Sie den Timeout aktivieren, um den Verbindungsabbau zu automatisieren. Andernfalls könnten unnötige Verbindungskosten für Sie entstehen.

■ Timeout

Mit diesem Parameter wird der Zeitraum festgelegt, der nach der letzten Datenbewegung (Empfang oder Versenden) verstreichen muss, bevor automatisch ein Verbindungsabbau erfolgt. Der Wert wird in Sekunden zwischen 0 und 65535 angegeben. Der Standardwert ist “100". Wenn Ihr Anschluss (ISDN oder analog) einen Gebührenimpuls erhält, verwendet die Client Software das Impulsintervall, um den optimalen Zeitpunkt des Verbindungsabbaus bezüglich dem von Ihnen gesetzten Wert zu ermitteln. Der nach Gebührentakt optimierte Timeout läuft im Hintergrund und hilft die Verbindungskosten zu reduzieren.

Hinweis: Um den Timeout zu aktivieren, ist es nötig, einen Wert zwischen 1 und 65356 einzutragen. Mit dem Wert “0" wird der automatische Timeout (Verbindungsabbau) nicht ausgeführt. Der Wert ”0" bedeutet, dass das Trennen der Verbindung manuell durchgeführt werden muss. Ziehen Sie bei diesem Parameter bitte Ihren Internet Provider oder Ihren Systemadministrator zu Rate.

Wichtig: Der Timer für das gewählte Zeitintervall läuft erst dann an, wenn keine Datenbewegung oder Handshaking mehr auf der Leitung stattfindet.

■ Zwei Phasen-Anmeldung

Mit dieser Funktion erfolgt zunächst eine Einwahl ins Internet, sodass z.B. eine Authentisierung auf einer Website möglich ist. Erst durch erneutes Klicken auf den Verbinden-Button in der grafischen Oberfläche des CE Clients erfolgt der Aufbau der VPN-Tunnelverbindung.

EAP-Authentisierung

Muss sich der Client mit EAP (Extensible Authentication Protocol) authentisieren, so muss diese Funktion aktiviert werden. Sie bewirkt, dass für dieses Zielsystem die EAP-Konfiguration im Monitor-Menü unter “EAP-Optionen” zum Einsatz kommt.

Bitte beachten Sie, dass die EAP-Konfiguration im Monitor-Menü für alle Zielsysteme gültig ist und aktiv geschaltet sein muss, wenn diese linkspezifische Einstellung wirksam sein soll.

EAP wird dann eingesetzt, wenn für das wireless LAN ein Access Point verwendet wird, der 802.1x-fähig ist und eine entsprechende Authentisierung verlangt. EAP kann aber auch dann eingesetzt werden, wenn der Client über einen Router auf ein anderes Netzsegment des Firmennetzes zugreifen möchte. Generell wird mit EAP verhindert, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.

Nach Konfiguration des EAP muss eine Statusanzeige im grafischen Feld des Monitors erscheinen. Ist dies nicht der Fall, so muss die EAP-Konfiguration im Monitor-Menü aktiv geschaltet werden. Durch einen Doppelklick auf das EAP-Symbol kann das EAP zurückgesetzt werden. Anschließend erfolgt die EAP-Verhandlung erneut.

HTTP-Authentisierung

Für die automatische HTTP-Authentisierung am Access Point (HotSpot) muss diese Funktion aktiviert werden.

Damit wird ein weiteres Parameterfeld “HTTP-Anmeldung” im Telefonbuch zugeschaltet, in welches im folgenden die Authentisierungsdaten eingegeben werden können (siehe oben → HTTP-Anmeldung).

5.1.6 IPSec-Einstellungen

In diesem Parameterfeld geben Sie die IP-Adresse des Gateways ein. Darüber hinaus legen Sie die Richtlinien fest, die für die IPSec-Verbindung in der Phase 1- und Phase 2-Verhandlung verwendet werden sollen. Sofern der automatische Modus genutzt wird, akzeptiert der Client die Richtlinien, wie sie vom Gateway der Gegenstelle vorgegeben werden. Soll der IPSec Client als Initiator der Verbindung eigene Richtlinien verwenden, so müssen diese mit dem Richtlinien-Editor konfiguriert werden. Die erweiterten Optionen können nach Abstimmung mit der Gegenstelle eingesetzt werden.

Parameter:

- ☐ Gateway
- ☐ IKE-Richtlinie
- ☐ IPSec-Richtlinie
- ☐ Richtlinien-Gültigkeit
- ☐ Richtlinien-Editor
- ☐ Exch. Mode
- ☐ PFS-Gruppe
- ☐ IP-Kompression (LZS) verwenden
- ☐ DPD (Dead Peer Detection) deaktivieren

Gateway

Dies ist die IP-Adresse des IPSec Gateways, auch Tunnel-Endpunkt. Sie erhalten die Adresse von Ihrem Administrator entweder als Hex-Adresse, wenn das Gateway über eine feste offizielle IP-Adresse verfügt – oder als Namens-String, wenn das Gateway eine wechselnde IP-Adresse von einem Internet Service Provider erhält.

Hex-Adresse: Die Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennte Zahlen.

Namens-String: Sie tragen den Namen ein, den Sie von Ihrem Administrator erhalten haben. Es handelt sich dabei um den DNS-Namen des Gateways, der beim DynDNS Service Provider hinterlegt wurde.

IKE-Richtlinie

Die IKE-Richtlinie wird aus der Listbox ausgewählt. In der Listbox werden alle IKE-Richtlinien aufgeführt, die Sie im Richtlinien-Editor unter der Verzweigung “IKE-Richtlinie” angelegt haben. Die Richtlinien erscheinen in der Box mit dem Namen, den Sie bei der Konfiguration vergeben haben.

Sie finden zwei vorkonfigurierte Richtlinien im Richtlinien-Editor unter “IKE-Richtlinie” als “Pre-shared Key” und “RSA-Signatur”. Inhalt und Name dieser Richtlinien können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf (siehe → IKE-Richtlinie (editieren)), d.h. eine Richtlinie besteht aus verschiedenen Vorschlägen. Funktional unterscheiden sich diese Richtlinien durch Verwendung eines statischen Schlüssels bzw. einer RSA-Signatur.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Automatischer Modus: In diesem Fall kann die Konfiguration der IKE-Richtlinie mit dem im Richtlinien-Editor entfallen. Die Richtlinie wird vom Gateway der Gegenstelle vorgegeben und vom Client akzeptiert.

Pre-shared Key: Diese vorkonfigurierte Richtlinie kann ohne PKI-Unterstützung genutzt werden. Beidseitig wird der gleiche “Statische Schlüssel” verwendet (siehe → Pre-shared Key verwenden, Shared Secret im Parameterfeld “Identität”).

RSA-Signatur: Diese vorkonfigurierte Richtlinie kann nur mit PKI-Unterstützung eingesetzt werden. Als zusätzliche, verstärkte Authentisierung ist der Einsatz der RSA-Signatur nur sinnvoll unter Verwendung einer Smart Card oder eines Soft-Zertifikats.

■ IPSec-Richtlinie

Die IPSec-Richtlinie wird aus der Listbox ausgewählt. In der Listbox werden alle IP-Sec-Richtlinien aufgeführt, die Sie mit dem Richtlinien-Editor angelegt haben. Die Richtlinien erscheinen in der Box mit dem Namen, den sie bei der Konfiguration vergeben haben.

Funktional unterscheiden sich zwei IPSec-Richtlinien nach dem IPSec-Sicherheitsprotokoll AH (Authentication Header) oder ESP (Encapsulating Security Payload). Da der IPSec-Modus mit AH-Sicherung für flexiblen Remote Access völlig ungeeignet ist, wird nur die IPSec-Richtlinie mit ESP-Protokoll, “ESP - 3DES - MD5", standardmäßig vorkonfiguriert mit der Software ausgeliefert.

Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu IPSec-Protokoll und Authentisierung auf (siehe → IPSec-Richtlinie (editieren)), d.h. eine Richtlinie besteht aus verschiedenen Vorschlägen.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Automatischer Modus: In diesem Fall kann die Konfiguration der IKE-Richtlinie mit dem Richtlinien-Editor entfallen.

ESP - 3DES - MD5 (oder anderer Name): Wenn Sie den Namen der vorkonfigurierten IPSec-Richtlinie wählen, muss die gleiche Richtlinie mit all ihren Vorschlägen für alle Benutzer gültig sein. Dies bedeutet, dass sowohl auf Client- als auch auf Server-Seite die gleichen Vorschläge für die Richtlinien zur Verfügung stehen müssen.

■ Exch. Mode

Der Exchange Mode (Austausch-Modus) bestimmt wie der Internet Key Exchange vonstatten gehen soll. Zwei unterschiedliche Modi stehen zur Verfügung, der Main Mode, auch Identity Protection Mode und der Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch deren Verschlüsselung.

Main Mode: Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch Identity Protection Mode.

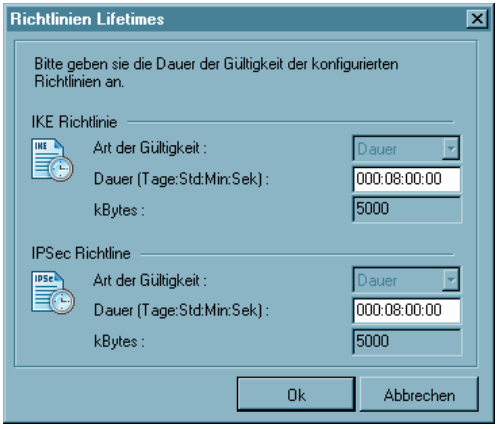
Aggressive Mode: Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.

■ PFS-Gruppe

Mit Auswahl einer der angebotenen Diffie-Hellman-Gruppen wird festgelegt, ob ein kompletter Diffie-Hellman-Schlüsselaustausch (PFS, Perfect Forward Secrecy) in Phase 2 zusätzlich zur SA-Verhandlung stattfinden soll. Standard ist “keine”.

Richtlinien-Gültigkeit

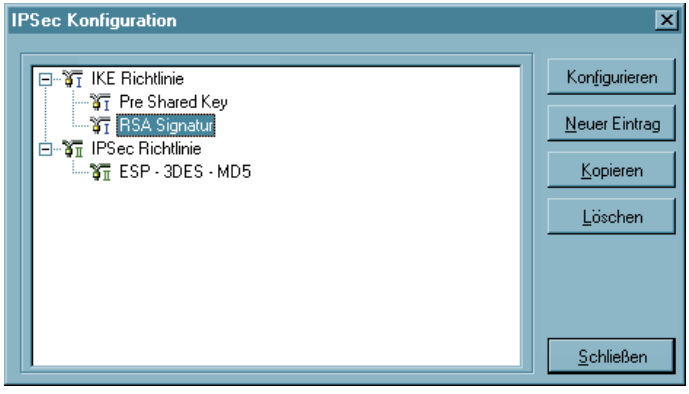
Die hier definierte Dauer der Gültigkeit gilt für alle Richtlinien gleichermaßen.



- **Dauer**

Die Größe der Zeitspanne kann eigens eingestellt werden.

Richtlinien-Editor



Zur Konfiguration der Richtlinien und gegebenenfalls einer statischen Secure Policy Database wird dieser Menüpunkt angeklickt. Damit öffnet sich ein Konfigurationsfenster mit der Verzweigung der Richtlinien und Secure Policy Database zu IPSec, sowie Buttons zur Bedienung auf der rechten Seite des Konfigurationsfensters.

Um die (Standard-)Werte der Richtlinien zu editieren, wählen Sie mit der Maus die Richtlinie, deren Werte Sie ändern möchten – die Buttons zur Bedienung werden dann aktiv.

Konfigurieren
Um eine Richtlinie oder eine SPD abzuändern, wählen Sie mit der Maus den Namen, der Gruppe deren Werte Sie ändern möchten und klicken auf “Konfigurieren”. Dann öffnet sich das entsprechende Parameterfeld mit den IPSec-Parametern.

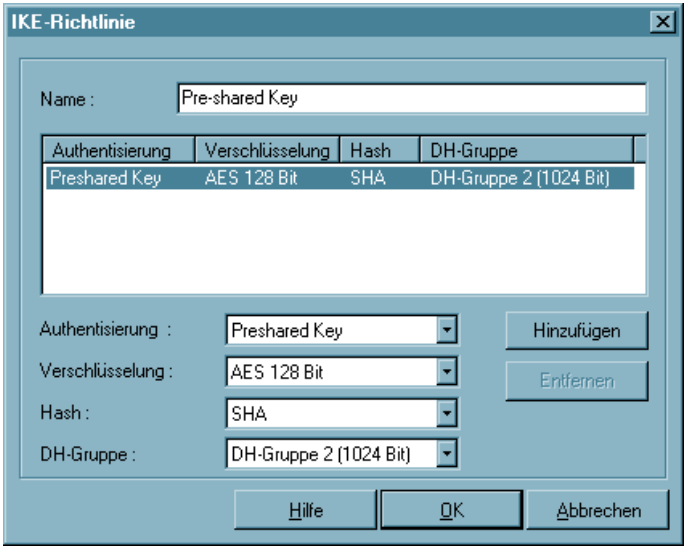
Neuer Eintrag
Wenn Sie eine neue Richtlinie oder SPD anlegen möchten, selektieren Sie eine der Richtlinien oder die SPD und klicken auf “Neuer Eintrag”. Die neue Richtlinie oder SPD wird erzeugt. Alle Parameter sind auf Standardwerte gesetzt, bis auf den Namen.

Kopieren
Um die Parameter-Einstellungen eines bereits definierten Richtlinie oder SPD zu kopieren, markieren sie die zu kopierende Richtlinie oder SPD und klicken auf “Kopieren”. Daraufhin wird das Parameterfeld geöffnet. Ändern Sie nun den Namen und klikken Sie anschließend Ok. Die neue Richtlinie oder SPD ist nun angelegt. Die Parameterwerte sind zu denen der kopierten identisch, bis auf den Namen.

Löschen
Wenn Sie eine Richtlinie oder SPD aus dem Konfigurationsbaum löschen wollen, selektieren Sie sie und klicken auf “Löschen”. Die Richtlinie oder SPD ist damit auf Dauer aus der IPSec-Konfiguration gelöscht.

Schließen
Wenn Sie das IPSec-Feld schließen, kehren Sie zum Monitor zurück. Die Daten werden so wie sie konfiguriert wurden behalten.

IKE-Richtlinie (editieren)



Die Parameter in diesem Feld beziehen sich auf die Phase 1 des Internet Key Exchange (IKE) mit dem der Kontrollkanal für die SA-Verhandlung aufgebaut wird. Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in dem Parameterfeld “IPSec-Richtlinien”. Die IKE-Richtlinien, die Sie hier konfigurieren, werden zur Auswahl gelistet.

Inhalt und Name dieser Richtlinien können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf, d.h. eine Richtlinie kann aus mehreren Vorschlägen bestehen.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Buttons “Hinzufügen” und “Entfernen” erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

Name | IKE-Richtlinie

Geben Sie dieser Richtlinie einen Namen, über den sie später einer SPD zugeordnet werden kann.

Authentisierung | IKE-Richtlinie

Bevor der Kontrollkanal für die Phase 1-Verhandlung (IKE Security Association) aufgebaut werden kann, muss beidseitig eine Authentisierung stattgefunden haben.

Zur gegenseitigen Authentisierung wird der allen gemeinsame pre-shared Key (statischer Schlüssel) verwendet. Diesen Schlüssel definieren Sie im Parameterfeld “Identität”.

Verschlüsselung | IKE-Richtlinie

Nach einem der optionalen Verschlüsselungsalgorithmen erfolgt die symmetrische Verschlüsselung der Messages 5 und 6 im Kontrollkanal, sofern der Main Mode (Identity Protection Mode) gefahren wird. Zur Wahl stehen: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

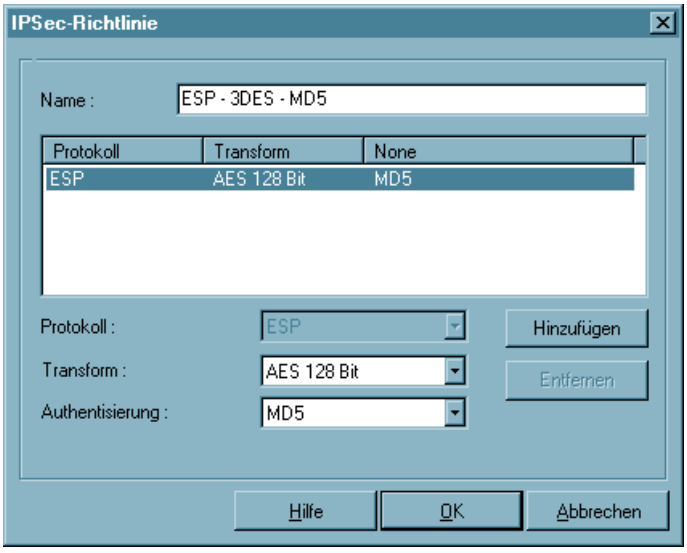
Hash | IKE-Richtlinie

Modus, wie der Hash-Wert über die ID bzw. das Zertifikat der Messages im Kontrollkanal gebildet wird. Zur Wahl stehen: MD5 (Message Digest, Version 5) und SHA (Secure Hash Alogrithm).

DH-Gruppe | IKE-Richtlinie

Mit der Wahl einer der angebotenen Diffie-Hellman-Gruppen wird festgelegt, wie sicher der Key Exchange im Kontrollkanal erfolgen soll, nach dem der spätere symmetrische Schlüssel erzeugt wird. Je höher die DH Group desto sicherer ist der Key Exchange.

IPSec-Richtlinie (editieren)



Die IPSec-Richtlinien (Phase-2-Parameter), die Sie hier konfigurieren, werden zur Auswahl für die SPD gelistet.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Buttons "Hinzufügen" und "Entfernen" erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

- **Name | IPSec-Richtlinie**

  Geben Sie dieser Richtlinie einen Namen, über den Sie sie später einer SPD zuordnen können.

