NCP
SECURE COMMUNICATIONS

Secure CE Client

NCP
SECURE COMMUNICATIONS

Secure CE Client

Version 2.30
Dezember 2006

Copyright

Gesamtherstellung dieses Handbuchs:
Michael Lösel
Dokumentation + Publikation
Pirckheimerstr. 47
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 CE Client**

  Der NCP Secure CE Client, bestehend aus Client Monitor und Client Service, wird auf dem mobilen Endgerät (PDA) installiert. Der PDA-Monitor mit integriertem Telefonbuch dient der Statusanzeige und Anwahl an das zentrale Secure Gateway.

  Betriebssysteme: Windows CE 3.0 (Handheld PC 2000, Pocket PC 2002), Windows CE.net 4.2 (Windows Mobile 2003 for Pocket PC), Windows CE 5 (Windows Mobile 5)

- **NCP Secure CE Client Configurator**

  Der NCP Secure CE Client Configurator ist die PC-Komponente. Sie dient der Synchronisation des Datenbestandes im PDA und der Erstellung aller Einträge im Telefonbuch (Konfiguration des Clients).

  Betriebssysteme: Windows 98se/NT(4.0) SP5/2000/XP/ME

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

1.1 Secure Enterprise CE Client

Die NCP Secure CE Client ist in der Enterprise- und in der Entry-Version verfügbar. Der Unterschied zwischen beiden Produkten besteht darin, dass die Enterprise CE Client Software zentral administrierbar ist (NCP Secure Enterprise Management zusätzlich erforderlich). Der NCP Secure Enterprise Client ist in Varianten der Betriebssysteme Windows, Linux und Windows CE erhältlich und unterstützt Virtual Private Networks (VPN) sowie eine Public Key Infrastructure (PKI). Der Client ist Bestandteil der Secure Enterprise Solution, die aus den Komponenten Secure Enterprise Client, Secure Enterprise Gateway, Secure Enterprise Management und Secure Enterprise High Availability Services besteht.

Der NCP Secure Enterprise CE Client ist eine Komponente der ganzheitlichen NCP Secure Enterprise Solution. Die Kommunikationssoftware dient dem universellen Teleworking in beliebigen Remote Access VPN-Umgebungen. Auf Basis des IPSec-Standards können hochsichere Datenverbindungen auch zu VPN-Gateways aller namhaften Anbieter hergestellt werden. Der Datentransfer erfolgt über beliebige öffentliche Funknetze, das Internet sowie Nahbereichs-Funknetze wie wireless LANs am Firmengelände und an Hotspots. Mobile Teleworker können beispielsweise mittels Pocket PC, Handheld oder Tablet PC, weltweit auf zentrale Datenbestände und Anwendungen zugreifen. Ein weiteres interessantes Einsatzgebiet ist die mobile Datenerfassung z. B. mittels PDA über einen integrierten Barcode-Leser im Warenlager und Datentransfer via WLAN in das zentrale Warenwirtschaftssystem.

Universelle Einsatzmöglichkeiten fordern umfangreiche Sicherheitsmechanismen zur Abwehr von Attacken in jeder Remote Access-Umgebung. Auch an Hotspots während des An- und Abmeldevorganges. Die wichtigsten, integrierten Security-Bausteine sind neben dem VPN-Tunneling: Datenverschlüsselung, eine dynamische Personal Firewall, die Unterstützung von OTP-Token (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure). Mittels der Personal Firewall können Regelwerke für: Ports, IP-Adressen und Segmente sowie Applikationen definiert werden.

Ein weiteres Sicherheitsmerkmal ist “Friendly Net Detection”, d. h. die automatische Erkennung von sicheren und unsicheren Netzen. In Abhängigkeit davon werden die entsprechenden Firewall-Regeln aktiviert bzw. deaktiviert. Alle Konfigurationen können zentral vom Administrator eingegeben und durch den Anwender nicht ver-änderbar eingestellt werden. Mechanismen des zentralen Managements ermöglichen eine automatische Übernahme aller Konfigurationsparameter in den Client. Der NCP-Dialer bietet zudem Schutz vor kostenintensiven Fremd-Dialern.

“Easy-to-use”, d. h. einfache Installation und Bedienung der Client Software. Dafür stehen der integrierte Konfigurations-Assistent für den Konfigurations-PC und eine intuitive, grafische Benutzeroberfläche am mobilen Endgerät. Unterbrechungen einer Funkverbindung während eines Datentransfers z. B. bei Funkausfällen oder beim Wechsel von Access Points im WLAN bleiben ohne Auswirkungen auf die transparente Arbeitsweise.

1.1.1 Leistungsmerkmale

WLAN-Handover und Roaming bei Wechsel des Funknetzes

Wechsel zwischen Access Points in einem WLAN oder verschiedenen Funknetzen (z. B. vom WLAN nach UMTS) während einer Datenverbindung in das Firmennetz, erfolgen für den Anwender ohne spürbare Unterbrechung. Ein umständlicher Neustart des PDA entfällt. Eine getunnelte Session zum Secure Gateway bleibt erhalten. Die Vergabe der dynamischen IP-Adresse wird innerhalb des Verbindungsmanagements automatisch gesteuert

Automatischer Wiederaufbau nach Unterbrechung der Funkstrecke

Werden in einem VPN-Tunnel von der Zentrale aus Daten an das mobile Endgerät übertragen z. B. im Falle eines E-Mail Push-Dienstes und die Funkstrecke wird unterbrochen, beispielsweise in einem Funkloch, etabliert der NCP Client bei erneuter Verfügbarkeit des Funknetzes automatisch eine sichere Verbindung in die Firmenzentrale, um wieder erreichbar zu sein.