- **Protokoll | IPSec-Richtlinie**

  Der fest eingestellte Standardwert ist ESP.

- **Transformation | IPSec-Richtlinie**

  Wenn das Sicherheitsprotokoll ESP eingestellt wurde, kann hier definiert werden wie mit ESP verschlüsselt werden soll. Zur Wahl stehen die gleichen Verschlüsselungsalgorithmen wie für Layer 2: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

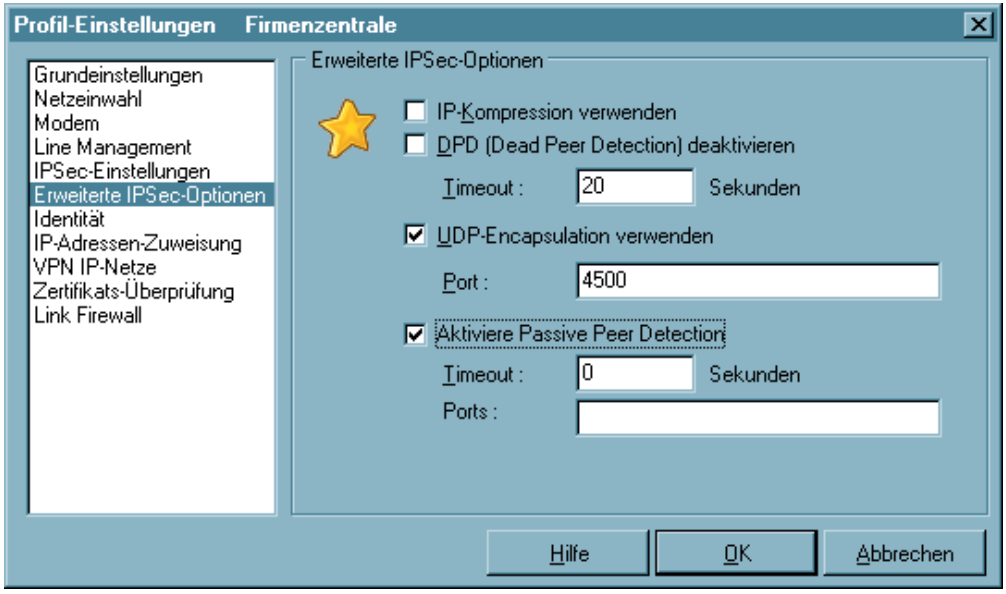
- **Transformation (Comp) | IPSec-Richtlinie**

  IPSec-Kompression. Die Datenübertragung mit IPSec kann ebenso komprimiert werden wie ein Transfer ohne IPSec. Dies ermöglicht eine Steigerung des Durchsatzes um maximal das 3-fache. Nach Selektion des Protokolls "Comp" (Kompression) kann zwischen LZS- und Deflate-Kompression gewählt werden.

- **Authentisierung | IPSec-Richtlinie**

  Für das Sicherheitsprotokoll ESP kann der Modus der Authentisierung eigens eingestellt werden. Zur Wahl stehen: MD5 und SHA.

5.1.7 Erweiterte IPSec-Optionen



In diesem Parameterfeld können weiterte Einstellungen vorgenommen werden.

Parameter:

☐ IP-Kompression (LZS) verwenden

☐ DPD (Dead Peer Detection) deaktivieren

☐ UDP-Encapsulation verwenden

☐ Aktiviere Passive Paar Detection

■ IP-Kompression (LZS) verwenden

Die Datenübertragung mit IPSec kann ebenso komprimiert werden wie ein Transfer ohne IPSec. Dies ermöglicht eine Steigerung des Durchsatzes um maximal das 3-fache.

■ DPD (Dead Peer Detection) deaktivieren

DPD (Dead Peer Detection) und NAT-T (NAT Traversal) werden automatisch im Hintergrund ausgeführt, sofern dies das Ziel-Gateway unterstützt. Der IPSec Client nutzt DPD, um in regelmäßigen Intervallen, die in Sekunden eingestellt werden können, zu prüfen, ob die Gegenstelle noch aktiv ist. Ist dies nicht der Fall erfolgt ein automatischer Verbindungsabbau.

Mit dieser Funktion kann DPD ausgeschaltet werden.

Mit DPD (Dead Peer Detection) wird das VPN Gateway aktiv (nach eingestelltem Zeitintervall) unabhängig vom tatsächlichen Nutzdatenverkehr “angepingt” und der Tunnel abgebaut, wenn keine Antwort vom Gateway erfolgt oder der Timeout abgelaufen ist (unabhängig vom Datenaufkommen). Über eine GPRS/UMTS-Verbindung kann DPD daher ein Datenaufkommen erzeugen, das ungewollte Kosten verursacht.

■ Aktiviere Passive Peer Detection

Wenn Hintergrund-Anwendungen aktiv sind bei einer GPRS/UMTS-Verbindung, die volumenabhängig (ohne Flatrate) abgerechnet werden, dann ist PPD sinnvoll.

Mit PPD wird der Timeout dann aufgezogen, wenn die Anwendung Daten zum Gateway schickt. Eingehende Daten vom Gateway stoppen den Timer wieder. Wenn der Timeout für PPD gänzlich abgelaufen ist, wird der Tunnel abgebaut.

Der Timeout für PPD kann in Sekunden eingegeben werden.

PPD ist ein Feature der Client Software, wobei das Gateway keine zusätzliche Funktion unterstützen muss. Die jeweilige Anwendung, für die PPD genutzt werden soll, wird über den TCP-Ziel-Port identifiziert, der hier eingegeben werden muss.

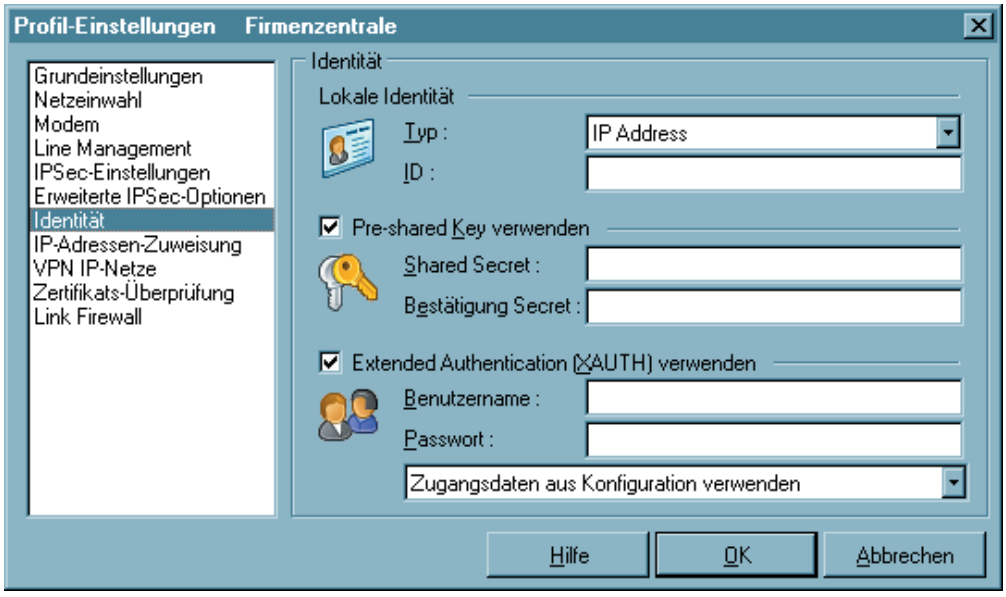
■ UDP-Encapsulation verwenden

Mit UDP-Encapsulation muss an der externen Firewall nur der Port 4500 freigeschaltet werden (anders bei NAT Traversal oder UDP 500 mit ESP). Wird die UDP-Encapsulation verwendet, so kann der Port frei gewählt werden.

Standard für IPSec mit UDP ist der Port 4500, für IPSec ohne UDP der Port 500.

Das NCP Gateway erkennt die UDP-Encapsulation automatisch.

5.1.8 Identität



Entsprechend des Sicherheitsmodus IPSec können noch detailliertere Sicherheitseinstellungen vorgenommen werden.

Parameter:

☐ Typ | Identität

☐ ID | Identität

☐ Pre-shared Key verwenden

☐ Extended Authentication (XAUTH) verwenden

☐ Benutzername | Identität

☐ Passwort | Identität

☐ Zugangsdaten aus Konfiguration verwenden

Typ | Identität

Bei IPSec wird zwischen abgehenden und eingehenden Verbindungen unterschieden. Der Wert, den der Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein.

Folgende ID-Typen stehen zur Auswahl:
– IP Address
– Fully Qualified Domain Name
– Fully Qualified Username
(entspricht der E-Mail-Adresse des Benutzers)
– IP Subnet Address
– ASN1 Distinguished Name
– ASN1 Group Name
– Free String used to identify Groups

ID | Identität

Bei IPSec wird zwischen abgehenden und eingehenden Verbindungen unterschieden. Der Wert, den der Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein.

Entsprechend dem ID-Typ muss die zugehörige ID als String eingetragen werden.

Pre-shared Key verwenden

Der Pre-shared Key ist ein String beliebiger Zeichen in einer maximalen Länge von 255 Zeichen. Alle alphanumerischen Zeichen können verwendet werden. Wenn die Gegenstelle einen pre-shared Key während der IKE-Verhandlung erwartet, dann muss dieser Schlüssel in das Feld “Shared Secret” eingetragen werden.

Bestätigen Sie das “Shared Secret” im darunter liegenden Feld. Der gleiche pre-shared Key muss auf beiden Seiten verwendet werden.

Extended Authentication (XAUTH) verwenden

Wird “IPSec-Tunneling” genutzt, so kann die Authentisierung über Extended Authentication (XAUTH Protokoll, Draft 6) erfolgen. Wird XAUTH eingesetzt und vom Gateway untersützt, so aktivieren Sie “Benutze erweiterte Authentisierung (XAUTH)”. Zusätzlich zum pre-shared Key können dann noch folgende Parameter gesetzt werden:

Benutzername = Benutzername des IPSec-Benutzers

Passwort = Kennwort des IPSec-Benutzers

Benutzername | Identität

Den Benutzernamen für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

Hinweis: Dieser Parameter wird nur benötigt, um Zugriff auf das Gateway der remote Seite zu bekommen.

Passwort | Identität

Das Passwort für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

Hinweis: Dieser Parameter wird nur benötigt, um Zugriff auf das Gateway der remote Seite zu bekommen.

Zugangsdaten aus Konfiguration verwenden

Als Zugangsdaten für das VPN können folgende Einträge ausgelesen und verwendet werden:

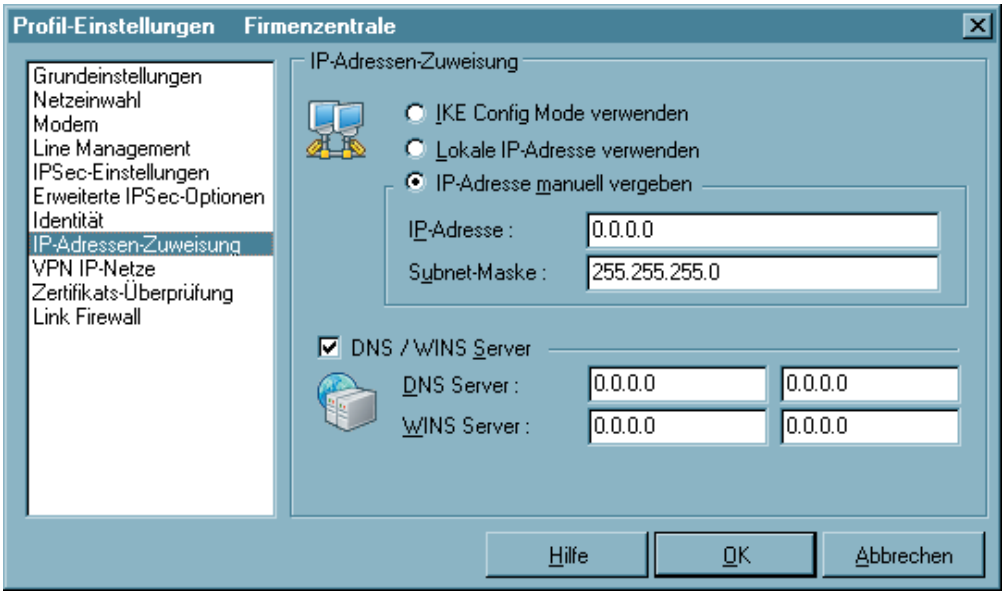
Zugangsdaten aus Konfiguration verwenden:
Dies bedeutet, dass die in diesem Parameterfeld unter “Benutzername” und “Passwort” gemachten Angaben zur erweiterten Authentisierung verwendet werden.

Zugangsdaten aus Zertifikat (E-Mail) verwenden:
Dies bedeutet, dass statt “Benutzername” und “Passwort” der E-Mail-Eintrag des Zertifikats verwendet wird.

Zugangsdaten aus Zertifikat (Common Name) verwenden:
Dies bedeutet, dass statt “Benutzername” und “Passwort” der Benutzer-Eintrag des Zertifikats verwendet wird.

Zugangsdaten aus Zertifikat (Seriennummer) verwenden:
Dies bedeutet, dass statt “Benutzername” und “Passwort” die Seriennummer des Zertifikats verwendet wird.

5.1.9 IP-Adressen-Zuweisung



In diesem Parameterfenster wird eingestellt, wie die IP-Adressen vergeben werden sollen. Außerdem kann der durch die PPP-Verhandlung automatisch zugewiesene Server durch alternative Server ersetzt werden. Dazu muss in den Netzwerk-Einstellungen des Betriebssystems der DNS-Modus eingestellt sein.

Parameter:

☐ IKE Config Mode verwenden

☐ Lokale IP-Adresse verwenden

☐ IP-Adresse manuell vergeben

☐ DNS/WINS

☐ DNS-Server

☐ WINS-Server

IKE Config Mode verwenden

IP-Adressen und DNS Server werden über das Protokoll IKE-Config Mode (Draft 2) zugewiesen. Für die NAS-Einwahl können alle bisherigen WAN-Schnittstellen verwendet werden.

Bei “IPSec-Tunneling” wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau. Der Einsatz von NAT Traversal erfolgt beim Client automatisch und ist immer nötig, wenn auf Seiten des Zielsystems ein Gerät mit Network Address Translation zum Einsatz kommt.

Lokale IP-Adresse verwenden

In diesem Fall wird die aktuell in den Netzwerkeinstellungen des PCs konfigurierte IP-Adresse (auch DHCP) für den IPSec Client genutzt.

IP-Adresse manuell vergeben

Dies ist die IP-Adresse und die Subnet-Maske, die hier frei eingegeben werden können. In diesem Fall wird die hier eingetragene Adresse genutzt, unabhängig von der Konfiguration in den Netzwerkeinstellungen.

DNS/WINS

Mit IKE Config Mode werden dynamisch IP-Adressen des Clients, des DNS- und WINS-Servers sowie der Domain Name zugewiesen.

Wird diese Funktion aktiviert, so kann alternativ zu dem DNS/WINS-Server, der automatisch während der PPP-Verhandlung zum NAS/ISP zugewiesen wird, ein anderer DNS/WINS Server bestimmt werden.

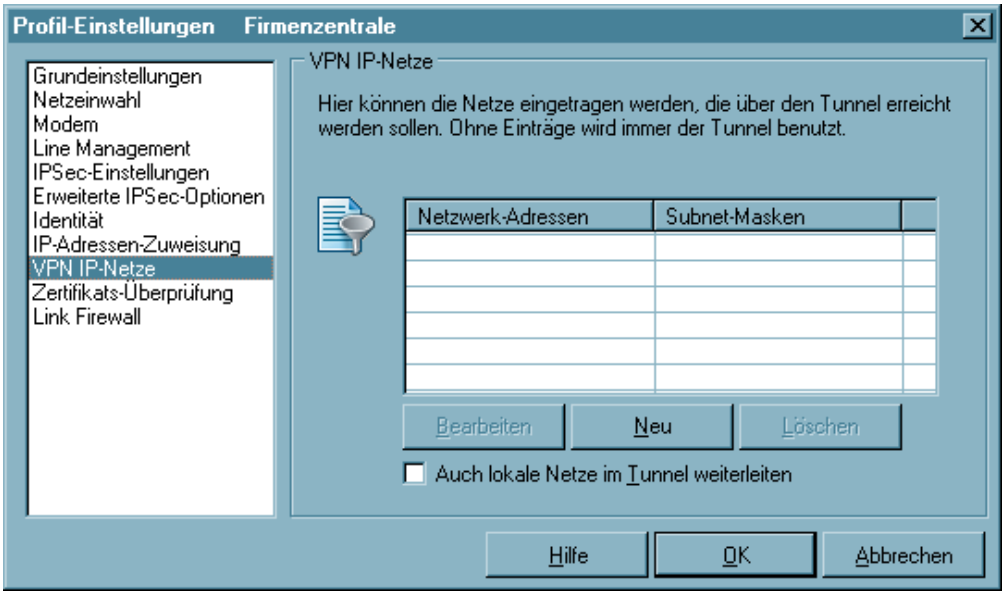
DNS-Server

Der zuerst eingetragene DNS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt.

WINS-Server

Der zuerst eingetragene WINS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt.

5.1.10 VPN IP-Netze



Hier können genau die IP-Netze definiert werden, über die der Client via VPN-Tunnel kommunizieren kann. Wenn Tunneling genutzt wird und hier keine Einträge erfolgen, so wird die Verbindung immer zum Tunnel-Endpunkt des Gateways aufgebaut. Soll alternierend einerseits ein Tunneling zur Zentrale erfolgen, andererseits über das Internet kommuniziert werden, so müssen hier die IP-Netze eingetragen werden, die vom Client erreicht werden sollen. Sie können dann zwischen dem Internet und dem Gateway der Firmenzentrale hin und her springen. Dies wird auch als "Split Tunneling" bezeichnet.