Netzwerkanmeldung trotz Standby-Betrieb oder Abschalten des PDAs

PDAs, MDAs etc. werden wie alle mobilen Endgeräte mit Akkus betrieben. Um Energie zu sparen schalten diese Geräte während eines Netzwerkzugriffes wenn aktuell kein Datenaustausch stattfindet, automatisch in den Standby-Mode. Oder sie werden ganz bewusst durch den Benutzer abgeschaltet. Um auch in diesen Fällen ein kontinuierliches Arbeiten zu gewährleisten, bleibt der User logisch im Firmennetz angemeldet (Reservierung der IP-Adresse). Er kann bei Bedarf jederzeit ohne Neuanmeldung weiterarbeiten.

Einfache Bedienung

Die intuitive, grafische Benutzeroberfläche (Monitor) zeigt alle Verbindungsparameter (Einwahl, Authentisierung, Verschlüsselung, Datenkompression) am mobilen Endgerät an. Der Anwender kann den kompletten Verbindungsaufbau verfolgen und ist zudem jederzeit über den Verbindungsstatus informiert. Im Fehlerfall ist eine schnelle, präzise Auskunft an den zentralen Support mit entsprechend kurzen Service-Zeiten möglich.

Hohe Sicherheit

Eine starke Kryptografie mit einer Schlüssellänge größer/gleich 128 Bit symmetrisch (3DES, Blowfish, AES) und 1024/2048 Bit asymmetrisch (z.B. RSA) sorgt für hochsichere Daten. Die mögliche Schlüsselanzahl beträgt 1038 Varianten. Um nur einen dieser Schlüssel zu knacken müssten 1000 Pentium-PCs 5 Jahre ununterbrochen rechnen. Hinzu kommt, dass bei jeder Verbindung ein neuer Schlüssel generiert wird!

1.2 Secure Enterprise Client

Die NCP Enterprise Client-Software setzt Maßstäbe und integriert alle Technologien, die dazu beitragen ein Maximum an Sicherheit, Universalität, Administrierbarkeit und Wirtschaftlichkeit (TCO) in Remote Access-Projekten zu erreichen. Stationäre und mobile PC-Arbeitsplätze werden über öffentliche Netze (via Internet) hinweg als vollwertige Teilnehmer in das Firmennetz integriert. Teleworker arbeiten in gewohnter Weise wie an einem Büroarbeitsplatz. Ihnen stehen alle LAN-Applikationen und -Resourcen 1:1 am remote PC zur Verfügung.

Die Software arbeitet nach dem Prinzip der LAN-Emulation, d.h. sie erscheint dem PC-Betriebssystem gegenüber als LAN-Adapter (virtueller Netzwerkadapter). Deshalb ist es u.a. möglich, dem remote Client vom zentralen Secure Enterprise Gateway eine private IP-Adresse zuzuweisen. Diese kann je nach Anforderung fest oder variabel (dynamisch) aus einem Adresspool zugeordnet werden. Bei Bedarf kann eine einmal zugewiesene IP-Adresse trotz physikalischem Verbindungsabbau (z.B. bei Short-Hold-Mode) beibehalten werden, d.h. die logische Verbindung zwischen remote Client und zentraler LAN-Resource bleibt erhalten. Auch die Einwahl in verschiedene Standort-Netze bereitet trotz wechselnder IP-Adressen keine Probleme. Der remote User ist immer mit demselben Namen im Unternehmensnetz identifizierbar, wo immer er sich auch befindet. Weiter ist die Einbindung in eine DDNS-Struktur (Dynamic Domain Name Service-Protokoll) möglich. Optional kann der Verbindungsaufbau und die Überwachung mit dem zentralen Server für den Anwender unbemerkt automatisiert im Hintergrund seiner Tätigkeiten erfolgen.

Der NCP Secure Enterprise Client ist in jeder Remote Access-Umgebungen universell einsetzbar. Das bedeutet:

- ☐ Unabhängigkeit vom Übertragungsmedium (Mediatyp-neutral)
- ☐ Unterstützung aller marktgängigen Betriebssysteme und unterschiedlichster Endgeräte
- ☐ Sicherheit und Managebarkeit durch Unabhängigkeit vom Microsoft DFÜ-Dialer
- ☐ Kommunikation mit IPSec-Gateways auch von Drittherstellern (Kompatibilität)
- ☐ Installation auf Einzelplatz-PCs und LAN-PCs (auch hinter IP-Routern mit IP-NAT)
- ☐ Unterstützung aller Sicherheits-Standards (Übertragungs- und Zugangssicherheit) Als Remote Access-Gegenstellen dienen die verschiedenen NCP Secure Enterprise Server.

Die NCP Secure Communications Lösung garantiert durch die standardmäßig integrierte Personal Firewall, dass ein Telearbeitsplatz aus dem Internet und von anderen LAN-Teilnehmern (z.B. an Hotspots) nicht attackiert werden kann!

Das NCP Secure Enterprise Management bietet einen lückenlosen Funktionsumfang. Maximale Transparenz für die Netzwerkadministration und Minimierung der TCOs (Total Costs of Ownership) sind garantiert.

1.3 Secure Communications

NCP Secure Communications steht für “hochsichere Datenkommunikation in öffentlichen Netzen” (Internet). Informationen jeder Art (z. B. Geschäfts-, Personen- oder Betriebsdaten) werden auf der gesamten Übertragungsstrecke gegen unberechtigte Zugriffe abgeschottet. Integrierte Sicherheitsmechanismen verhindern zudem Attacken auf die Endgeräte und letztlich den unerlaubten Zugriff auf das Firmennetz (Back Doors).

Stationäre und mobile Teleworker sowie Filialen können in ein zentral administrierbares Datennetz eingebunden werden. Für eine starke User-Authentisierung können elektronische Zertifikate in einer Public Key-Infrastruktur (PKI) genutzt werden.

NCP Secure Communications bedeutet für Sie

1. Realisierung beliebiger Remote Access-Umgebungen

   – Mobil, stationär, im remote LAN (z.B. Filiale)
   – Laptop, Notebook, MDA, PDA, Tablet PC, Smartphone etc.
   – Betriebsdatenerfassungsgeräte, Automaten
   – ISDN, analoges Fernsprechnetz, GSM, GPRS, UMTS, xDSL, Internet, WLANs (lokal, remote)

2. Hochsicherer Transfer aller Daten zwischen remote Client und zentralem Server nach dem End-to-End-Prinzip

3. Nutzung aller LAN-Applikationen 1:1 auf dem Telearbeitsplatz

4. Unabhängigkeit von den Schwächen und Defiziten der PC-Betriebssysteme bezüglich Security und Wirtschaftlichkeit.

5. Hohe Integrationsfähigkeit in eine bereits existierende IT-Infrastruktur (VPN-Gateways, Firewalls, Router etc.) durch konsequente Umsetzung von Standards

6. Schaffung einer einheitlichen Plattform für High Security Remote Access-Anwendungen mit zentralem Management

7. Hohe Flexibilität und Wirtschaftlichkeit durch einfache Software-Updates und -Upgrades sowie integrierte Automatismen für Gebührenminimierung, Roll Out und Administration.

8. Komplett-Lösung, d.h. alles aus einer Hand: Produkte & Services

9. Partnerschaftliche Zusammenarbeit “Made in Germany”

Secure Communications bietet ein differenziertes Produktportfolio. Sei es für jede Unternehmensgröße als Einzelkomponenten oder als preiswertes Kompakt-Paket für kleinere Remote Access-Umgebungen. Die komplette NCP-Lösung besteht aus Secure Client-, Secure Gateway- und Secure Management-Software.

1.4 Secure Enterprise Solution

Die NCP Secure Enterprise Solution ist eine umfassende Remote Access-Lösung auf höchstem technischen Niveau. Sie bietet alle Komponenten, die für Einführung, Umsetzung, Betrieb, Management- und Bedienbarkeit erforderlich sind. Communications- & Security-Technologien bilden eine integrative Gesamtheit auf einmalige Art und Weise.

Alle Enterprise-Produkte: Secure Enterprise Client, Secure Enterprise Gateway, Secure Enterprise Management und die Secure Enterprise High Availability Services sind optimal aufeinander abgestimmt. Auch umfangreiche Remote Access-Projekte bleiben überschaubar. Rollout, Konfiguration und Administration der verteilten PC-Arbeitsplätze bzw. Datenendgeräte werden durch übersichtliche Oberflächen und integrierte Automatismen des zentralen Enterprise Managements optimiert. Die Verfügbarkeit der zentralen Gateways wird permanent überwacht. Die integrierte Firewall-Funktionalität sorgt für zentrale und dezentrale Sicherheit gegen Attacken aus dem Internet.

Die Einwahl auf das zentrale Secure Gateway kann über den NCP oder Microsoft RAS Dialer erfolgen. Welcher Dialer genutzt wird, hängt einerseits von der eingesetzten Hardwarekomponente bzw. dem Handy oder Modem ab das für den Verbindungsaufbau genutzt wird und andererseits davon, ob der Einwahlpunkt (ISP) ein Einwahl-Skript benötigt.

Unterstützt werden Modems (Handys) und LAN-Adapter. Die Konfiguration des PDAs erfolgt über einen separaten Standard-PC. Der Secure CE VPN/PKI Client unterstützt digitale Zertifikate (X.509 v3) auf Smart Cards und als Software (Soft-Zertifikate). Der Verbindungsaufbau erfolgt erst nach erfolgreicher Überprüfung des Server-Zertifikates. Updates können optional über den Secure Update Server durchgeführt werden.

1.4.1 Technische Daten

- **Kommunikationsschnittstellen**

  – ISDN CAPI 2.0
  – NDIS
  – PPPoE
  – PPPoC (mit AVM Fritz! DSL)
  – Modem
  – IP
  – GPRS/UMTS

- **Netzwerkprotokolle**

  – IP
  – IPX

- **VPN-Tunneling**

  – IPSec (IPSec nach RFC 2401-2409, XAUTH, IKE-Config, DPD, NAT-T)
  – IPSec over L2TP (Pre-Shared-Key, Zertifikate, zentrale Konfiguration der Proposals)
  – L2Sec (SSL-Handshake in PPP-Verh., TLS/EAP RFC 2716, SSLCP ohne/mit Zertifikat)

- **Verschlüsselung**

  – Triple DES (128, 192 Bit)
  – Blowfish (128 Bit)
  – AES (128, 192, 256 Bit)
  – RSA (1024, 2048 Bit)
  – BitDH-Group (1,2,5)

- **Hash-Verfahren**

  – SHA1 (Secure Hash Algorithm 1)
  – MD5 (Message Digit 5)
  – SNMP over SSL: Verschlüsselung der im SNMP-Protokoll im Klartext übertragenen Daten auf Basis einer SSL-Verbindung