Parameter:

☐ Netzwerk-Adressen | VPN IP-Netze

☐ Subnet-Masken

☐ Auch lokale Netze im Tunnel weiterleiten

■ Netzwerk-Adressen | VPN IP-Netze

In diesem Parameterfenster definieren Sie, in welchem IP-Netz oder welchen IP-Netzen der Client über VPN-Tunneling kommunizieren kann. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Bitte achten Sie ferner darauf, daß die IP-Adresse des Gateways nicht im Bereich der Netz-Adresse liegt.

■ Subnet-Masken

Hier tragen Sie die zugehörige Netzmaske des IP-Netzes ein. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Bitte achten Sie darauf, daß die IP-Adresse des Gateways nicht im Bereich der Netz-Adresse liegt.

■ Auch lokale Netze im Tunnel weiterleiten

Wenn der Datenverkehr des lokalen Netzes über VPN-Tunneling weitergeleitet werden soll, so muss diese Funktion aktiviert werden.

5.1.11 Zertifikats-Überprüfung

Im Parameterfeld "Zertifikats-Überprüfung" kann pro Zielsystem des IPSec Clients vorgegeben werden, welche Einträge in einem Zertifikat der Gegenstelle (Gateway) vorhanden sein müssen (siehe → Eingehendes Zertifikat anzeigen, Allgemein).

Siehe auch:

- ☐ Benutzer des eingehenden Zertifikats
- ☐ Aussteller des eingehenden Zertifikats
- ☐ Fingerprint des Aussteller-Zertifikats
- ☐ SHA1 Fingerprint verwenden
- ☐ Weitere Zertifikats-Überprüfungen

Benutzer des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Benutzers, soweit bekannt – auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu, welche Einträge bei “eingehendes Zertifikat anzeigen” unter Benutzer aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

```
cn     = Common Name / Name
s      = Surname / Nachname
g      = Givenname / Vorname
t      = Title / Titel
o      = Organisation / Firma
ou     = Organization Unit / Abteilung
c      = Country / Land
st     = State / Bundesland, Provinz
l      = Location / Stadt, Ort
email  = E-mail
```

Beispiel:
`cn=VPNGW*, o=ABC, c=de`
Der Common Name des Security Servers wird hier nur bis zur Wildcard “*” überprüft. Alle nachfolgenden Stellen können beliebig sein, etwa 1 - 5 als Numerierung. Die Organzation Unit muss in diesem Fall immer ABC sein und das Land Deutschland.

Aussteller des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Ausstellers, soweit bekannt – auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu welche Einträge bei “eingehendes Zertifikat anzeigen” unter Aussteller aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

```
cn     = Common Name / Name
s      = Surname / Nachname
g      = Givenname / Vorname
t      = Title / Titel
o      = Organisation / Firma
ou     = Organization Unit / Abteilung
c      = Country / Land
st     = State / Bundesland, Provinz
l      = Location / Stadt, Ort
email  = E-mail
```

Beispiel:
`cn=ABC GmbH`
Hier wird nur der Common Name des Ausstellers überprüft.

■ Fingerprint des Aussteller-Zertifikats

Um zu verhindern, dass ein Unberechtigter, der die vertrauenswürdige CA imitiert, ein gefälschtes Aussteller-Zertifikat verwenden kann, kann zusätzlich der Fingerprint des Ausstellers, soweit bekannt, eingegeben werden.

■ SHA1 Fingerprint verwenden

Der Algorithmus zur Erzeugung des Fingerprints kann MD5 (Message Digit 5) oder SHA1 (Secure Hash Algorithm 1) sein.

Weitere Zertifikats-Überprüfungen

Neben der Zertifikats-Überprüfung nach Inhalten erfolgt am IPSec Client eine weitere Zertifikatsprüfung in mehrfacher Hinsicht.

1. Auswahl der CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies geschieht dadurch, dass er die CA-Zertifikate seiner Wahl in das Windows-Verzeichnis \ncple\cacerts\ gespielt. Das Einspielen kann bei einer Software-Distribution mit Disketten automatisiert stattfinden, wenn sich die Aussteller-Zertifikate bei der Installation der Software im Root-Verzeichnis der ersten Diskette befinden. Nachträglich können Aussteller-Zertifikate automatisch über den Secure Update Server verteilt werden (siehe → Handbuch zum Update Server), oder – sofern der Benutzer über die notwendigen Schreibrechte in genanntem Verzeichnis verfügt – von diesem selbst eingestellt werden (siehe → CA-Zertifikate anzeigen).

Derzeit werden die Formate *.pem und *.crt für Aussteller-Zertifikate unterstützt. Sie können im Monitor unter dem Hauptmenüpunkt “Verbindung, Zertifikate, CA-Zertifikate anzeigen” eingesehen werden.

Wird am IPSec Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Verzeichnis NCPLE\CACERTS\. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande.

Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

2. Überprüfung der Zertifikats-Erweiterung

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zerifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den IPSec Client und das Gateway sind drei Erweiterungen von Bedeutung:
– extendedKeyUsage
– subjectKeyIdentifier
– authorityKeyIdentifier

extendedKeyUsage:

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der IPSec Client, ob der definierte erweiterte Verwendungszweck “SSL-Server-Authentisierung” enthalten ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck “SSL-Server-Authentisierung” beinhalten muss. Dies gilt auch bei einem Rückruf an den Client über VPN.

subjectKeyIdentifier / authorityKeyIdentifier:

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann keine Übereinstimmung erkannt werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades.

(Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.)

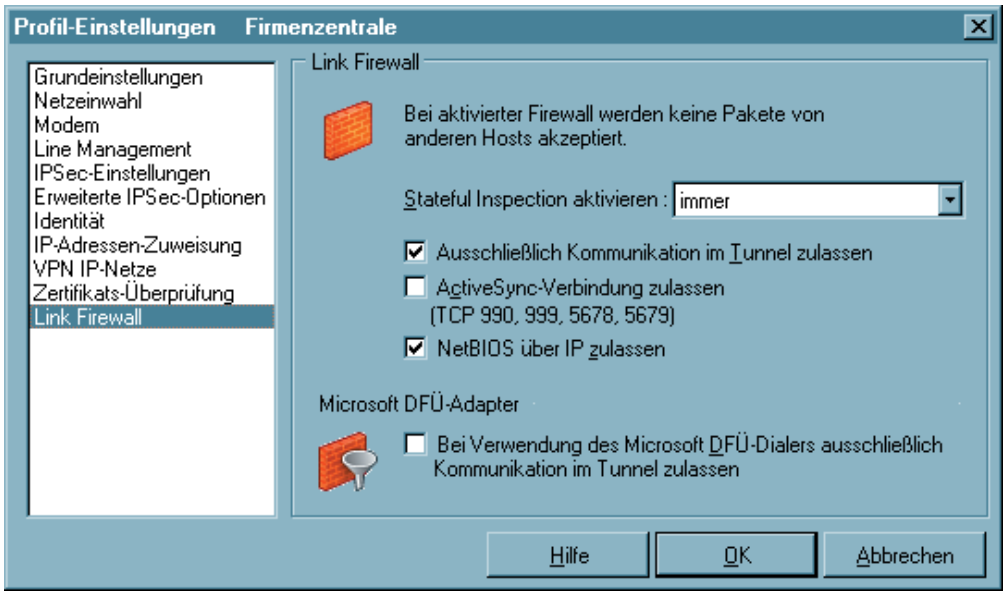
3. Überprüfung von Sperrlisten

Zu jedem Aussteller-Zertifikat kann dem IPSec Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Windows-Verzeichnis \ncple\crls\ gespielt. Ist eine CRL vorhanden, so überprüft der IPSec Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Gleiches gilt für eine ARL (Authority Revocation List), die in das Windows-Verzeichnis \ncple\arls\ gespielt werden muss.

Sind eingehende Zertifikate in den Listen von CRL oder ARL enthalten, wird die Verbindung nicht zugelassen.

Sind CRLs oder ARLs nicht vorhanden findet keine diesbezügliche Überprüfung statt.

5.1.10 Link Firewall



Die Firewall-Einstellungen können für alle Netzwerkadapter wie auch für RAS-Verbindungen genutzt werden. Die aktivierte Firewall wird in der grafischen Oberfläche des Clients als Symbol (Mauer mit Pfeil) dargestellt. Grundsätzliche Aufgabe einer Firewall ist es, zu verhindern, dass sich Gefahren aus anderen bzw. externen Netzen (Internet) in das eigene Netzwerk ausbreiten. Deshalb wird eine Firewall auch am Übergang zwischen Firmennetz und Internet installiert. Sie prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis vorher festgelegter Konfigurationen, ob ein Datenpaket durchgelassen wird oder nicht. Die hier zu aktivierende Firewall arbeitet nach dem Prinzip der Stateful Inspection. Stateful Inspection ist eine neue Firewall-Technologie und bietet den derzeit höchstmöglichen Sicherheitsstandard für Internet-Verbindungen und somit das Firmennetz. Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen verhindert diese Funktionalität den unbefugten Zugriff auf Daten und Ressourcen im zentralen Datennetz. Zum anderen überwacht sie als Kontrollinstanz den jeweiligen Status aller bestehenden Internet-Verbindungen. Die Stateful Inspection Firewall erkennt darüber hinaus, ob eine Verbindung "Tochterverbindungen" geöffnet hat – wie beispielsweise bei FTP oder Netmeeting – deren Pakete ebenfalls weitergeleitet werden müssen. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf (siehe → Handbuch, Beispiele und Erklärungen).

Parameter:

- ☐ Stateful Inspection aktivieren
- ☐ Ausschließlich Kommunikation im Tunnel zulassen
- ☐ ActiveSync-Verbindung zulassen
- ☐ NetBIOS über IP zulassen
- ☐ Bei Verwendung des MS DFÜ-Dialers ausschließlich Kommunikation im Tunnel zulassen

■ Stateful Inspection aktivieren

aus: Die Sicherheitsmechanismen der Firewall werden nicht in Anspruch genommen.

immer: Die Sicherheitsmechanismen der Firewall werden immer in Anspruch genommen, d.h. auch wenn keine Verbindung aufgebaut ist, ist der PC vor unberechtigten Zugriffen geschützt.

bei bestehender Verbindung: Der PC ist dann nicht angreifbar, wenn eine Verbindung besteht.

ActiveSync-Verbindungen werden als normale TCP-Verbindungen von der Link Firewall behandelt. Obwohl ActiveSync die TCP-Verbindung in beide Richtungen (PC ⟷ PDA) etabliert, wird bei aktiviertem Stateful Inspection-Filter in der Link Firewall zugelassen. Die Verbindung wird gesperrt, wenn “Ausschließlich Kommunikation im Tunnel zulassen” aktiviert ist.

Auch komprimierte Verbindungen des RAS-Dialers können vom Client als normaler IP-Verkehr überwacht werden, da sowohl die Kompression (CCP) als auch die VanJacobson-IP-Header-Kompression (im IPCP) nicht mehr ausgehandelt werden.

■ Ausschließlich Kommunikation im Tunnel zulassen

Ausschließlich Kommunikation im Tunnel zulassen: Bei aktivierter Firewall kann diese Funktion zusätzlich eingeschaltet werden, um in ein- und ausgehender Richtung ausschließlich VPN-Verbindungen zuzulassen.

■ ActiveSync-Verbindung zulassen

ActiveSync-Verbindungen werden als normale TCP-Verbindungen von der Link Firewall behandelt. Obwohl ActiveSync die TCP-Verbindung in beide Richtungen (PC <—> PDA) etabliert, wird die ActiveSync-Kommunikation bei aktiviertem Stateful Inspection-Filter in der Link Firewall zugelassen.

Die ActiveSync-Verbindung wird dann gesperrt, wenn “Ausschließlich Kommunikation im Tunnel zulassen” aktiviert ist. Um bei dieser Einstellung die ActiveSync-Verbindung zuzulassen, muss die Funktion “ActiveSync-Verbindung zulassen” aktiviert werden.

Die (globale) Firwall muss bei einer Direktverbindung (über USB, seriell oder Infrarot) für ActiveSync freigeschaltet werden. Dies erfolgt in den Firewall-Einstellungen des Monitors unter “Optionen - ActiveSync-Verbindungen (TCP 990, 999, 5678, 5679, 26675, 5721) zulassen”. Diese Einstellung kann auch am PDA über das Popup-Menü vorgenommen werden, wenn die (globale) Firewall aktiv ist.

Unter Windows Mobile 5.0 wird eine ActiveSync-Verbindung über die USB-Schnittstelle des PCs unabhängig von Firewall-Regeln zugelassen. Bei älteren Betriebssystemen oder ActivSync-Verbindung über alternative Schnittstellen, z. B. über Bluetooth, muss die Verbindung über den Parameter “ActiveSync zulassen” freigeschaltet werden.

Wird ActiveSync über Netzwerk betrieben (LAN oder WLAN), so muss zusätzlich manuell eine eigene Firewall-Regel für die Namensauflösung (DNS/WINS) erstellt werden.

- **NetBIOS über IP zulassen**

Mit diesem Parameter wird ein Filter aufgehoben, der Microsoft NetBios Frames unterdrückt. Diesen Filter aufzuheben, um den Verkehr von NetBios Frames zu gestatten, ist immer dann zweckmäßig, wenn Sie zum Beispiel Microsoft Networking über den IPSec Client nutzen.

In der Standardeinstellung ist dieser Filter gesetzt, das heißt der Checkbutton nicht mit einem Haken markiert, so dass Microsoft NetBios Frames unterdrückt werden, damit sie den Datenverkehr nicht unnötig belasten. Markieren Sie den Checkbutton mit einem Haken, werden NetBios Frames over IP erlaubt.

- **Bei Verwendung des Microsoft DFÜ-Dialers ausschließlich Kommunikation im Tunnel zulassen**

Bei Verwendung des Client-Monitors wird bei Aktivierung dieser Funktion verhindert, dass eine Kommunikation über den DFÜ-Dialer zum Internet stattfinden kann.

6. Eine Verbindung herstellen

Bitte beachten Sie, dass vor einem Verbindungsaufbau verschiedene Einstellungen vorgenommen werden müssen. Die Art des Verbindungsaufbaus zum Zielsystem legen Sie bei der Konfiguration mit der PC-Komponente fest, die Einstellungen der Wahlparameter definieren Sie am PDA.

Schlägt ein Verbindungsaufbau fehl, so werden Fehlercodes als roter Text im grafischen Feld des Monitors angezeigt. Diese Meldungen wurden so erweitert, dass bei einem Scheitern eines Verbindungsaufbaus immer ein Text angezeigt wird, wenn der Client den Fehlversuch erkennt. Es kann z. B. kein Fehler angezeigt werden, wenn die Verbindung über den Server wieder getrennt wurde.

6.1 Die Art des Verbindungsaufbaus zum Zielsystem

Die Client Software gestattet die Definition verschiedenster Zielsysteme, die je nach Anforderung benannt und vorher mit der PC-Komponente konfiguriert werden können.

Sobald die Software installiert und das Telefonbuch auf den PDA übertragen wurde, kann die Anwahl an ein Zielsystem stattfinden. Dabei ist auch die Art der Anwahl Bestandteil der Konfiguration eines Zielsystems. Sie können aus drei Anwahl-Modi für den Verbindungsaufbau wählen: automatisch, manuell und wechselnd. Sie definieren den Modus des Verbindungsaufbaus für ein Zielsystem im Telefonbuch unter “Verbindungssteuerung / Verbindungsaufbau”.

Automatischer Verbindungsaufbau:

Die Verbindung wird, entsprechend den Parametern des Zielsystems, automatisch aufgebaut. Auch wenn Sie für den Verbindungsaufbau “automatisch“ gewählt haben, müssen Sie die Verbindung beim ersten Mal manuell aufbauen.

Manueller Verbindungsaufbau:

Es ist auch möglich manuell die Verbindung zu einem ausgewählten Ziel herzustellen, indem Sie in der Button-Leiste des PDA-Monitors “Verbinden” aktivieren.

Wechselnder Verbindungsaufbau:

Wird dieser Modus gewählt, muss zunächst die Verbindung “manuell” aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau wie folgt:
– Wird die Verbindung mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung “automatisch” hergestellt,
– wird die Verbindung “manuell” abgebaut, muss sie auch wieder “manuell” aufgebaut werden.

6.2 Anpassung der Wahlparameter

Vor der Anwahl mit dem PDA-Monitor müssen Sie die Wahlparameter bzw. das Wählmuster am PDA konfigurieren bzw. neu anlegen. Dazu aktivieren Sie unter Pocket 2002 das Menü zu den Systemeinstellungen wie folgt:

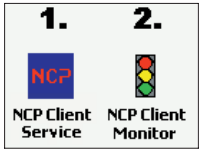
Aus dem Startmenü wählen Sie →
Einstellungen, danach →
Verbindungen, danach nochmals →
Verbindungen, dann →
Wahlparameter und schließlich →
Wählmuster (siehe Bild rechts)

Hier ändern Sie die Einstellungen für Ortsgespräche, Ferngespräche und Auslandsgespräche ab, indem Sie jeweils ein “G” eintragen (siehe Bild) und bestätigen diese Konfiguration mit OK.

Nur so ist gewährleistet, dass der CE Client die in seinem Telefonbuch eingetragene Nummer wählt. Ist später eine andere Vorwahl nötig, z.B. zur Amtsholung in einem Hotel, so kann der entsprechende Eintrag ergänzt werden.

6.3 Starten

Bevor eine Verbindung hergestellt werden kann, muss am PDA zunächst der Service und anschließend der Monitor gestartet werden. Dazu selektieren Sie aus der Programmgruppe die jeweiligen Icons (siehe Bild rechts).