- **Personal Firewall**

  – IP-NAT (Network Address Translation)
  – Stateful Packet Inspection
  – Friendly Net-Erkennung (Auswertung der aktuellen Adresse, IP-Adr. des DHCP-Servers)
  – Automatische Hotspot-Erkennung
  – Differenzierte Filterregeln bezüglich: Applikation, Protokoll, Port, Adresse, Verbindung

- **Line Management**

  Short hold, Timeout (zeit-und gebührenimpulsgesteuert)

■ **Datenkompression**

Stac, Deflate

■ **Kanalbündelung**

Dynamisch (bis 8 Kanäle), frei konfigurierbarer Schwellwert

■ **Filtering**

IP Broadcasts, NetBIOS over IP

■ **Leitungs-Backup xDSL/ISDN mit Fallback**

■ **Budget-Manager**

■ **DPD Timeout**

Vom Timeout unabhängige Überwachung einer etablierten VPN Layer-2-Tunnelverbindung durch Polling. Bei einer Störung erfolgt automatischer Verbindungsabbau. Die freien Resourcen stehen anderen Secure Clients zur Verfügung.

■ **PKI**

– Unterstützung von Public Key Infrastrukturen nach X.509 v.3 Standard, Entrust (Entrust Ready)
– SmartCards: PKCS#11, TCOS 1.2 und 2.0 (über CT-API oder PC/SC)
– Soft Zertifikate: PKCS#12
– PIN-Richtlinie: Administrative Vorgabe für die Eingabe beliebig komplexer PINs
– Revocation Lists: Überprüfung der CRL (Certificate Revocation List) und ARL (Authority Revocation List)
– Automatischer Download der Sperrliste von der CA (Certification Authority) in definierten Zeitintervallen
– Online-Check: Überprüfung der Zertifikate mittels OCSP oder OCSP over http gegen die CA
– Zertifikatskontrolle: Überprüfung und Hinweis der Gültigkeitsdauer eines Zertifikates

■ **Einmal-Passwort (OTP)**

– Komfortable Eingabe durch Trennung von PIN und Passwort
– RSA SecurID-Unterstützung
– Das Secure Gateway kann während der Einwahlphase mit zwei Arten von AAA-Servern korrespondieren:
  – zur Client-Authentisierung mit dem OTP-Server
  – für die Client-Link-Konfiguration mit dem RADIUS Server

Das One Time Password kann für einen definierbaren Zeitraum seine Gültigkeit behalten. Die in Sekunden zu bestimmende Haltedauer läuft ab dem Zeitpunkt der Ersteinwahl ab.

Extensible Authentication Protocol (EAP)

– EAP-MD5 Extensible Authentication Protocol, erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2) auf Basis von User-ID/Password
– EAP-TLS Extensible Authentication Protocol – Transport Layer Security, erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2) auf Basis von Zertifikaten

DynDNS

Unterstützung von Dynamic DNS (Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse, Abfrage der aktuellen IP-Adresse über einen öffentlichen DynDNS-Server)

DDNS

– Dynamic DNS Server-Protokoll Erweiterung des Domain Name Servers (DNS) ermöglicht das Hinzufügen, Löschen und Ersetzen von Domainnamen. Das Secure Gateway vergibt eine IP-Adresse an den Secure Client und leitet diese jeweils an den internen DNS-Server weiter.
– Erreichbarkeit des remote Users unter einem (festen) Namen trotz wechselnder IP-Adressen.

Lockruf

Dial Out-Funktionalität, Anwahl des remote Servers/Gateways mittels dem ISDN-Leistungsmerkmal “Anklopfen im D-Kanal”.

Benutzerverwaltung

Drei Möglichkeiten der Benutzerverwaltung:
– lokal d.h. Daten sind im Secure Gateway abgelegt
– RADIUS, d.h. Daten werden in einem externen RADIUS Server gepflegt z.B. integrierter RADIUS-Server im NCP Secure Enterprise Management
– Verzeichnisdienst (LDAP), d.h. Daten werden im Verzeichnisdienst verwaltet (Kombinationen sind konfigurierbar)

Pooladressen-Verwaltung

Reservierung einer bestimmten IP-Adresse aus einem Poolinnerhalb einer definierbaren Haltedauer (Lease Time)

Low-Level-Call-Back

Rückruf nach Anklopfen im ISDN D-Kanal (Cisco-kompatibel)

Connection Manager

Für die internationale Einwahl in das T-Online Netz, GRIC, UuNet, Infonet.

Point-to-Point Protokolle

– PPP over ISDN
– PPP over GSM (V.110)
– PPP over PSTN (Modem)
– PPP over Ethernet (xDSL)
– PPP over Capi (Unterstützung von AVM Fritz DSL)
– PPP LCP Link Control Protocol
– PPP IPCP IP Control Protocol
– PPP IPXCP IPX Control Protocol
– PPP MLP Multilink Protocol
– PPP Call Back Verhandlung im LLCP
– PPP CCP Compression Control Protocol
– PPP PAP Password Authentication Protocol
– PPP CHAP Callenge Handshake Authenication Protocol
– PPP ECP Encryption Control Protocol

Grafische Benutzeroberfläche

– Intuitive Bedienung
– Client Monitor mit übersichtlicher Anzeige des Verbindungsstatus und einfacher Eingabe von Konfigurationsparametern vor Ort (wenn zentral freigegeben).

Eigener Dialer

Von Microsoft DFÜ-Netzwerk unabhängiger Dialer mit erweitertem Leistungsumfang:
– Short Holde Mode
– Betriebssystemunabhängigkeit
– Remote Administration: Über IP und CAPI, Verbindungstests, Konfiguration, Traces
– Integrierte Personal-Firewall
– Schutz vor fremden Dialern (0190, 0900)
– Für ISP-Einwahl mittels Einwahlskript wird MS RAS-Dialer unterstützt.

iPass-Integration

Clients und iPass-Clients unter einer einheitlichen Benutzeroberfläche. (Optional mit zentralem Management)

Management

Secure Enterprise Management für die zentrale Verwaltung eines VPN

High Availability Services

Failsafe- und Loadbalancing-Server für max. Verfügbarkeit und gleichmäßige Auslastung aller zentralen Gateways

Systemanforderungen (empfohlene Mindestausstattung)

■ Secure Enterprise VPN Gateway (ohne und mit PKI)

– Pro 250 gleichzeitig nutzbarer Tunnel 64 MB Arbeitsspeicher
– CPU Pentium III
– Taktung: Pro 150 MHz kann ein Datendurchsatz von ca. 2 Mbit realisiert werden (inkl. Symmetrische Verschlüsselung von 128 / 448 Bit)
– Ca. 50 MB freier Speicher auf der Festplatte
– Betriebssysteme: WinNT 4.0 (ab SP5), Win2000 (s.u.), Linux

■ Secure Enterprise CE Client

Systemanforderungen für das mobile Endgerät:
– Betriebssysteme Windows CE 3.0, Windows CE.net 4.2, Windows Mobile 5.0
– ca. 3 MB Programmspeicher
– ca. 1 MB freier Datenspeicher
– StrongARM-Prozessor (mind. 200 MHz)

Systemanforderungen für die PC-Komponente:
– Betriebssysteme Windows 98se/NT(4.0) SP5 /2000/XP
– 32 MB Arbeitsspeicher
– 15 MB freier Speicher auf der Festplatte
– Installation von Microsoft ActiveSync ab Version 3.0

■ Secure Enterprise High Availability Server

– 64 MB Arbeitsspeicher
– CPU Pentium III, Taktung: min. 500 MHz
– Mind. 20 MB freier Speicher auf der Festplatte
– Betriebssysteme: WinNT 4.0 (ab SP5), Win2000 (s.u.)
  Das Betriebssystem ist abhängig von den genutzten Netzwerkprotokollen:
  1. IP, statisches Routing: NT 4.0 Workstation ab SP5; Win2000 Professional
  2. IP oder IPX mit RIP, dynamisches Routing (für IP): NT 4.0 Server ab SP5, Win2000 Server
– Folgende Dienste sollten deaktiviert werden (Empfehlung):
  Computer Suchdienst (Browser)
  Serverdienst
  MS IIS sollte nicht installiert sein, ebenso FTP

Diese Seite ist frei

2. Installation

Die Installation der Secure CE Client Software erfolgt für alle Windows-Systeme komfortabel über Setup. Bevor Sie die Software installieren, müssen jedoch die Installationsvoraussetzungen erfüllt sein, die im folgenden Kapitel beschrieben sind.

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

- **PC-Komponente**

  Die PC-Komponente verfügt über den NCP Secure CE Client Configurator zur Erstellung des Telefonbuchs. Von diesem Configurator wird über ActiveSync das Telefonbuch auf den PDA kopiert.

- **PDA-Komponente**

  Die PDA-Komponente besteht aus dem NCP Secure 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 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 Service am PDA (bei Einsatz der Strong Security-Version)

☑ Konfiguration des Zielsystems am PC

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

☑ Inbetriebnahme am PDA

2.1 Installationsvoraussetzungen

Betriebssysteme

Die PC-Komponente der Secure CE Software kann auf Computern mit den Betriebssystemen Microsoft Windows 98se/NT(4.0) SP5, Windows 2000, Windows XP und Windows ME installiert werden. (Andere Betriebssysteme auf Anfrage.) Außerdem:
– 32 MB Arbeitsspeicher
– 15 MB freier Speicher auf der Festplatte
– Installation von Microsoft ActiveSync ab Version 4.x

Über das Programm Microsoft ActiveSync 4.x oder höher wird die PDA-Komponente installiert und erfolgt der Datenaustausch zwischen mobilem Endgerät (PDA) und PC.

Auf dem mobilen Endgerät muss eines der folgenden Betriebssysteme installiert sein: Windows CE 3.0 (Handheld PC 2000, Pocket PC 2002), Windows CE.net 4.2 (Windows Mobile 2003 for Pocket PC), Windows CE 5 (Windows Mobile 5).Außerdem:
– ca. 3 MB Programmspeicher
– ca. 2 MB freier Datenspeicher
– StrongARM-Prozessor (mind. 200 MHz)

Lokales System

Die Einwahl an das Zielsystem erfolgt über das mobile Endgerät. Als Endgerät dient ein PDA (Personal Digital Assistant), MDA, Tablet PC oder Smart Phone. 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.

Datenverbindungen, zu deren Aufbau ein Initialisierungs-String nötig ist (meist GPRS) können nur über den NCP-Dialer aufgebaut werden, d.h. wenn nicht der Microsoft RAS-Dialer genutzt wird (siehe → Telefonbuch, Modem).

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

■ LAN-Adapter (LAN 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.