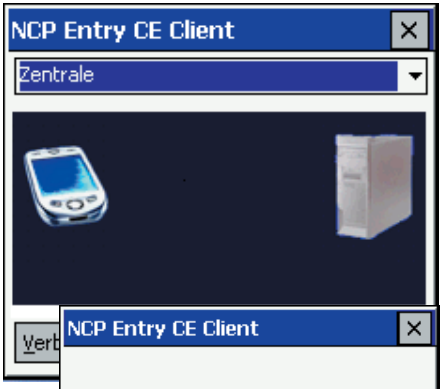


Vergessen Sie außerdem nicht die Smart Card einzustecken bzw. den Reader zu initialisieren, wenn Sie PKI mit Smart Cardsnutzen! In diesem Fall muss nach dem Start des Monitors ein Smart Card-Symbol dargestellt werden (siehe Bild rechts)

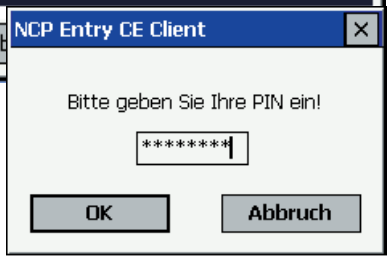
6.4 Verbinden

Gleich in welcher Art die Verbindung aufgebaut wird, der Monitor, sofern er im Vordergrund sichtbar ist, zeigt immer den Status des Verbindungsaufbaus wie in folgendem Beispiel an:

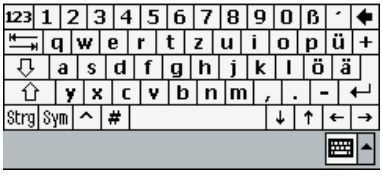
Zunächst wird das Zielsystem über den Auswahl-Button ausgewählt.



Danach wird die Verbindung hergestellt – hier manuell über den Button “Verbinden”.



Wurde die Verwendung eines (Soft-)Zertifikats konfiguriert – wie bei der Testverbindung mit SSL – so muss zunächst die PIN eingegeben werden.



Anschließend wird eine Verbindung zum Internet Service Provider (ISP) hergestellt (gelbe Linie).

Die Einwahl dorthin hat erfolgreich statt gefunden, wenn der grüne Globus erscheint.

Die Authentisierung am VPN Gateway wird als Händeschütteln dargestellt.

Die erfolgreich durchlaufenen Stationen werden als kleine Symbole unter der grünen Linie dargestellt.

Zusätzlich kann noch eine Verschlüsselung konfiguriert werden (Schlüssel).

(Wenn die Konfiguration der Gegenstelle darauf eingestellt ist, kann auch Kompression konfiguriert werden.)

Ist die letzte Station des Verbindungsaufbaus (hier die Verschlüsselung, bzw. Entschlüsselung) durchlaufen, ist die Verbindung damit hergestellt!

6.4.1 Passwörter und Benutzernamen

Das Passwort (siehe → Netzeinwahl, Passwort) benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 256 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie vom Zielsystem auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.

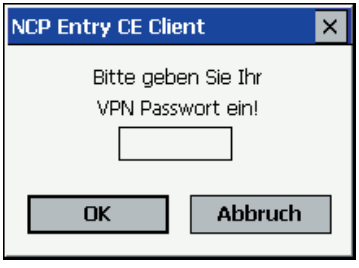
Benutzernamen und Passwörter für die Einwahl zum NAS und zum VPN Gateway (siehe → Tunnel-Parameter) können in der Konfiguration des Zielsystems vollständig eingegeben werden. Der “VPN-Benutzername” *muss* bei der Konfiguration eingegeben werden.

Ein einmal eingegebenes Passwort bleibt gespeichert bis
– das Profil gewechelt wird oder
– der Dienst neu gestartet wird oder
– über manuellen Verbindungsaufbau ein anderes Passwort eingegeben wird

Nicht eingegebene Benutzernamen und Passwörter werden bei der Einwahl dynamisch abgefragt (siehe Bild rechts).

6.4.2 Zugangsdaten speichern im Passwort- und XAUTH-Dialog

Sowohl im Passwort-Dialog als auch im XAUTH-Dialog gibt es die Möglichkeit, die Zugangsdaten für das jeweils aktuelle Profil zu speichern.



■ **XAUTH-Dialog mit Tokencode-Eingabefeld**

Ist die Option “OTP für NAS- oder VPN-Passwort” aktiv, so werden in den XAUTH-Dialogen zwei Eingabefelder angezeigt:
– eines für die PIN (mit maskierter Eingabe)
– eines für den Tokencode (mit lesbarer Eingabe)
Das endgültige Passwort ergibt sich durch Aneinanderhängen der Werte beider Felder.

Wird ein Passwort gespeichert (siehe oben) erscheint dieser Dialog nicht. Wird das Passwort falsch eingegeben oder muss es geändert werden so erscheinen die Standard XAUTH-Dialoge, mit den vom Gateway vorgegebenen Eingabefeldern. (Z. B. PocketPC- und Smartphone-Variante).

6.4.3 Disable Auto-PowerOff

Wird der PDA längere Zeit nicht benutzt, schaltet er automatisch ab in den Stromsparmodus. Dies kann auch geschehen, während eine VPN-Verbindung aktiv ist. Im Client-Monitor kann dieser Automatismus ausgeschaltet werden. Dazu gehen Sie wie folgt vor: Halten Sie den Eingabestift einige Sekunden auf das grafische Feld des Monitors gedrückt, dann erscheint ein Popup-Menü über das die aktuelle Einstellung angezeigt wird und geändert werden kann. Schalten Sie hier auf “Disable Auto-Poweroff”, um ein Abschalten des PDAs zu verhindern (standard).

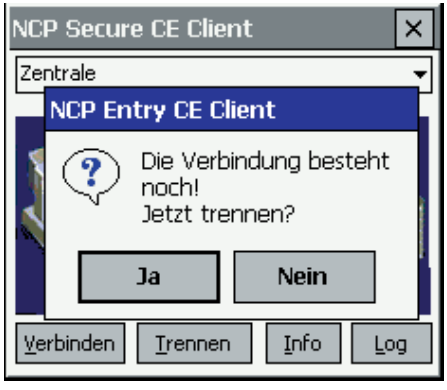
6.5 Trennen

Mit dem Button “Trennen“ im PDA-Monitor wird der Abbau der aktuell bestehenden Verbindung manuell durchgeführt. Wenn Sie die Möglichkeit behalten wollen, jederzeit die Verbindung manuell abbauen zu können, setzen Sie bei der Konfiguration mit der PC-Komponente den Verbindungsaufbau auf “manuell” und deaktivieren den automatischen Timeout, indem Sie ihn auf Null (0) setzen (siehe → Verbindungsaufbau).

6.5.1 Trennen und Beenden des Monitors

Besteht eine Verbindung noch, und wird der PDA-Monitor mit dem Schließen-Button beendet, so wird nicht automatisch die Verbindung getrennt. Soll die möglicherweise kostenpflichtige Verbindung bestehen bleiben, obwohl der Monitor beendet wird, so wird dazu ausdrücklich eine Bestätigung von der Software verlangt (siehe Bild unten).

Klicken Sie in diesem Bestätigungsfenster auf “Nein”, so haben Sie auf Ihrer Desktop-Oberfläche kein Icon und keinen Hinweis mehr darauf, dass noch eine Verbindung aktiv ist und Gebühren anfallen können! In diesem Fall müssen Sie den Monitor erneut starten, um die bestehende Verbindung korrekt zu beenden!



7. Beispiele und Erklärungen

In diesem Abschnitt des Handbuchs werden einige Grundbegriffe des Routings und des IPSec-Verkehrs erklärt. Anhand von Beispielen wird die Konfiguration des IPSec Clients für bestimmte Funktionalitäten dargestellt.

7.1 IP-Funktionen

Um ein IP-Netzwerk korrekt zu konfigurieren, müssen die Regeln der IP-Adressierung eingehalten werden. Untenstehend sind einige Richtlinien und Terminologien aufgeführt. Zu weiteren Informationen über IP-Netzwerke wird entsprechende Fachliteratur empfohlen.

7.1.1 Geräte eines IP-Netzwerks

IP-Adressen werden den Schnittstellen der Geräte eines IP-Netzwerks zugewiesen. Diese Geräte werden auch als Hosts oder Rechner bezeichnet. Mehrfach vernetzten Geräten (z.B. Router) können auch mehrere Adressen zugeordnet werden. Der Begriff Host-Adresse bezeichnet die IP-Adresse des Rechners eines IP-Prozesses, unabhängig von der tatsächlichen physikalischen Struktur des Geräts oder der Schnittstellen.

7.1.2 IP-Adress-Struktur

IP-Adressen haben eine Länge von vier Oktetten, 32 Bits (4 Bytes), und werden in dezimaler oder hexadezimaler Schreibweise mit Punkt "." getrennt notiert. Zum Beispiel:

```
198.10.6.27 oder
C6.0A.06.1B oder
0xC6.0x0A.0x06.0x1B
```

Die Adressen werden getrennt in einen Netzwerk-Abschnitt, der das zugehörige Netz adressiert, und eine lokale Adresse, dem sogenannten "Restfeld" (auch Host-Abschnitt), der das jeweilige Gerät innerhalb des Netzwerks adressiert. Alle Geräte innerhalb eines einzelnen Netzwerks haben denselben Netzwerk-Abschnitt gemeinsam. Jedes Gerät (Host) hat dabei sein eigenes Restfeld.

Es gibt drei Klassen von Internet-Adressen, je nachdem wieviele Bytes der IP-Adresse für Netzwerk-Abschnitt und Restfeld verwendet werden.

Klasse (Class) A, große Netzwerke: Netzwerknummern 1 - 127

Bei Adressen der Klasse A ist das höchste Bit gleich Null, die nächsten sieben Bits entsprechen dem Netzwerk und die verbleibenden 24 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 1 Byte (max. 126 unterschiedliche Netzwerke)

Restfeld beansprucht 3 Bytes (max. 2 hoch 24 = 16.777.216 verschiedene Geräte)

Damit können max. 127 unterschiedliche Netzwerke, jedes mit max. 16.777.216 verschiedenen Geräten, adressiert werden.

Klasse (Class) B, mittlere Netzwerke: Netzwerknummern 128 - 191

Bei Adressen der Klasse B haben die beiden höchsten Bits die Werte 1 und 0, die nächsten 14 Bits entsprechen dem Netzwerk und die verbleibenden 16 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 2 Byte (max. 16.384 unterschiedliche Netzwerke)

Restfeld beansprucht 2 Bytes (max. 2 hoch 16 = 65.536 verschiedene Geräte)

Damit können max. 16.384 unterschiedliche Netzwerke, jedes mit max. 65.526 verschiedenen Geräten, adressiert werden.

Klasse (Class) C, kleine Netzwerke: Netzwerknummern 192 - 223

Bei Adressen der Klasse C haben die drei höchsten Bits die Werte 1, 1 und 0, die folgenden 21 Bits entsprechen dem Netzwerk und die letzten 8 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 3 Bytes (max. 2.097.152 unterschiedliche Netzwerke)

Restfeld beansprucht 1 Byte (max. 256 verschiedene Geräte)

Damit können max. 2.097.152 unterschiedliche Netzwerke, jedes mit max. 256 verschiedenen Geräten, adressiert werden.

Beispiel:

```
           Netz    Host
Klasse A: 122. | 087.   156.   045
Klasse B: 162.   143. | 085.   132
Klasse C: 195.   076.   212. | 024
```

Bitte beachten Sie bei der Adressvergabe, dass für einen einzelnen physikalischen Rechner mehrere IP-Adressen verwendbar sein müssen. Eine Workstation kann mit einer IP-Adresse auskommen. Ein Router benötigt für jede seiner Schnittstellen eine IP-Adresse, mindestens jedoch zwei – eine für den Anschluss zum lokalen Netz (LAN IP-Adresse), eine für den Anschluss zur WAN-Seite.

7.1.3 Netzmasken (Subnet Masks)

In einem Wide Area Network können verschiedene, physikalisch getrennte Netze (LANs) dem gleichen Netzwerk (WAN) mit der gleichen Netzwerknummer angehören. Anhand dieser Netzwerknummer allein kann kein Router entscheiden, ob er bei einer IP-Kommunikation eine Verbindung zu einem physikalisch anderen Netz innerhalb des WANs aufbauen soll. Das Netzwerk (WAN) muss daher in kleinere Abschnitte (LANs) unterteilt werden, die einen eigenen Adressblock erhalten. Jeder Adressblock der einzelnen physikalischen Netze wird als Subnet bezeichnet. Durch diese Unterteilung eines Netzwerks in Subnets wird die Hierarchie aus Netzwerk und Rechner zu einer Hierarchie erweitert aus Netzwerk, Subnet und Rechner.

Diese erweiterte Hierarchie erleichtert zum einen das Auffinden eines Rechners im Gesamtnetz (WAN). Man kann sich dies vorstellen analog zur Nomenklatur im Telefonnetz, wo zum Beispiel die Ortsvorwahl aussagt in welchem Bereich sich ein Anschluss befindet. Diese Hierarchie gewährt auch eine gewisse Zugriffssicherheit. So kann in einem Firmennetz zum Beispiel der Rechner eines Subnets nicht ohne weiteres auf Ressourcen eines anderen Subnets zugreifen – etwa ein Mitarbeiter aus der Fertigungsabteilung auf Datenbestände aus der Personalabteilung – wenn die Netz-Masken nach Firmenabteilungen entsprechend gewählt sind.

Die Netz-Maske (Subnet Mask) gibt den Standort des Subnet-Felds in einer IP-Adresse an. Die Netz-Maske ist eine binäre 32-Bit-Zahl wie eine IP-Adresse. Sie hat eine “1” an allen Stellen des Netzwerk-Abschnitts der IP-Adresse (je nach Netzwerk-Klasse innerhalb des ersten bis dritten Oktetts). Das darauf folgende Oktett gibt die Position des Subnet-Feldes an. Die im Subnet-Feld an den Netzwerk-Abschnitt aufschließenden Einsen geben die Subnet-Bits an. Alle übrigen Stellen mit ”0” verbleiben für den Host-Abschnitt.

■ Beispiele

Beispiel 1:

Die Netzmaske dient der Interpretation der IP-Adresse. So kann eine Adresse 135.96.7.230 mit der Maske 255.255.255.0 so interpretiert werden: Das Netzwerk hat die Adresse 135.96.0.0, das Subnet hat die Nummer 7, der Rechner Nummer 230. Eine IP-Adresse mit 135.96.4.190 gehört dem gleichen Netzwerk aber einem anderen Subnet (4) an.

Binäre Darstellung:

```
135.96.7.230     = 10000111 11000000 | 00000111 | 11100110
135.96.4.190     = 10100000 10010101 | 00000100 | 10111110
255.255.255.0    = 11111111 11111111 | 11111111 | 00000000
                   Netzwerk          | Subnet   |
255.255.248.0    = 11111111 11111111 | 11111|000  00000000
```

Hätte die Netz-Maske in obigem Beispiel nicht den Standardwert 255.255.255.0, sondern 255.255.248.0, befänden sich die IP-Adressen im gleichen Subnet – und Routing würde nicht stattfinden.

Beispiel 2:

Zwei IP-Adressen mit 160.149.115.8 und 160.149.117.201 und der Netz-Maske 255.255.252.0 befinden sich im gleichen Netzwerk 160.149, gehören aber unterschiedlichen Subnets an.

Binäre Darstellung:

```
160.149.115.8    = 10100000 10010101 | 011100|11 00001000
160.149.117.201  = 10100000 10010101 | 011101|01 11001001
255.255.252.0    = 11111111 11111111 | 111111|00 00000000
                     Netzwerk        | Subnet|
```

Die Wahl einer geeigneten Netzmaske hängt von der Netzwerk-Klasse, der Beschaffenheit der möglichen Subnets, ihrer Anzahl und ihrem Wachstum ab. Ziehen Sie zur Planung einschlägige Tabellen oder einen Subnet-Taschenrechner zu Rate.

Subnet-Tabelle Klasse C:

Subnet-Bits	Host-Bits	Netz-Maske	Subnets	Rechner
2	6	255.255.255.192	2	62
3	5	255.255.255.224	6	30
4	4	255.255.255.240	14	14
5	3	255.255.255.248	30	6
6	2	255.255.255.252	62	2

(Berechnung: 2 hoch n minus 2 = Anzahl der Subnets/Rechner
n: Anzahl der Subnet/Host-Bits)

Mit einer Netz-Maske 255.255.255.240 wird ein Netz der Klasse C in Subnets geteilt. Mit dieser Netz-Maske sind insgesamt 14 Subnets mit jeweils max. 14 Rechnern möglich.

```
255.255.255.240  11111111 11111111 11111111 | 1111 | 0000
199.  9. 99.130  11000111 00001001 01100011 | 1000 | 0010  Subnet-Nummer 8
199.  9. 99.146  11000111 00001001 01100011 | 1001 | 0010  Subnet-Nummer 9
                 Netzwerk                   |Subnet| Host
```

■ Standard-Masken

Netzmaske für Klasse A: 255. 0. 0. 0

Netzmaske für Klasse B: 255. 255. 0. 0

Netzmaske für Klasse C: 255. 255. 255. 0

Reservierte Adressen

Einige IP-Adressen dürfen Geräten eines Netzwerks nicht zugeordnet werden. Dazu gehören die Netzwerk- oder Subnet-Adresse und die Rundsendungsadresse für Netzwerke bzw. Subnets. Netzwerk-Adressen bestehen aus der Netzwerknummer und dem Host-Feld, das mit binären Nullen gefüllt ist (z.B. 200.1.2.0, 162.66.0.0., 10.0.0.0) – auch Loop Back, es findet keine Übertragung ins Netzwerk statt. Die Rundsendungsadresse eines Netzwerks besteht aus der Netzwerknummer und dem Host-Feld mit binären Einsen (z.B. 200.1.2.255, 162.66.255.255., 10.255.255.255) – daher auch "All One Broadcast", alle Stationen eines Netzwerks werden adressiert.

Beispiel:

198.10.2.255	adressiert alle Stationen im Netz 198.10.2.
255.255.255.255	adressiert alle Stationen in allen angeschlossenen Netzen
0.0.0.0	All Zero Broadcast: Ungültige Adresse.