■ WLAN-Adapter unter Windows Mobile (WLAN)

Unter Windows Mobile kann der WLAN-Adapter mit der Verbindungsart “WLAN” betrieben werden. Im Configurator-menü erscheint eigens der Menüpunkt “WLAN-Einstellungen”, worin die Zugangsdaten zum Funknetz in einem Profil hinterlegt werden können. Wird diese “WLAN-Konfiguration aktiviert”, so muss das Management-Tool der WLAN-Karte deaktiviert werden. (Alternativ kann auch das Management-Tool der WLAN-Karte genutzt werden, dann darf die WLAN-Konfiguration im Configuratormenü nicht aktiviert werden.)

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 Monitor 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 Monitor der PC-Komponente, Konfiguration, Zertifikate) muss zu dem Ort der Datei auf dem PDA passen!

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

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

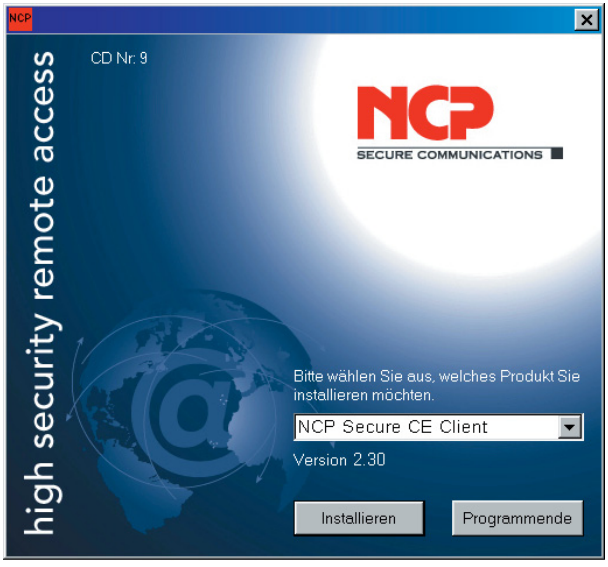
2.2 Installation der PC-Komponente

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

2.2.1 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 den unter “Installation von Diskette” beschriebenen identisch.

2.2.2 Installation von CD



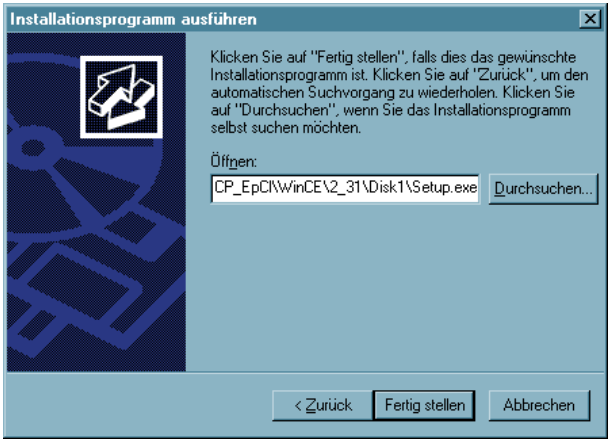
Nachdem Sie die CD in das Laufwerk Ihres Computers eingelegt haben, erscheint nach einigen Sekunden automatisch die NCP-Begrüßungsmaske auf Ihrem Monitor (siehe Bild links).

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

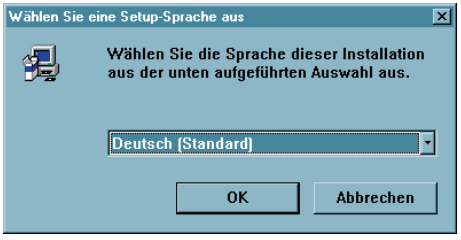
2.2.3 Installation von Wechseldatenträger

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.” Hier wählen Sie “Software” und klicken anschließend auf den Button “Neue Programme hinzufügen”. Legen bzw. stecken Sie nun den Wechsel-datenträger mit der Software in das Laufwerk Ihres Computers (siehe Bild links) und klicken Sie “Weiter”...



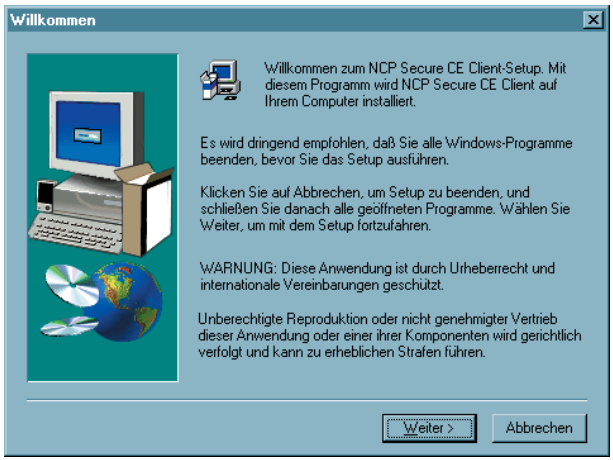
Wenn “SETUP.EXE” angezeigt wird, klicken Sie auf “Fertigstellen”.



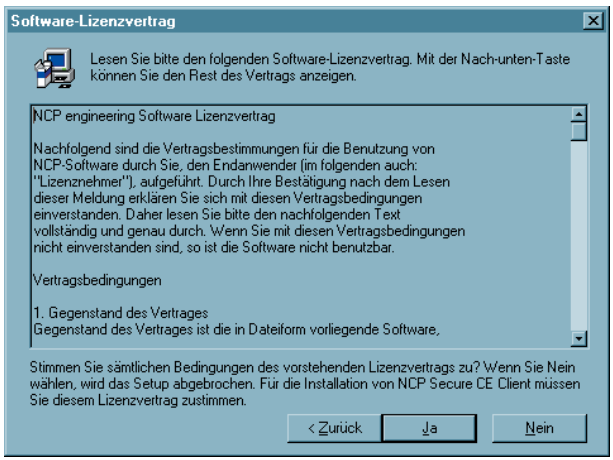
Im folgenden Fenster können Sie die Setup-Sprache auswählen. Klicken Sie danach auf “OK”.