Bitte beachten Sie, dass diese Adresse oft für Standard-Einstellungen benutzt wird.

7.1.4 Zum Umgang mit IP-Adressen

- ☐ Jede IP-Adresse im unternehmensweiten Netz sollte nur einmalig vorhanden sein. Beachten Sie dies bei Internet-Anschluss und Anschluss neuer Netze.
- ☐ Benutzen Sie ein nachvollziehbar logisches Schema bei der Adress-Vergabe, z.B. Verwaltungseinheiten, Gebäude, Abteilungen etc.
- ☐ Für den Anschluss ans Internet benötigen Sie eine offizielle einmalige Internet-Adresse.
- ☐ Vergeben Sie, wenn möglich, keine IP-Adresse, deren Netzwerk- oder Host-Abschnitt mit "0" endet. Dies könnte zu Fehlinterpretationen und undefinierbaren Fehlern im Netz führen.
- ☐ Netzmasken werden vom Internet-Protokoll nur ausgewertet, wenn die Netzwerknummern der Kommunikationspartner gleich sind.
- ☐ Wie die Adress-Klassen haben auch die Netz-Masken unterschiedlich lange Netzwerk-Abschnitte.

7.2 Security

Im Parameterfeld “IPSec-Einstellungen” der Profil-Einstellungen sind die Konfigurationsparameter zu IPSec für den Einsatz in Remote Access-Umgebungen gesammelt. Im folgenden wird auf einige Konfigurationsmöglichkeiten Bezug genommen.

7.2.1 IPSec – Übersicht

IPSec kann nur für IP-Datenverkehr eingesetzt werden. Die IPSec-Spezifikation umfasst nicht nur das (Layer 3-) Tunneling, sondern auch alle notwendigen Sicherheitsmechanismen, wie starke Authentisierung, Schlüsselaustausch und Verschlüsselung.

Mit den IPSec RFCs (2401 - 2409) lässt sich ein VPN mit vorgegebener Security für IP realisieren. Tunneling und Security sind für IPSec vollständig beschrieben, so dass ein komplettes Rahmenwerk für das VPN zur Verfügung steht. Prinzipiell ist es möglich, herstellerunabhängige veschiedene Komponenten zu nutzen. In Site to Site VPNs etwa könnten die VPN Gateways von veschiedenen Herstellern stammen, in End to Site VPNs könnten die Clients von einem anderen Hersteller als die Gateways sein.

Der Verbindungsaufbau zum IPSec-Verkehr erfolgt auf Basis des Internet Key Exchange-Protokolls (IKE).

■ IPSec – allgemeine Funktionsbeschreibung

In jedem IP-Host (Client oder Gateway) der IPSec unterstüzt, gibt es ein IPSec-Modul, bzw. eine IPSec-Maschine. Dieses Modul untersucht jedes IP-Paket nach bestimmten Eigenschaften, um die jeweils entsprechende Security-Behandlung darauf anzuwenden.

Die Prüfung der vom IP Stack ausgehenden IP-Pakete erfolgt bezüglich einer Secure Policy Database (SPD). Dabei werden alle konfigurierten SPDs abgearbeitet. (Bei Einsatz des IPSec Clients werden die SPDs nur zentralseitig am Gateway gehalten.)

Die SPD besteht aus mehreren Einträgen (SPD Entries), die wiederum einen Filterteil beinhalten. Der Filterteil (siehe → Erweiterte Firewall-Einstellungen) oder Selektor eines SPD-Eintrags besteht hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderer IP Header-spezifischer Einträge. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des SPD-Eintrags übereinstimmen, wird aus den SPD-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist. Das Paket kann einfach durchgelassen werden (permit), es kann abgelehnt bzw. weggeworfen werden (deny) oder bestimmte Security-Richtlinien des IPSec-Prozesses kommen an ihm zur Anwendung. Diese Security-Richtlinien stehen auch im SPD-Eintrag beschrieben.

Wird auf diese Weise festgestellt, dass ein IP-Paket mit einem SPD-Eintrag verknüpft ist, der einen IPSec-Prozess einleitet, so wird überprüft, ob bereits eine Sicherheits-

Verknüpfung (Security Association, SA) für diesen SPD-Eintrag existiert. Existiert noch keine SA, wird vor dem Aushandeln einer SA zunächst eine Authentisierung und ein Schlüsselaustausch (siehe unten → IPSec-Verhandlung Phase 1) vorgenommen.

Nach der SA-Verhandlung erfolgen in einem weiteren Schritt (siehe unten → IPSec-Verhandlung Phase 2) die Verhandlungen für eine Verschlüsselung (ESP) und/oder Authentisierung (AH) der Datenpakete.

Die SA beschreibt, welches Sicherheitsprotokoll verwendet werden soll. ESP (Encapsulating Security Payload) unterstützt die Verschlüsselung und die Authentisierung von IP-Paketen, AH (Authentication Header) unterstüzt nur die Authentisierung von IP-Paketen. Die SA beschreibt auch, in welcher Betriebsart das Sicherheitsprotokoll benutzt werden soll (Tunnel- oder Transportmodus). Im Tunnelmodus wird ein IP Header hinzugefügt, im Transportmodus wird der Original-Header verwendet. Weiter beschreibt die SA, welcher Algorithmus zur Authentisierung verwendet werden soll, welche Verschlüsselungsmethode (bei ESP) und welcher Schlüssel zur Anwendungen kommen sollen. Die Gegenstelle muss selbstverständlich nach der gleichen SA arbeiten.

Ist die SA ausgehandelt, wird jedes Datenpaket gemäß Betriebsmodus (Tunnel oder Transport) und Protokoll (ESP oder AH) bearbeitet. Der IPSec Client nutzt immer das ESP-Protokoll im Tunnelmodus.

7.2.2 Firewall-Einstellungen

Die Firewall-Einstellungen bestehen hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderer IP Header-spezifischer Einträge. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des Regel-Eintrags übereinstimmen, wird aus den Regel-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist.

Im folgenden die Einträge zur Konfiguration im IPSec Client:

☐ Ausführung / Command

gestatten (permit), sperren (deny), inaktiv (disabled)

☐ IP-Protokoll / IP Protocol

Dies ist das Transportprotokoll (ICMP, TCP oder UDP). Eines der angebotenen Protokolle kann ausgewählt werden oder ein beliebiges (alle / any) wird genutzt.

☐ IP-Adresse (Quelle) / Source IP Address

Dies kann eine einfache IP-Adresse oder ein Adressbereich sein. Letzteres ist nötig, wenn mehrere Ausgangssysteme mit einer gemeinsamen SA unterstützt werden sollen (z.B. hinter einer Firewall).

☐ IP-Adresse (Ziel) / Destination IP Address

Dies kann eine einfache IP-Adresse oder ein Adressbereich sein. Letzteres ist nötig, wenn mehrere Zielsysteme mit einer gemeinsamen SA unterstützt werden sollen (z.B. hinter einer Firewall).

☐ Port (Quelle) / Source Port

Dies können einzelne TCP- oder UDP-Portnummern oder ein Bereich von Portnummern sein. Die Portnummern mit zugeordnetem Service bestimmen Sie über den Auswahlbutton [...].

☐ Port (Ziel) / Destination Port

Dies können einzelne TCP- oder UDP-Portnummern oder ein Bereich von Portnummern sein. Die Portnummern mit zugeordnetem Service bestimmen Sie über den Auswahlbutton [...].

7.2.3 SA-Verhandlung und Richtlinien / Policies

Damit der IPSec-(Filter-)Prozess in Gang kommen kann, müssen vorher verschiedene SAs verhandelt worden sein. Es wird eine SA für Phase 1 (IKE-Richtlinie) sowie mindestens zwei (je für ein- und ausgehende Verbindung) für Phase 2 (IPSec-Richtlinie) ausgehandelt. [Für jedes Zielnetz (siehe → Profil-Einstellungen, VPN Networks) werden ebenfalls zwei SAs ausgehandelt.]

- **Phase 1 (Parameter der IKE-Richtlinie / IKE Policy):**

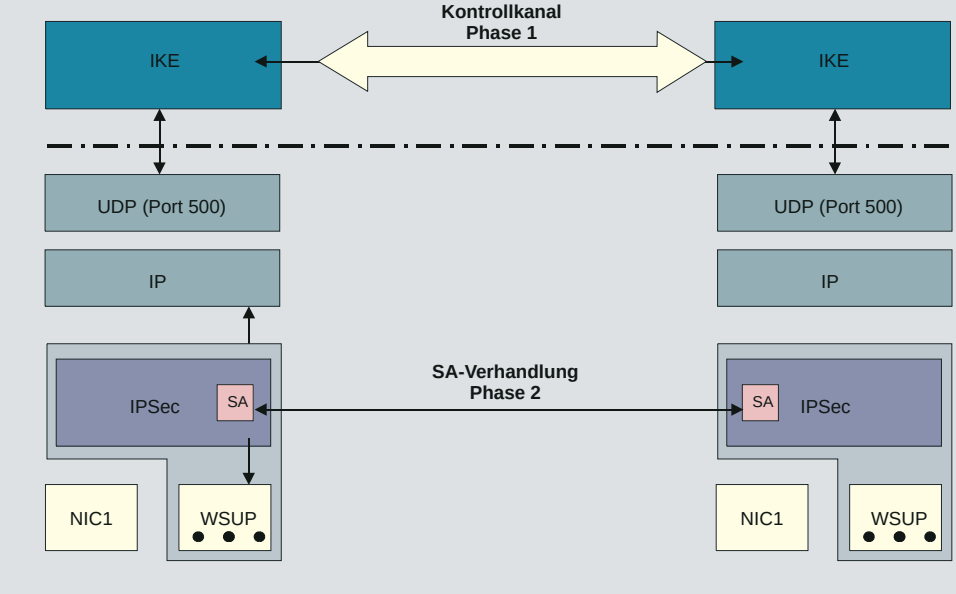
Der Kontrollkanal wird im Tunnelmodus von IPSec über das IKE-Protokoll zur IP-Adresse des Gateways aufgebaut, im Transportmodus direkt zur IP-Adresse der Gegenstelle.

Parameter zur Festlegung von Verschlüsselungs- und Authentisierungsart über das IKE-Protokoll definieren Sie in den IKE-Richtlinien. Dabei kann die Authentisierung über einen Pre-shared Key oder eine RSA Signatur erfolgen. (Entsprechende Richtlinien sind im Richtlinien-Editor vorkonfiguriert.)

- **Phase 2 (Parameter der IPSec-Richtlinie / IPSec Policy):**

Die SA-Verhandlung wird über den Kontrollkanal abgewickelt. Von der IPSec-Maschine wird die SA an das IKE-Protokoll übergeben, das sie über den Kontrollkanal zur IP-Sec-Maschine der Gegenstelle überträgt.

Kontrollkanal und SA-Verhandlung



Bildbeschreibung:

Damit der IPSec-Prozess in Gang kommen kann, muss vorher die SA verhandelt worden sein. Diese SA-Verhandlung findet pro SPD – die für verschiedene Ports, Adressen und Protokolle angelegt sein können – einmal statt. Für diese SA-Verhandlung wird ein Kontrollkanal benötigt.

Im Client muss nun zunächst eine Layer 2-(PPP)-Verbindung zum Provider hergestellt werden. Dabei bekommt er (bei jeder Einwahl) eine neue IP-Adresse. Das IPSec-Modul im Client bekommt ein IP-Paket mit der Zieladresse der Firmenzentrale. Ein SPD-Eintrag für dieses IP-Paket wird gefunden aber es existiert noch keine SA. Das IPSec-Modul stellt die Anforderung an das IKE-Modul, eine SA auszuhandeln. Dabei werden auch die angeforderten Sicherheits-Richtlinien, wie sie im SPD-Eintrag vorhanden sind, an das IKE-Modul übergeben. Eine IPSec-SA auszuhandeln wird als Phase-2-Verhandlung bezeichnet. Bevor jedoch eine IPSec-SA mit der Gegenstelle (Gateway) ausgehandelt werden kann, muss ein Kontrollkanal vom Client zum Gateway existieren. Dieser Kontrollkanal wird über die Phase-1-Verhandlung hergestellt, deren Ergebnis eine IKE-SA ist. Die Phase-1-Verhandlung übernimmt somit die komplette Authentisierung vom Client gegenüber dem VPN Gateway und erzeugt einen verschlüsselten Kontrollkanal. Über diesen Kontrollkanal kann dann rasch die Phase 2 (IPSec SA) durchgeführt werden. Die Phase-1-Verhandlung ist ein Handshake, über den auch der Austausch von Zertifikaten möglich ist und die den Schlüsselaustausch für den Kontrollkanal beinhaltet.

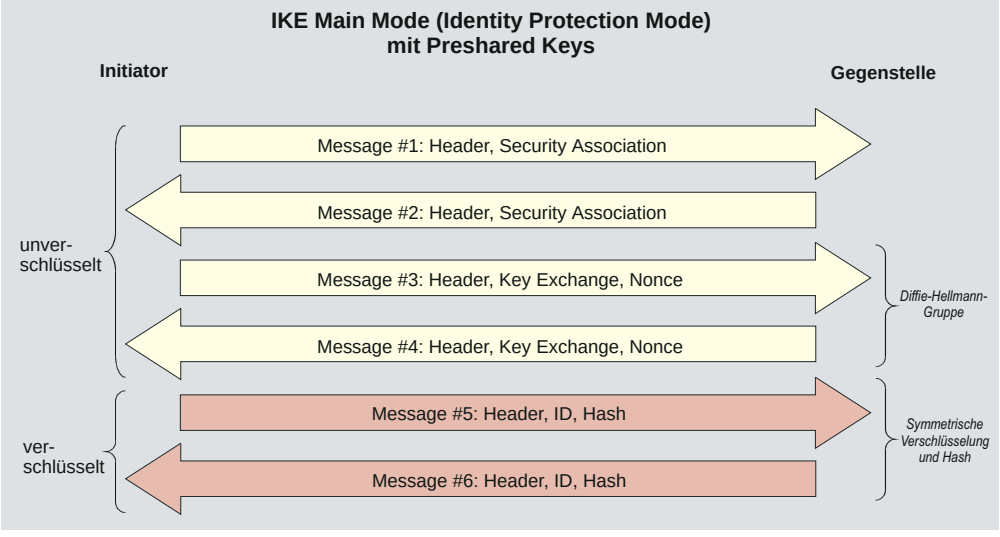
IKE-Modi

Im wesentlichen können zwei Arten der IKE-Richtlinien konfiguriert werden. Sie unterscheiden sich durch die Art der Authentisierung, entweder über Pre-shared Key oder über RSA-Signatur. Beide Arten des Internet Key Exchanges können in zwei unterschiedlichen Modi ausgeführt werden, dem Main Mode, auch Identity Protection Mode, oder dem Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch die Verschlüsselung.

Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch Identity Protection Mode.

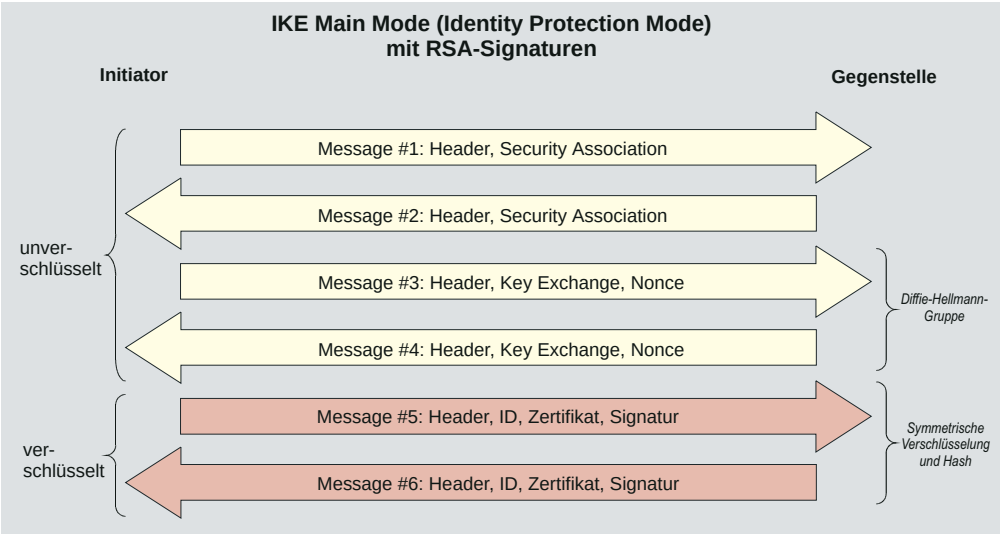
Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.

Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in den Profil-Einstellungen im Parameterfeld “IPSec-Einstellungen”.



Wird die Pre-shared Key-Methode im Main Mode genutzt (Bild oben), so muss der Client am VPN/GW durch seine IP-Adresse eindeutig identifizierbar sein, da der Pre-shared Key mit in die symmetrische Schlüsselberechnung einbezogen und verschlüsselt wird, bevor sonstige Informationen übertragen werden, die den Client identifizieren könnten. Ein Client, der sich beim Provider einwählt, ist jedoch nicht durch die IP-Adresse zu erkennen, da er bei jeder Provider-Anwahl eine neue zugewiesen bekommt. Letztlich kann im Main Mode an alle Clients nur derselbe Pre-shared Key vergeben werden, was allerdings die Authentisierung abschwächt.

Eine Möglichkeit, einen allgmeinen Pre-shared Key zu vermeiden, wäre, den Aggressive Mode zu nutzen (Bild oben), doch wird dabei die ID des Clients nicht verschlüsselt.



Werden RSA-Signaturen eingesetzt (Bild oben und unten), so bedeutet dies, dass Zertfikate zum Einsatz kommen, womit die Vorkonfiguration jedweder "Secrets" überflüssig wird.

7.2.4 IPSec Tunneling

Der IPSec Client kann gegenüber IPSec-Gateways unterschiedlicher anderer Hersteller zum Einsatz kommen.

Die Kompatibilität mit den IPSec-Modi der anderen Hersteller beruht auf der Konformität mit folgenden RFCs und Drafts zu IPSec:

RFC 2104 - Keyed-Hashing for Message Authentication
RFC 2401 - Security Architecture for the Internet Protocol
RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH
RFC 2404 - The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2406 - IP Encapsulating Security Payload (ESP)
RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 - The Internet Key Exchange (IKE)
DRAFT - draft-beaulieu-ike-xauth-05 (XAUTH)
DRAFT - draft-dukes-ike-mode-cfg-02 (IKECFG)
DRAFT - draft-ietf-ipsec-dpd-01 (DPD)
DRAFT - draft-ietf-ipsec-nat-t-ike-01 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-02 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-03 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-05 (NAT-T)
DRAFT - draft-ietf-ipsec-udp-encaps-06 (UDP-ENCAP)

■ **Implementierte Algorithmen für Phase 1 und 2:**

Unterstützte Authentisierung für Phase 1 (IKE-Richtlinie)

– RSA-Signatur

– PSK (Pre-shared Key)

Unterstützte symmetrische Verschlüsselungsalgorithmen (Phase 1 + 2)

– DES

– 3DES

– AES-128, AES-192, AES-256

Unterstützte asymmetrische Verschlüsselungsalgorithmen (Phase 1 + 2)

– DH 1,2,5 (Diffie-Hellmann)

– RSA

Unterstützte Hash-Algorithmen

– MD5

– SHA-1

Zusätzliche Unterstützung für Phase 2

– PFS (Perfect Forward Secrecy)

– IPCOMP (LZS)

– Seamless re-keying

In den Profil-Einstellungen des IPSec Clients werden automatisch einige Standards gesetzt:

– IKE Phase 1 Richtlinie - Automatischer Modus

– IKE Phase 2 Richtlinie - Automatischer Modus

– IKE Phase 1 Modus RSA - Main Mode

– IKE Phase 1 Modus PSK - Aggressive Mode

Diese automatisch gesetzten Richtlinien und Verhandlungsmodi sind in den Profil-Einstellungen konfigurierbar gehalten, sodass sie anderslautenden Verbindungsanforderungen entsprechend modifiziert werden können.

Standard IKE-Vorschläge:

1. Wenn für die IKE-Richtlinie der automatische Modus in den IPSec-Einstellungen gewählt wurde und im Parameterfeld “Identität” die Verwendung eines Pre-shared Keys nicht aktiviert wurde (ohne Haken!), so werden an die Gegenstelle standardmäßig folgende Vorschläge für die IKE-Richtlinie versendet, wobei die Authentisierung immer mit Zertifikat erfolgt:

Notation:

```
EA    = Encryption Algorithm (Verschlüsselung)
HASH  = Hash Algorithm (Hash)
AUTH  = Authentication Method (Authentisierung)
GROUP = Diffie-Hellmann Group Number (DH-Gruppe)
LT    = Life Type (Dauer)
LS    = Life Seconds (Dauer)
KL    = Key Length (Schlüssellänge)
```

EA	HASH	AUTH	GROUP	LT	LS	KL
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	256
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	256
AES_CBC	SHA	RSA	DH5	SECONDS	28800	256
AES_CBC	MD5	RSA	DH5	SECONDS	28800	256
AES_CBC	SHA	XAUTH_RSA	DH2	SECONDS	28800	256
AES_CBC	MD5	XAUTH_RSA	DH2	SECONDS	28800	256
AES_CBC	SHA	RSA	DH2	SECONDS	28800	256
AES_CBC	MD5	RSA	DH2	SECONDS	28800	256
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	192
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	192
AES_CBC	SHA	RSA	DH5	SECONDS	28800	192
AES_CBC	MD5	RSA	DH5	SECONDS	28800	192
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	128
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	128
AES_CBC	SHA	RSA	DH5	SECONDS	28800	128
AES_CBC	MD5	RSA	DH5	SECONDS	28800	128
AES_CBC	SHA	XAUTH_RSA	DH2	SECONDS	28800	128
AES_CBC	MD5	XAUTH_RSA	DH2	SECONDS	28800	128
AES_CBC	SHA	RSA	DH2	SECONDS	28800	128
AES_CBC	MD5	RSA	DH2	SECONDS	28800	128
DES3	SHA	XAUTH_RSA	DH5	SECONDS	28800	0
DES3	MD5	XAUTH_RSA	DH5	SECONDS	28800	0
DES3	SHA	RSA	DH5	SECONDS	28800	0
DES3	MD5	RSA	DH5	SECONDS	28800	0
DES3	SHA	XAUTH_RSA	DH2	SECONDS	28800	0
DES3	MD5	XAUTH_RSA	DH2	SECONDS	28800	0
DES3	SHA	RSA	DH2	SECONDS	28800	0
DES3	MD5	RSA	DH2	SECONDS	28800	0

Wird ein spezifischer IKE-Vorschlag in der IPSec-Konfiguration der Profil-Einstellungen eingestellt, so wird immer auch automatisch der gleiche Vorschlag zusätzlich mit Extended Authentication generiert und versendet.

2. Wird in das Feld für “Pre-shared Key” ein String eingetragen, so werden an die Gegenstelle standardmäßig folgende Vorschläge für die IKE-Richtlinie versendet, wobei die Authentisierung immer ohne Zertifikat erfolgt:

```
EA       HASH AUTH       GROUP LT      LS     KL
AES_CBC SHA  XAUTH_PSK DH5   SECONDS 28800 256
AES_CBC MD5  XAUTH_PSK DH5   SECONDS 28800 256
AES_CBC SHA  PSK       DH5   SECONDS 28800 256
AES_CBC MD5  PSK       DH5   SECONDS 28800 256
AES_CBC SHA  XAUTH_PSK DH2   SECONDS 28800 256
AES_CBC MD5  XAUTH_PSK DH2   SECONDS 28800 256
AES_CBC SHA  PSK       DH2   SECONDS 28800 256
AES_CBC MD5  PSK       DH2   SECONDS 28800 256
AES_CBC SHA  XAUTH_PSK DH5   SECONDS 28800 192
AES_CBC MD5  XAUTH_PSK DH5   SECONDS 28800 192
AES_CBC SHA  PSK       DH5   SECONDS 28800 192
AES_CBC MD5  PSK       DH5   SECONDS 28800 192
AES_CBC SHA  XAUTH_PSK DH5   SECONDS 28800 128
AES_CBC MD5  XAUTH_PSK DH5   SECONDS 28800 128
AES_CBC SHA  PSK       DH5   SECONDS 28800 128
AES_CBC MD5  PSK       DH5   SECONDS 28800 128
AES_CBC SHA  XAUTH_PSK DH2   SECONDS 28800 128
AES_CBC MD5  XAUTH_PSK DH2   SECONDS 28800 128
AES_CBC SHA  PSK       DH2   SECONDS 28800 128
AES_CBC MD5  PSK       DH2   SECONDS 28800 128
DES3    SHA  XAUTH_PSK DH5   SECONDS 28800 0
DES3    MD5  XAUTH_PSK DH5   SECONDS 28800 0
DES3    SHA  PSK       DH5   SECONDS 28800 0
DES3    MD5  PSK       DH5   SECONDS 28800 0
DES3    SHA  XAUTH_PSK DH2   SECONDS 28800 0
DES3    MD5  XAUTH_PSK DH2   SECONDS 28800 0
DES3    SHA  PSK       DH2   SECONDS 28800 0
DES3    MD5  PSK       DH2   SECONDS 28800 0
```

Als Vorschläge für die IPSec-Richtlinie (Phase 2) wird standardmäßig versendet:
Notation:

```
PROTO  - Protocol (Protokoll)
TRANS  - Transform (Transformation (ESP))
LT     - Life Type (Dauer)
LS     - Life Seconds (Dauer)
KL     - Key Length (Schlüssellänge)
COMP   - IP Compression (Transformation (Comp))
```

```
PROTO TRANS AUTH LT      LS    KL  COMP LZS
ESP   AES   MD5  SECONDS 28800 128 Yes  Yes
ESP   AES   SHA  SECONDS 28800 128 Yes  Yes
ESP   AES   MD5  SECONDS 28800 128 No   No
ESP   AES   SHA  SECONDS 28800 128 No   No
ESP   AES   MD5  SECONDS 28800 192 Yes  Yes
ESP   AES   SHA  SECONDS 28800 192 Yes  Yes
ESP   AES   MD5  SECONDS 28800 192 No   No
ESP   AES   SHA  SECONDS 28800 192 No   No
ESP   AES   MD5  SECONDS 28800 256 Yes  Yes
ESP   AES   SHA  SECONDS 28800 256 Yes  Yes
ESP   AES   MD5  SECONDS 28800 256 No   No
ESP   AES   SHA  SECONDS 28800 256 No   No
ESP   DES3  MD5  SECONDS 28800 0   Yes  Yes
ESP   DES3  MD5  SECONDS 28800 0   No   No
```

7.2.5 Zur weiteren Konfiguration

Pre-shared Key oder *RSA-Signatur*: Entsprechend den Vorgaben durch die Gegenstelle kann als “IKE-Richtlinie” die automatisch vorgenommene Einstellung “Automatischer Modus” auf “Pre-shared Key” oder “RSA Signatur” (Zertifikat) abgeändert werden. Erwartet die Gegenstelle “Pre-shared Key”, so muss der Schlüssel in das Feld eingetragen werden. (Der Pre-shared Key muss in diesem Fall für alle Clients identisch sein.)

IP-Adressen und *DNS Server* können über das Protokoll IKE-Config Mode (Draft 2) zugewiesen werden. Für die NAS-Einwahl können alle üblichen WAN-Schnittstellen verwendet werden.

Die *Authentisierung* bei IPSec Tunneling kann über das XAUTH Protokoll (Draft 6) erfolgen. Dazu müssen außerdem noch folgende Parameter im Konfigurationsfeld “Identität” gesetzt werden:

Benutzername	=	Kennwort des IPSec-Benutzers
Passwort	=	Passwort des IPSec-Benutzers
Zugangsdaten aus ...		
verwenden	=	optional

Bei IPSec Tunneling wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der IPSec Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau. Unterstützt die Gegenstelle DPD nicht, so kann DPD im Parameterfeld “IPSec-Einstellungen” deaktiviert werden. Der Einsatz von NAT Traversal erfolgt beim IPSec Client automatisch und ist immer nötig, wenn auf dem weg zum Zielsystem ein Gerät mit Network Address Translation zum Einsatz kommt.

■ Basiskonfigurationen in Abhängigkeit vom IPSec Gateway

Im folgenden sind Konfigurationsmöglichkeiten aufgeführt, die zu beachten sind, je nachdem ob das IPSec Gateway Extended Authentication (XAUTH) und IKE-Config Mode unterstützt oder nicht.

Gateway unterstützt nicht XAUTH

Der IPSec Client als Initiator der IPSec-Verbindung schlägt standardmäßig immer die Extended Authentication vor. Diese Eigenschaft kann nicht konfiguriert werden. Unterstützt das Gateway die Extended Authentication nicht, so wird sie auch nicht durchgeführt.

Gateway unterstützt IKE-Config Mode

Sofern das Gateway den IKE-Config Mode unterstützt, kann im Parameterfeld “IP-Adressen-Zuweisung” die Funktion “IKE Config Mode verwenden" aktiviert werden.

Gateway unterstützt IKE-Config Mode nicht

Unterstützt das Gateway den IKE-Config Mode nicht, so sind zwei Konfigurationen möglich.

1. Wird die Funktion “IP-Adresse manuell vergeben” (siehe → Profil-Einstellungen, IP-Adressen-Zuweisung) aktiviert, so muss die IP-Adresse eingetragen werden, die vom Gateway bzw. Administrator für diesen Client bzw. Benutzer vorgegeben wurde.

2. Wird “Lokale IP-Adresse verwenden” (siehe → Profil-Einstellungen, IP-Adressen-Zuweisung) aktiviert, so wird die IP-Adresse gleich der öffentlichen IP-Adresse gesetzt, die der Client pro Internet Session vom Provider erhält oder, unter der Verbindungsart “LAN”, die Adresse, die der LAN-Adapter besitzt.

   Wird die lokale IP-Adresse verwendet und der “Typ” im Parameterfeld “Identität” steht auf “IP-Adresse”, dann darf im Feld für die “ID” keine IP-Adresse eingetragen sein. Nur dann ist gewährleistet, dass die jeweils aktuelle öffentliche IP-Adresse automatisch zur Identifikation für Phase 1 an das Gateway übertragen wird.

7.2.6 IPSec Ports für Verbindungsaufbau und Datenverkehr

Bitte beachten Sie, dass der IPSec Client exklusiven Zugriff auf den UDP Port 500 benötigt. Sofern NAT Traversal eingesetzt wird, wird auch Zugriff auf Port 4500 benötigt. Ohne NAT Traversal wird das IP-Protokoll ESP (Protokoll-ID 50) benutzt.

Standardmäßig wird der Port 500, der für den Verbindungsaufbau genutzt wird, unter Windows-Systemen von den IPSec-Richtlinien genutzt. Um dies zu ändern gehen Sie wie folgt vor:

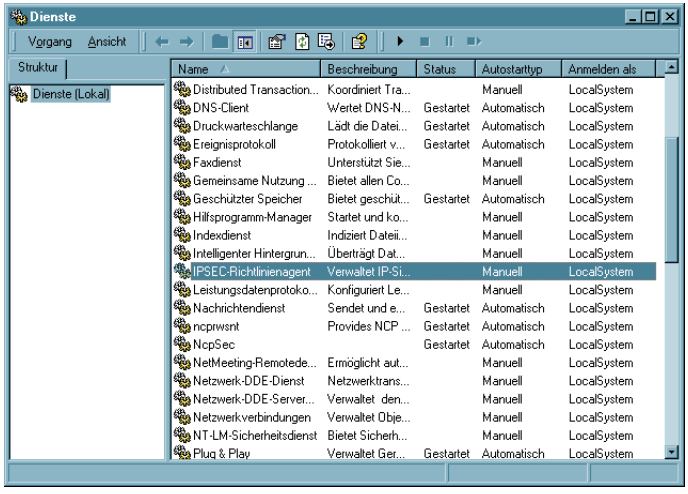
1. Um sich zu vergewissern, welche Ports aktuell von Ihrem System genutzt werden, können Sie unter der MS-DOS-Eingabeaufforderung mit dem Kommando
   `netstat -n -a`
   den aktuellen Netzstatus anzeigen lassen. In der Abbildung rechts erkennen Sie, dass der UDP Port 500 genutzt wird.

```
F:\>netstat -n -a

Aktive Verbindungen

  Proto  Lokale Adresse          Remoteadresse          Status
  TCP    0.0.0.0:135            0.0.0.0:0              ABHÖREN
  TCP    0.0.0.0:445            0.0.0.0:0              ABHÖREN
  TCP    0.0.0.0:1025           0.0.0.0:0              ABHÖREN
  TCP    0.0.0.0:1032           0.0.0.0:0              ABHÖREN
  TCP    0.0.0.0:5000           0.0.0.0:0              ABHÖREN
  TCP    172.16.113.140:139     0.0.0.0:0              ABHÖREN
  TCP    172.16.113.140:1032    62.153.165.34:21       HERGESTELLT
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:162            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1027           *:*
  UDP    0.0.0.0:1028           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    172.16.113.140:123     *:*
  UDP    172.16.113.140:137     *:*
  UDP    172.16.113.140:138     *:*
  UDP    172.16.113.140:1900    *:*
```

2. Wird der Port genutzt, so muss im Windows-Startmenü das Fenster “Sytem → Dienste-Verwaltung” geöffnet werden. Dort wird der “IPSEC-Richtlinienagent” markiert, der Dienst gestoppt und der “Autostarttyp” auf “Manuell” gestellt (Bild rechts).



3. Wurde die Änderung des Autostarttyps durchgeführt, so kann das Kommando
   `netstat -n -a`
   erneut ausgeführt werden. Der UDP Port 500 darf dann unter den aktiven Verbindungen nicht mehr aufgeführt sein.

7.3 Zertifikats-Überprüfungen

Neben der Zertifikats-Überprüfung nach Inhalten erfolgt am IPSec Client eine weitere Zertifikatsprüfung in mehrfacher Hinsicht.

7.3.1. Auswahl der CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies geschieht dadurch, dass er die CA-Zertifikate seiner Wahl in das Windows-Verzeichnis \ncple\cacerts\ gespielt. Das Einspielen kann bei einer Software-Distribution mit Disketten automatisiert stattfinden, wenn sich die Aussteller-Zertifikate bei der Installation der Software im Root-Verzeichnis der ersten Diskette befinden (siehe → CA-Zertifikate anzeigen).

Derzeit werden die Formate *.pem und *.crt für Aussteller-Zertifikate unterstützt. Sie können im Monitor unter dem Hauptmenüpunkt “Verbindung – Zertifikate – CA-Zertifikate anzeigen” eingesehen werden.

Wird am IPSec Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der NCP Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Verzeichnis NCPLE\CACERTS\. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande. Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

7.3.2. Überprüfung der Zertifikats-Erweiterung

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zerifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben. Für den IPSec Client und das Gateway sind drei Erweiterungen von Bedeutung:

- ☐ extendedKeyUsage
- ☐ subjectKeyIdentifier
- ☐ authorityKeyIdentifier

- **extendedKeyUsage**

  Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der IPSec Client, ob der definierte erweiterte Verwendungszweck “SSL-Server-Authentisierung” enthalten ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

  Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck “SSL-Server-Authentisierung” beinhalten muss. Dies gilt auch bei einem Rückruf an den Client über VPN.

  Ausnahme: Bei einem Rückruf des Servers an den Client nach einer Direkteinwahl ohne VPN aber mit PKI prüft der Server das Zertifikat des Clients auf die Erweiterung extendedKeyUsage. Ist diese vorhanden, muss der Verwendungszweck “SSL-Server-Authentisierung” beinhaltet sein, sonst wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

- **subjectKeyIdentifier / authorityKeyIdentifier**

  Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann keine Übereinstimmung erkannt werden, wird die Verbindung abgelehnt.

  Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades.

  (Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.)

7.3.3. Überprüfung von Sperrlisten

Zu jedem Aussteller-Zertifikat kann dem IPSec Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Windows-Verzeichnis \ncple\crls\ gespielt. Ist eine CRL vorhanden, so überprüft der IPSec Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Gleiches gilt für eine ARL (Authority Revocation List), die in das Windows-Verzeichnis \ncple\arls\ gespielt werden muss.

7.4 Stateful Inspection-Technologie für die Firewall-Einstellungen

Die Firewall-Technologie der Stateful Inspection kann für alle Netzwerkadapter wie auch für RAS-Verbindungen eingesetzt werden. Sie wird am Client im Telefonbuch unter “Firewall-Einstellungen” aktiviert (siehe → Konfigurations-Parameter, Firewall-Einstellungen). Am Gateway ist sie dann aktiv, wenn im Server Manager unter “Routing Interfaces – Allgemein” die Funktion “LAN-Adapter schützen” eingeschaltet wird.

Grundsätzliche Aufgabe einer Firewall ist es, zu verhindern, dass sich Gefahren aus anderen bzw. externen Netzen (Internet) in das eigene Netzwerk ausbreiten. Deshalb wird eine Firewall auch am Übergang zwischen Firmennetz und z.B. Internet installiert. Sie prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis vorher festgelegter Konfigurationen, ab ein Datenpaket durchgelassen wird oder nicht.

Stateful Inspection ist die Firewall-Technologie, die den derzeit höchstmöglichen Sicherheitsstandard für Internet-Verbindungen und somit das Firmennetz bietet. Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen verhindert diese Funktionalität den unbefugten Zugriff auf Daten und Ressourcen im zentralen Datennetz. Zum anderen überwacht sie als Kontrollinstanz den jeweiligen Status aller bestehenden Internet-Verbindungen. Die Stateful Inspection Firewall erkennt darüber hinaus, ob eine Verbindung “Tochterverbindungen” geöffnet hat – wie beispielsweise bei FTP oder Netmeeting – deren Pakete ebenfalls weitergeleitet werden müssen. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf. Alternative Bezeichnungen für Stateful Inspection sind: Stateful Packet Filter, Dynamic Packet Filter, Smart Filtering, Adaptive Screening.

Stateful Inspection vereinigt konzeptionell die Schutzmöglichkeiten von Packet Filter und Application Level Gateways d.h. sie integriert als Hybrid die Funktionen beider Security-Verfahren und arbeitet sowohl auf der Netz- als auch Anwenderschicht. Bei der “zustandsabhängigen Paket-Filterung” werden nicht nur die Internet- und Transportschicht sondern auch Abhängigkeiten vom Zustand einer Verbindung berücksichtigt. Alle aktuellen und initiierten Verbindungen werden mit Adresse und zugeordnetem Port in einer dynamischen Verbindungstabelle hinterlegt. Der Stateful Inspection-Filter entscheidet anhand festgelegter Raster (Informationen), welche Pakete zu welcher Verbindung gehören. Zustände können sein: Verbindungsaufbau, Übertragung, Verbindungsabbau und gelten sowohl für TCP- als auch UDP-Verbindungen. Ein Beispiel an einer Telnet-Sitzung: Der Zustand “Verbindungsaufbau” wird dadurch definiert, dass noch keine Benutzer-Authentisierung stattgefunden hat. Hat der Benutzer sich mit Benutzername und Kennwort angemeldet, wird diese Verbindung in den Zustand “normale Verbindung” gesetzt. Da der jeweilige Status einer Verbindung ständig überwacht wird, bleibt Unbefugten der Zugriff auf das interne Unternehmensnetz verwehrt.

Der Vorteil gegenüber statischen Paketfiltern ist, dass die Entscheidung, ob ein NCP Secure Gateway oder Client ein Paket weiterleitet oder nicht, nicht nur auf Grund von Quell- und Zieladresse oder Ports fällt. Das Security-Management prüft darüber hinaus

den Zustand (state) der Verbindung zu einem Partner. Weitergeleitet werden ausschließlich die Pakete, die zu einer aktiven Verbindung gehören. Datenpakete, die sich keiner etablierten Verbindung zuordnen lassen, werden verworfen und im Log-File protokolliert. Neue Verbindungen lassen sich nur entsprechend der konfigurierten Regeln öffnen.

In der einfachsten Firewall-Funktion werden nur die ein- und ausgehenden Verbindungen im Hinblick auf das Protokoll (TCP/IP, UDP/IP, ICMP, IPX/SPX), die entsprechenden Ports und die beteiligten Rechner überprüft und überwacht. Verbindungen werden in Abhängigkeit eines festgelegten Regelwerkes erlaubt oder gesperrt. Weitere Prüfungen (z.B. Inhalt der übertragenen Daten) finden nicht statt.

Die Stateful Inspection Filter sind eine Weiterentwicklung der dynamischen Packet-Filter und bieten eine komplexere Logik. Die Firewall prüft, ob eine am Portfilter erlaubte Verbindung auch zu dem definierten Zweck aufgebaut wird.

Es werden folgende zusätzliche Informationen zu einer Verbindung verwaltet:

– Nr. zur Identifizierung einer Verbindung
– Zustand der Verbindung (z.B. Aufbau, Datenübertragung, Abbau)
– Quell-Adresse des ersten Pakets
– Ziel-Adresse des ersten Pakets
– Interface, durch welches das erste Paket kam
– Interface, durch welches das erste Paket verschickt wurde

Anhand dieser Informationen kann der Filter entscheiden, welche nachfolgenden Pakete zu welcher Verbindung gehören. So kann ein Stateful Inspection-System auch das UDP-Problem ausschalten. Hintergrund ist die verhältnismäßig leichte Fälschbarkeit von UDP-Paketen z.B. beim UDP-basierten Dienst DNS. Da Stateful Inspection-Filter in der Lage sind, sich die aktuelle Status- und Kontextinformation einer Kommunikationsbeziehung zu merken, ist es erforderlich, dass neben der Quell- und Zieladresse sowie Quell- und Zielport, auch der DNS-Header im Anfrage-Paket in die Speicherung der Status- und Kontextinformation einbezogen wird. Es erfolgt eine Interpretation auf der Anwendungsschicht.

Beispiel: Eine gehenden Verbindung zum Port 21 eines Rechners ist für einen reinen Portfilter eine FTP-Verbindung. Eine weitere Überprüfung findet nicht statt. Der Stateful Inspection-Filter prüft zusätzlich, ob die über diese Verbindung übertragenen Daten zu einer etablierten FTP-Verbindung gehören. Wenn nicht, wird die Verbindung sofort unterbrochen. Weiter ist ein Stateful Inspection-Filter in der Lage, Regeln in Abhängigkeit von notwendigen Kommunikationsprozessen anzupassen. Wenn z.B. eine abgehende FTP-Verbindung erlaubt ist, so ermöglicht die Firewall auch automatisch die Etablierung des zugehörigen Rückkanals. Die entsprechenden Informationen (Ports) werden aus der Kontrollverbindung herausgelesen.

Ein vorteilhafter Aspekt von Stateful Inspection-Filtern ist die Fähigkeit, die Daten auf allen Protokollebenen (d.h. von Netzwerk- bis Anwendungsebene) zu prüfen. So kann z.B. ein FTP-GET erlaubt, ein FTP-PUT jedoch verboten werden. Ein positiver Effekt der im Vergleich zu konventionellen Paketfiltern erhöhten Eigenintelligenz ist die Op-

tion, einzelne Pakete während einer Kommunikationsbeziehung zu assemblieren und damit erweiterte Möglichkeiten zur Benutzer-Authentisierung zur Anwendung zu bringen. Als Folge der nicht verlässlichen Trennung der Netzwerksegmente sind Stateful Inspection-Filter nicht immun gegen bestimmte auf unteren Protokollebenen stattfindende Angriffe. So z.B. werden fragmentierte Pakete i.d.R. von außen nach innen ohne weitere Prüfung durchgelassen.

Diese Seite ist frei →

Abkürzungen und Begriffe

3DES	TripleDES. Verschlüsselungsstandard mit 112 Bit.
AES	Advanced Encryption Standard. Europäische Entwicklung der belgischen Verschlüsselungsexperten Joan Daemen und Vincent Rijmen (“Rijndael-Algorithmus”). Nachfolger von DES (Data Encryption Standard). Verschlüsselungsalgorithmus, der bis zu 256 Bit Schlüssellänge besitzt. n hoch 256 gilt als Maßeinheit für die mögliche Anzahl der Schlüssel, die mit diesem Algorithmus generiert werden können. Trotz steigender Prozessorgeschwindigkeiten wird erwartet, dass der AES-Algorithmus eine akzeptable Sicherheit für die nächsten 30 Jahre bietet. Wird in VPN- und SSL-Verschlüsselungen bald große Verbreitung finden.
AH	Authentication Header RFC 2402
Asymmetrische Verschlüsselung	(Public-Key-Verfahren) Bei einer asymmetrischen Verschlüsselung besitzt jeder Teilnehmer zwei Schlüssel: einen geheimen, privaten und einen öffentlichen Schlüssel. Beide Schlüssel stehen in einer mathematisch definierten Beziehung zueinander. Der private Schlüssel des Teilnehmer ist streng geheim, der öffentliche Schlüssel für jedermann zugänglich. Das Schlüsselmanagement gestaltet sich auch bei großen Teilnehmerzahlen überschaubar: Zwei Schlüssel pro Teilnehmer – ergibt insgesamt 2.000 Schlüssel, um 1.000 Teilnehmern in allen Sender-Empfänger-Kombinationen die sichere Kommunikation zu ermöglichen. Das bekannteste asymmetrische Verschlüsselungsverfahren ist RSA. Nachteil der asymmetrischen Verfahren: Sie sind rechenintensiv und damit vergleichsweise langsam.

Basisanschluss (So / BRI = Basic Rate Interface)
ISDN-Anschlusstyp mit So-Schnittstelle (“S” für Subscriber Interface: Benutzerschnittstelle), bestehend aus einem D-Kanal (Bandbreite: 16 kBit/s) für die Steuerung und zwei B-Kanälen (Bandbreite jeweils 64 kBit/s) für die Übertragung von Nutzinformationen.

BCP
Bridge Control Protocol

BITS
Bump In The Stack. Art der Implementierung von IPsec.

BITW
Bump In The Wire. Art der Implementierung von IPsec.

Blowfish
Verschlüsselungsstandard mit 128/448 Bit

BRI
Basic Rate Interface (ISDN-Schnittstelle, Basis So) mit 2 B-Kanälen und 1 D-Kanal.

Browser
Der Browser stellt die Anwender-Schnittstelle zum Internet dar. Mit seiner HTTP-Fähigkeit (Hypertext-Transfer-Protokoll) kann er verschiedene Formate (z.B. HTML, GIF, CAD), die für eine multimediale Darstellung der Information benötigt werden, in Sound und Grafik umsetzen.

CA
Certification Authority, auch Trust Center (z.B. D-Trust, ein Gemeinschaftsunternehmen der Bundesdruckerei und Debis). Eine CA stellt mittels PKI-Manager (Software) digital signierte Bestätigungen (Zertifikate) aus und brennt sie auf eine Smartcard (Chipkarte). Eine CA kann ein privater Dienstleister oder eine öffentiche Einrichtung sein. Diese Zertifizierungsstellen bedürfen nicht der Genehmigung durch den Staat. Sie haften für die Richtigkeit der Zertifikate.

CAPI
Common Application Programm Interface. Diese Schnittstelle wird im ISDN als Common ISDN API bezeichnet und entspricht der PCI-Schnittstelle (Programmable Communication Interface). Die Schnittstelle erlaubt den direkten Zugang zum ISDN und den unteren Protokoll-schichten (Ebene 1-3). Höhere Protokolle (Anwendungen) wie Telex oder Filetransfer können unabhängig von der eingesetzten Hardware-Plattform verwendet werden. Die CAPI gibt es in zwei Versionen, 1.1 und 2.0.

	Entsprechend sind auch dieISDN-Anwendungsprogramme programmiert, die entweder auf CAPI 1.1 oder CAPI 2.0 aufsetzen, bzw. die jeweilige CAPI voraussetzen. Eine Hybrid-CAPI gestattet sowohl den Einsatz einer Anwendungs-Software für CAPI 1.1 als auch den von CAPI 2.0-Software. (Siehe Hybrid-CAPI)
CCP	Compression Control Protocol
CHAP	Challenge Handshake Authentication Protocol
CLI	Calling Line Identification (Rufnummern-Identifizierung im Euro-ISDN)
COSO	Charge One Side Only. COSO-Rückruf, auch Low Level- oder D-Kanal Rückruf. Für den Initiator des Rückrufs im D-Kanal fallen keine Gebühren an.
CTAPI	Schnittstelle zu Smartcard Readern
CUG	Closed User Group (geschlossene Benutzergruppe im Euro-ISDN)
DES	Datenverschlüsselungsnorm, Data Encryption Standard
DHCP	Mit DHCP (Dynamic Host Control Protocol) zu kommunizieren, bedeutet, dass für jede Session automatisch eine IP-Adresse zugewiesen wird.
Directory Service	Remote Access-Zugänge werden wie E-Mail-Adressen, Telefonnummern etc. in Verzeichnissen auf unterschiedlichen Datenbanken abgelegt. Das Problem bei dieser Vielzahl von Verzeichnissen ist, dass einerseits viele Daten mehrfach erfasst werden und zudem die einzelnen Einträge nicht untereinander verknüpft sind. Der Pflegeaufwand ist enorm und Inkonsistenzen sind nicht auszuschließen. Gefordert ist ein standardisiertes Prozedere, mit Hilfe dessen die Erfassung und Pflege aller Informationen in einer zentralen Directory ermöglicht wird. Das T-Online Security Management unterstützt die standardisierten Protokolle Radius (Remote Authorization Dial In User Service) und LDAP (Lightweight Directory Access Protocol), wobei letztere den Zugriff auf zentralisierte Verzeichnisdienste gewährleistet.

DMZ	Demilitarisierte Zone, zwischen Firewall und Unternehmensnetz, zum Beispiel mit Web-, Email- und VPN-Server.
DNS	Der Domain Name Server (DNS) stellt die IP-Adresse für eine Internet-Sitzung zur Verfügung, nachdem die Anwahl mit Benutzername und Passwort erfolgte. Er routet weiter im Internet, indem er die Namen, die im Browser als gewünschtes Ziel angegeben werden, in IP-Adressen rückübersetzt und die Verbindung zu dieser Adresse herstellt.
D-Kanal-Protokoll	Das D-Kanal-Protokoll sorgt dafür, dass sich Endgeräte mit dem Netz verständigen können. Es steuert unter anderem Verbindungsauf- und abbau. Es umfasst Schicht 2 und 3. Auf Schicht 2 von ISDN ist HDLC für die logische Datenübertragungssteuerung eingesetzt. Das eigentliche D-Kanal-Protokoll ist auf Schicht 3 angesiedelt. Mittlerweile ist DSS1 als europaweites D-Kanal-Protokoll verfügbar.
DSA	Directory System Agent
DSS1	European Digital Subscriber System No. 1. Europäisches ISDN-Protokoll für den D-Kanal.
DUA	Directory User Agent
ECP	Encryption Control Protocol
ESP	Encapsulating Security Payload RFC 2406
Euro-ISDN	ITU-Standard für Europäisches ISDN; bezieht sich auf das D-Kanal-Protokoll DSS1 und mögliche Dienstmerkmale, wie Gebührenanzeige (Advice of Charge), Rückruf bei Besetzt (Completion of Calls to Busy Subscriber), Rufumleitung (Call Forwarding), Anklopfen (Call Waiting), etc. Im Euro-ISDN mit dem D-Kanal-Protokoll DSS1 werden einzelne Endgeräte mit der Multible Subscriber Number (MSN) adressiert.
Firewall	Trennt Public-Netz von Private-Netz. Schutzmechanismus in Netzen, der den Zugriff der Stationen regelt. Ein Firewall-Rechner schottet ein Netzwerk

	vor allem WAN-seitig gegen unautorisierten Zugriff ab. Die Berechtigung kommender und abgehender Verbindungen wird zum Beispiel geregelt durch Herausfiltern bestimmter Netzteilnehmer und Netzdienste und Festlegung der Zugriffsberechtigungen. Vom WAN aus betrachtet stehen hinter der Firewall (in der DMZ) für gewöhnlich Web-Server, Email-Server und VPN-Server.
FTP	File Transfer Protocol. Basiert auf TCP und dem Terminalprotokoll TELNET (Port 21).
GPRS	Standard für schnelle Handy-Kommunikation
GRE	Generic Router Encapsulation. CISO-Spezifisches Tunnel-Protokoll.
GSM	Global System Mobile. Standard für Handy-Kommunikation
Hash-Wert	siehe Signatur
HBCI	Standard für Smartcard Reader (Online Banking)
HTTP	Hypertext Transfer Protocol. Multimedia-Network im Internet (Port 80)
Hybride Verschlüsselung	Hohe Performance plus viel Sicherheit: Hybride Verschlüsselung vereint die Vorteile symmetrischer und asymmetrischer Verfahren. Während die Inhalte der Kommunikation mit schnellen symmetrischen Algorithmen gesichert werden, erfolgen Authentisierung der Teilnehmer und Schlüsselaustausch auf Basis asymmetrischer Verfahren. Die eigentliche Verschlüsselung der Daten eines Dokuments geschieht auf Basis einer Zufallszahl (Session-Key), die für jede einzelne Kommunikationsverbindung neu erzeugt wird. Dieser Einmalschlüssel wird mit dem öffentlichen Schlüssel des Empfängers chiffriert und der Nachricht beigefügt. Der Empfänger wiederum rekonstruiert mit seinem privaten Schlüssel den Session-Key und entschlüsselt die Nachricht.
IETF	Internet Engineering Task Force. Interessengemeinschaft, die sich mit Problemen des TCP/IP und dem Internet befasst, unter anderem den Well Known Ports (Ports 0 bis 1023).