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.

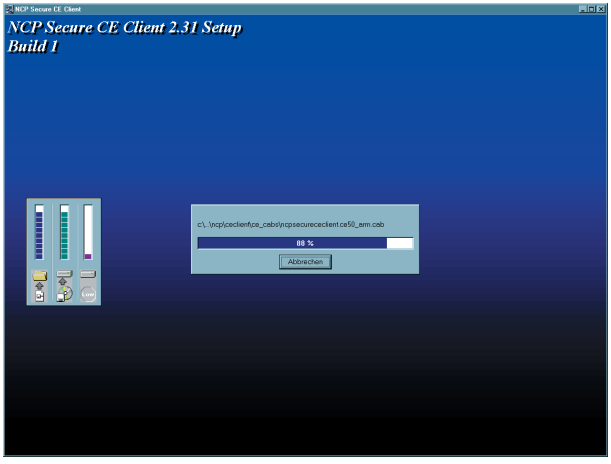
(Die Lizenzierung erfolgt erst auf Ihrem PDA-Gerät.)

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

→ *weiter nächste Seite*

Außerdem können Sie den Programmordner festlegen ...

... und schließend das Programm-Icon auf dem Desktop anzeigen lassen.



Dann werden die Dateien eingespielt.

→ *weiter nächste Seite*

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

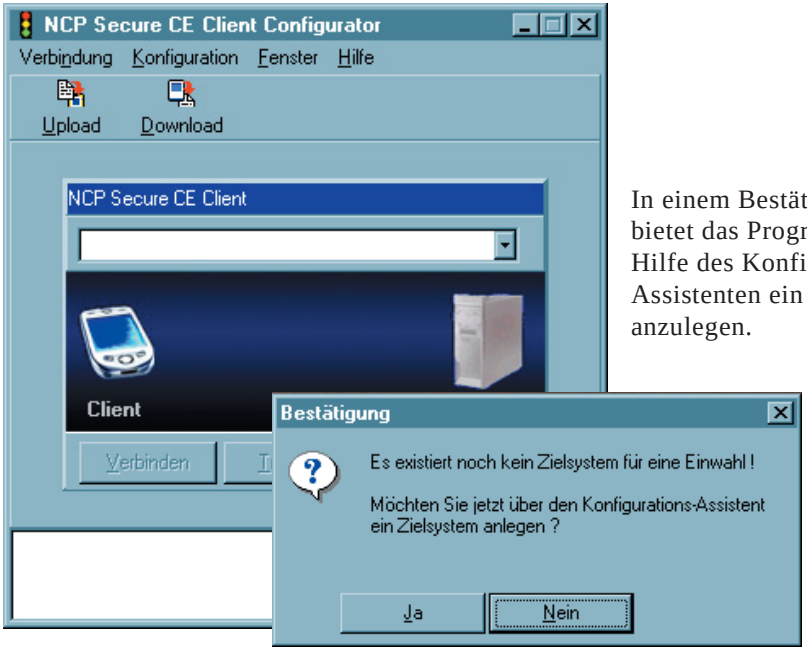
Belassen Sie die Einstellung “PDA-Installation starten”, so wird automatisch nach Beendigung der Installation der PC-Komponente die PDA-Komponente installiert. Entfernen Sie die Installationsautomatik, so kann die PDA-Komponente auch zu einem späteren Zeitpunkt installiert werden. Siehe dazu

→ *2.6 Installation der PDA-Komponente*

Im Windows-Startmenü finden Sie nach der Installation in der Programmgruppe “NCP Secure Client” das Programm “Secure Enterprise CE Client Configurator”. Mit diesem Programm erfolgt die Konfiguration der Zielsysteme, die Zusammenstellung des Telefonbuchs und die Übertragung des Telefonbuchs auf den PDA (siehe →Client Monitor der PC-Komponente).

2.3 Vor der Inbetriebnahme

Nach der Installation zeigt sich der NCP Secure Enterprise CE Configurator wie in untenstehender Abbildung. Um den Secure Entry CE Client nutzen zu können, muss zunächst im Telefonbuch ein Eintrag für ein Zielsystem erzeugt werden, zu dem eine 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 / Telefonbuch und IPSec

Zu einer weiteren Parametrisierung beachten Sie bitte
– 5.1 Telefonbuch (Die Parameterfelder zur Konfiguration der Verbindung)

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

2.4 Übertragen des Telefonbuchs und der Zertifikate

2.4.1 Telefonbuch

Vor dem Übertragen des Telefonbuchs muss zunächst das Zielsystem am PC konfiguriert werden und das Telefonbuch komplettiert sein. Beachten Sie deshalb zunächst die Abschnitte “Client-Monitor 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 Monitor 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 Telefonbuchs ist im Abschnitt “Upload des Telefonbuchs” beschrieben.

2.4.2 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.