IKE

Internet Key Exchange. Bestandteil von IPsec für sicheres Schlüssel-Management. Separate security association negotiation and key management protocol RFC 2409

Internet

Das Internet ist ein weltweites, offenes Rechnernetz. Es ist allgemein zugänglich. Jeder Betrieb und jede Privatperson kann sich daran anschließen und mit allen anderen angeschlossenen Benutzern kommunizieren, unabhängig von der eingesetzten Rechnerplattform oder der jeweiligen Netztopologie. Damit der Datenaustausch zwischen den unterschiedlichen Rechnern und Netzen innerhalb des Internets möglich wird, ist ein allen gemeinsames Netzwerkprotokoll nötig. (siehe TCP/IP)

IP-Adresse

Jeder Rechner im Internet besitzt für die Dauer seiner Zugehörigkeit zum Internet eine IP-Adresse (Internet-Protokoll-Adresse), die ihn eindeutig identifiziert. Eine IP-Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennte Zahlen. Für jede Zahl stehen 8 Bits zur Verfügung, womit sie 256 Werte annehmen kann. Die Anzahl der möglichen IP-Adressen insgesamt bleibt jedoch begrenzt. Der Internet-User bekommt daher nicht einmalig eine unveränderliche IP-Adresse zugeteilt, sondern für jede seiner Sessions die IP-Adresse, die gerade noch nicht vergeben ist. Die IP-Adressen werden also für die Dauer eines Zeitschlitzes zugeteilt. Diese Adress-Zuteilung erfolgt im Regelfall automatisch per PPP-Verhandlung über DHCP. Die IP-Adresse kann von speziellen Programmen in einen Namen übersetzt werden. Diese Programme laufen auf einem Domain Name Server (DNS).

IP Network Address Translation

(IP Network Address Translation wird bei der Installation der Workstation Software bereits vorgesehen und ist standardmäßig beim Anlegen eines neues Zielsystems aktiviert!) Wenn IP Network Address Translation verwendet wird, werden alle übertragenen Frames mit der ausgehandelten (PPP) IP-Adresse verschickt. Die Workstation Software übersetzt diese öffentliche IP-Adresse in die systemeigene des Intranets oder, im Falle der Workstation, in deren eigene vom Benutzer festgelegte. Allgemein: Über NAT ist es möglich, in einem LAN mit inoffiziellen IP-Adressen, die nicht im

	Internet gültig sind, zu arbeiten und trotzdem vom LAN aus auf das Internet zuzugreifen. Dazu werden die inoffiziellen IP-Adressen von der Software in offizielle IP-Adressen übersetzt. Dies spart zum einen ofizielle IP-Adressen, die nicht in unbegrenzter Anzahl zur Verfügung stehen. Zum anderen wird damit ein gewisser Schutz (Firewall) für das LAN aufgebaut.
IPCP	Internet Protocol Control Protocol
IPsec	Standards festgelegt von IETF: RFCs 2401-2412 (12/98)
IPX	Internet Packet Exchange, Netware-Protokoll von Novell
IPXCP	Internetwork Packet Exchange Control Protocol
ISDN	Integrated Services Digital Network. Dienste-integrierendes digitales Fernmeldenetz. Digitales Netz mit Integration aller Schmalband-Kommunikationsdienste (z.B. Fernsprechen, Telex, Telefax, Teletext, Bildschirmtext), bestehend aus Kanälen mit einer Übertragungsgeschwindigkeit von 64.000 bit/s. Ein Basisanschluss im sogenannten Schmalband-ISDN besitzt drei Übertragungskanäle:Kanal B1: 64.000 bit/sKanal B2: 64.000 bit/sKanal D: 16.000 bit/sDie Gesamtübertragungsrate beträgt 144.000 bit/s. Dieses Netz soll bis zum Ende dieses Jahrtausends europaweit einheitlich aufgebaut werden. Die Spezifikationen hierfür werden von ITU und CEPT erarbeitet.
ISDN-Adapter	ISDN-Adapter ermöglichen den Anschluss von vorhandenen, nicht ISDN-fähigen Endgeräten an das ISDN. Der Adapter übernimmt dabei die sowohl soft- als auch hardwaremäßige Anpassung der Endgeräteschnittstelle an die ISDN-Schnittstelle (So). Ein ISDN-Adapter mit Upo-Schnittstelle ermöglicht an ISDN TK-Anlagen die Umsetzung der ISDN-Zweidraht-Schnittstelle Upo (Reichweite ca. 3,5km) auf die busfähige ISDN-Vierdraht-Schnittstelle So (Reichweite ca. 150m) nach den Richtlinien der Telekom.
ISP	Internet Service Provider

Kryptographie	Anwendungen sind Verschlüsselung, elektronische Signatur, Authentifikation und Hash-Wert-Berechnung. Mathematische Verfahren, die mit Schlüssel verwendet werden.
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol, siehe Directory Service
MAC-Adresse	Medium Access Control Layer-Adresse. Physikalische Adresse im Netzwerk.
MIB	Management Information Base. Beschreibt die Struktur der Managementinformationen beim SNMP.
MD5	Message Digit 5. Verfahren zur Bildung eines Hash-Werts
NAS	Network Access System
NetBios	Network Basic Input Output System. Schnittstelle, die Datagramm- und streamorientierte Kommunikation bietet.
OCSP	Online Certificate Status Protocol. Wird als Protokoll für die Online-Prüfung von Zertifikaten verwendet.
OSI-Referenzmodell	Von der ISO standardisiertes Modell, das Kommunikation in sieben Schichten beschreibt: 7. Anwendungsschicht (application layer), 6. Darstellungsschicht (presentation layer), 5. Steuerungsschicht (session layer), 4. Transportschicht (transport layer), 3. Netzwerkschicht (network layer), 2. Datenverbindungsschicht (data link layer), 1. physikalische Schicht (physical layer). Die im Netz zu übermittelnden Daten durchlaufen auf der Senderseite die Schichten von 7 – 1, auf der Empfängerseite in umgekehrter Reihenfolge.
PAP	Password Authentication Protocol. Sicherungsmechanismus innerhalb des PPP zur Authentisierung der Gegenstelle. PAP definiert eine Methode, nach dem Aufbau einer Verbindung anhand eines Benutzernamens und eines Passworts die Rechte des Senders zu prüfen. Dabei geht das Passwort im Klartext über die Leitung. Der Empfänger ver-

	gleicht die Parameter mit seinen Daten und gibt bei Übereinstimmung die Verbindung frei.
PC/SC	Schnittstelle zu Smartcard Readern
PEM	Ältere Form von Soft-Zertifikaten (ohne Private Key).
Personal Firewall	Die Security-Mechanismen der Client Software vereinigen Tunneling-Verfahren und Personal Firewalling. IP-Network Address Translationen (IP-NAT) sowie universelle Filtermechanismen. Von zentraler Bedeutung ist IP-NAT, denn es sorgt dafür, dass nur vom Rechner ins Internet ausgehende Verbindungen möglich sind. Ankommende Datenpakete werden auf der Basis eines ausgeklügelten Filterings nach genau definierten Eigenschaften überprüft und bei Nichtübereinstimmung abgewiesen. Das heißt: Der Internet-Port des jeweiligen Rechners wird vollständig getarnt und der Aufbau von unerwünschten Verbindungen unmöglich.
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard. Verschlüsselungssystem mit öffentlichem Schlüssel.
PKCS#10	Die Form, wie ein Zertifikat vom PKI-Manager an die CA (Certification Authority) übertragen wird. Meist geschieht dies per Http – mit SSL verschlüsselt als Https.
PKCS#11	Basis des Smartcard-Standards
PKCS#12	Soft-Zertifikat. Standard der die Syntax der Dateistruktur beschreibt.
PKCS#15	Pointerbeschreibung: Wo befindet sich was auf der Smartcard.
PKI	(Public Key Infrastructure) Die erforderliche Schlüsselinfrastrukur zur authentischen Verteilung öffentlicher Schlüssel wird PKI genannt. Private und öffentliche Schlüssel werden für asymmetrische Kryptographie verwendet. Transaktionsbezogene Sicherheit erfordert eine eindeutige Partner-Authentisierung mittels Zertifikaten, die von einer

	vertrauenswürdigen PKI ausgestellt wurden. Insbesondere für E-Commerce bietet PKI den Rahmen für Vertraulichkeit (Geheimhaltung), Integrität (Fälschungssicherheit), Authentizität (Identitätssicherheit) und Nichtbestreitbarkeit.
PoP	Point of Presence
POP3	Protokoll zum Download von E-Mails. Gegenstück zu SMTP (Port 110)
PPP	Point-to-Point-Protokoll. Übertragunsprotokoll in verbindungsorienten Netzen.
PPP-Verhandlung	Point-to-Point-Protokoll. In einer PPP-Verhandlung wird die IP-Adresse nach Anwahl an den Provider automatisch übergeben.
PRI	Primary Rate Interface (ISDN-Schnittstelle, Primär-Multiplex S2m) mit 30 B-Kanälen und 2 D-Kanälen.
Radius	Remote Authentication Dial In User Service, siehe Directory Service
RA	Registration Authority. Meist ist die Registrierungsstelle die Stelle, die die Daten für die Beantragung eines Zertifikats entgegen nimmt. Die RA ist auch die Stelle, der der Verlust oder der Verfall eines gültigen Zertifikats gemeldet wird und die eine Widerrufsliste (Revocation List) ungültig gewordener Zertifikate herausgibt.
RAS	Remote Access Services. Firmenspezifische (Microsoft) Einwahlhilfe für Remote Access.
RIP	Routing Information Protocol, auch Routing-Modus
RFC	Request for Comment. Normentwurf, Vornorm, die im Internet diskutiert wird und so lange in der Liste der RFCs gehalten wird, so lange sie sich in der Praxis bewährt. Vorformen der RFCs sind Drafts.
Routing-Tabellen	Router benötigen für die Wegewahl im Netz Informationen über die günstigsten Routen von der Quelle zum Ziel. Mit Hilfe der Routing-Tabellen werden diese Strecken vom Router kalkuliert.

Während beim statischen Routing die Tabellen fest vorgegeben sind, erhält der Router beim dynamischen Routing über Router-Informationsprotokolle (z.B. RIP, NLSP, OSPF) Informationen über das Netz, die zu selbst erlernten Routing-Tabellen zusammengesellt werden und ständig aktualisiert werden.

RSA

Das erste Verfahren, das die Anforderungen an die Public Key-Kryptographie erfüllte. Wurde 1977 von Ron Rivest, Adi Shamier und Leonard Adlemann erfunden.

Schnittstelle

(Interface) Festlegung der zwischen zwei Geräten – bei der Datenfernübertragung im allgemeinen zwischen Datenendeinrichtung und Datenübertragungseinrichtung – erforderlichen elektrischen Verbindungsleitungen, der auf diesen herrschenden elektrischen Werten, der zur Funktion erforderlichen Signale sowie der Betriebsweise und Bedeutung dieser Signale. Man unterscheidet nach parallelen und seriellen Interfaces.

SHA

Secure Hash Algorithm, siehe auch Signatur

Signatur

Bei der digitalen Signatur wird mathematisch eine Verknüpfung zwischen Dokument und dem geheimen, persönlichen Signaturschlüssel des Teilnehmers erzeugt. Der Absender des Dokuments generiert eine Prüfsumme (sogenannter Hash-Wert), diese codiert er wiederum mit seinem Geheimschlüssel und erzeugt so einen digitalen Signaturzusatz zur ursprünglichen Nachricht. Der Empfänger des Dokuments kann mit dem öffentlichen Schlüssel des Absenders die Signatur prüfen, indem er seinerseits den Hash-Wert aus der Nachricht bildet und diesen mit der entschlüsselten Signatur vergleicht. Da die Signatur des Absenders unmittelbar in das Dokument eingebunden ist, würde jede spätere Änderung bemerkt. Auch ein Abfangen oder Abhören der Signatur über Lauschangriffe erwiese sich als zwecklos: Die digitale Signatur ist nicht nachahmbar, da sie den geheimen, privaten Schlüssel verwendet; eine Ermittlung des geheimen Schlüssels aus der Signatur ist nicht möglich.

Smartcard	Wird die Funktionalität der Smartcard genutzt, so wird nach der CHAP-Authentisierung (User ID und Passwort) die "Erweiterte Authentisierung" (Strong Authentication) mittels der auf Smartcard und Gateway hinterlegten Zertifikate durchgeführt. Auf der Smartcard befinden sich unter anderm das Benutzer-Zertifikat, das Root-Zertifikat und der geheime private Schlüssel. Die Smartcard kann nur mit PIN genutzt werden.
SMTP	Simple Mail Transport Protocol. Internet Standard zur Verteilung elektronischer Post. Ist textorientiert und setzt auf TCP auf (Port 25)
SNA	Systems Network Architecture. Hierarchisch orientiertes Netz zur Steuerung von Terminals und zur Unterstützung des Zugriffs auf Anwendungen in IBM Host-Systemen.
SNMP	Simple Network Management Protocol. Netzwerk-Managementprotokoll auf Basis von UDP/IP.
Source Routing	Möglichkeit, in Token Ring-Netzwerken eine Wegewahl zwischen Bridges zu optimieren. Dabei werden die Wegeinformationen an den Datenblock angehängt mit übertragen. Auf diese Weise liegt auch der Weg für die Bestätigung eindeutig fest.
SPD	Security Policy Database
SSL	Secure Socket Layer. Gemäß dem SSL-Protokoll kann der dynamische Schlüsselaustausch (Dynamic Key Exchange) genutzt werden. SSL, von Netscape entwickelt, ist mittlerweile das Standard-Protokoll für dynamischen Schlüsselaustausch.
SSLCP	Secure Socket Layer Control Protocol
STARCOS	Betriebssystem für Smartcards
Symmetrische Verschlüsselung	Sender und Empfänger verwenden bei der symmetrischen Chiffrierung und Dechiffrierung den gleichen Schlüssel. Symmetrische Algorithmen sind sehr schnell und sehr sicher – dies allerdings nur dann, wenn die Schlüsselübergabe zwischen dem Sender und dem Empfänger ungefährdet erfolgen kann. Gelangt ein Unbefugter in den Besitz des Schlüssels, so kann dieser alle Nachrichten ent-

schlüsseln bzw. sich unter Verwendung des Schlüssels als Absender von Nachrichten ausgeben. Soll bei der symmetrischen Verschlüsselung in größeren Gruppen jeder Teilnehmer nur an ihn adressierte Nachrichten lesen können, so ist für jedes Sender-Empfänger-Paar ein eigener Schlüssel notwendig. Die Folge: ein aufwendiges Schlüsselmanagement. So sind bei 1.000 Teilnehmern bereits 499.500 (!) unterschiedliche Schlüssel erforderlich, um sämtliche Wechselbeziehungen zu unterstützen. Bekannteste symmetrische Verschlüsselung ist heute der DES-Algorithmus.

TCP/IP

Transmission Control Protocol / Internet Protocol. TCP/IP ist ein Netzwerkprotokoll für heterogene Netze und an kein Transportmedium gebunden. Es kann auf X.25, Token Ring oder einfach auf die serielle Schnittstelle aufsetzen und eignet sich deshalb besonders als Kommunikati-onsprotokoll für unterschiedliche (Netz-) Topologien und Rechner-Plattformen, wie sie im Internet gekoppelt sind. Dabei wird jeder Rechner im Netzverbund Internet durch seine IP-Adresse identifiziert. TCP/IP umfaßt außerdem vier Internet-Standardfunktonen: 1. FTP: File Transfer Protocol für den Dateitransfer von einem zum anderen Rechner, 2. SMTP: Simple Mail Transport Protocol für E-Mail, 3. TELNET: Teletype Network für Terminalemulation, 4. RLOGIN: Remote Login zur Rechnerfernbedienung

TECOS

Betriebssystem für Smartcards (Versionen 1.2, 2.0)

Token Ring

Netzwerktopologie mit Ringstruktur von IBM.

UDP

User Data Protocol. Baut direkt auf dem darunter liegenden Internet Protokoll auf. Wurde definidert, um auch Anwendungsprozessen die direkte Möglichkeit zu geben, Datagramme zu versenden. UDP liefert über die Leistungen von IP hinaus lediglich eine Portnummer und eine Prüfsumme der Daten. Durch das Fehlen des Overheads mit Quittungen und Sicherungen ist es besonders schnell und effizient.

UMTS	Universal Mobile Telecommunications Service. Künftiger Standard für schnelle Handy-Kommunikation.
VPN	Virtual Private Network. Ein VPN kann als virtuelles Netz grundsätzlich über alle IP-Trägernetze – also auch das Internet – eingerichtet werden. Für die Realisation haben sich zwei Spezifikationen herauskristallisiert: L2F (Layer 2 Forwarding) und L2TP (Layer 2 Tunneling Protocol). Beide Verfahren dienen dazu, einen Tunnel aufzubauen, den man als eine Art “virtuelle Standleitung” bezeichnen kann. Über eine solche logische Verbindung lassen sich neben IP-Frames auch IPX-, SNA- und NetBIOS-Daten transparent übertragen. Am Tunnelende müssen die Datenpakete interpretiert und zu einem Datenstrom auf der Basis des verwendeten Protokolls umgewandelt werden.
WAP	Wireless Application Protocol. Entwicklung von Nokia, Ericson und Motorola.
X.509 v3	Standard Zertifizierung
Zertifikate	Zertificate (Certificates) werden von einer CA (Certification Authority) mittels PKI-Manager (Software) ausgestellt und auf eine Smartcard (Chipkarte) gebrannt. Diese Smartcard enthält u.a. mit den Zertifikaten digitale Signaturen, die ihr den Status eines digitalen Personalausweises verleihen.

Index

E

F

G

H

I

K

L

M

N

P

R

S

T

U

V

W

X

Z

A

B

C

D

E

F

G

H

I

K

L

M

N

P

R

X

Z