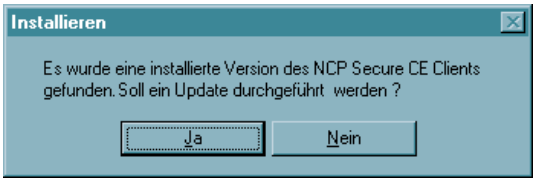
Nutzen Sie eigene Soft-Zertifikate, so müssen diese vom PC via ActiveSync übertragen werden. Beachten Sie dabei, dass der PDA nur CA-Zertifikate im DER-Formats (Distinguished Encoding Rules) mit den Dateiendungen DER, CER oder CRT lesen kann! Das PEM-Format wird nicht unterstützt.

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

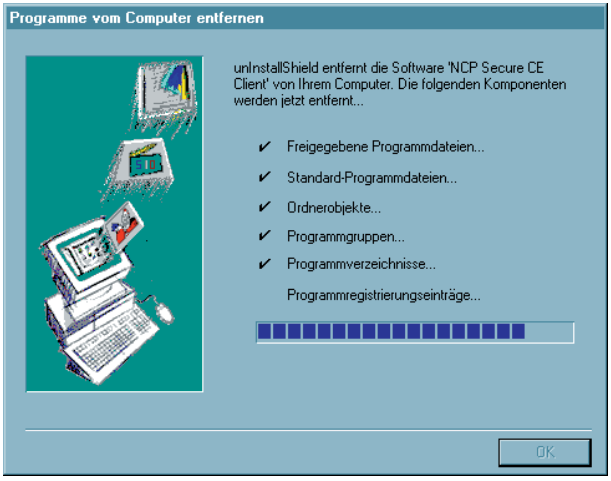
Das Zielverzeichnis auf dem PDA für das Benutzer-Zertifikat heißt:
`\Programme\NCP Secure CE Client\Certs`

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 Monitor der PC-Komponente gewählt wird (siehe → Client Monitor der PC-Komponente, Konfiguration)

2.5 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. Das Telefonbuch wird 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 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, ist das Telefonbuch des Clients erhalten geblieben, so dass es für neuere Versionen des Secure CE Clients genutzt werden kann. Um die Datei vollständig vom PC zu löschen, müssen Sie per Hand vorgehen. Das Telefonbuch befindet sich im Verzeichnis:

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

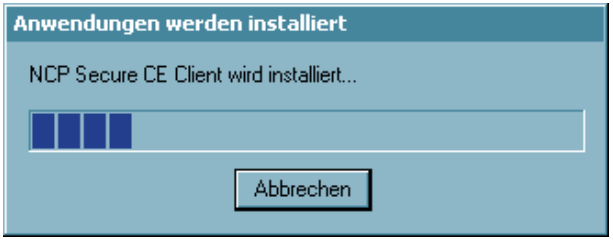
2.6 Installation der PDA-Komponente

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 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”.



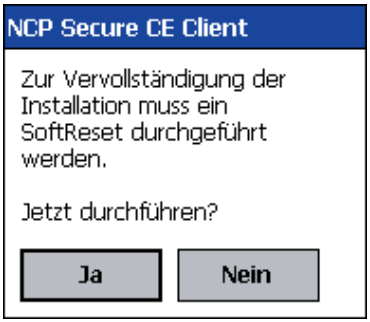
Anschließend werden die Daten für den NCP Secure CE Client übertragen.

(Windows Mobile 5.0 merkt an, dass die Software nicht signiert ist.)

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

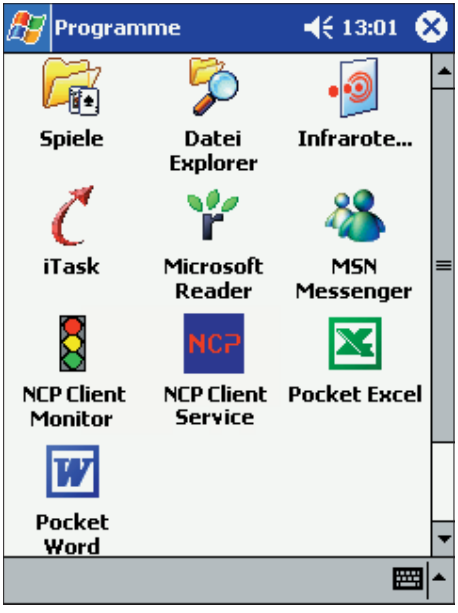
Auf dem PDA erfolgt die Installation mit dem Entpacken der übertragenen Daten.

→ *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 Service gestartet worden sein! Siehe → “Eine Verbindung herstellen” und “PDA-Monitor”.)

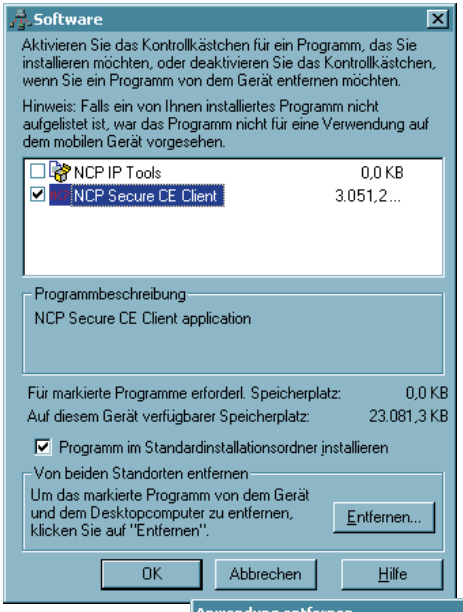
Bevor eine Verbindung aufgebaut werden kann, muss zunächst noch das Telefonbuch mit den konfigurierten Zielsystemen und gegebenenfalls die Zertifikats-Daten auf den PDA übertragen werden!

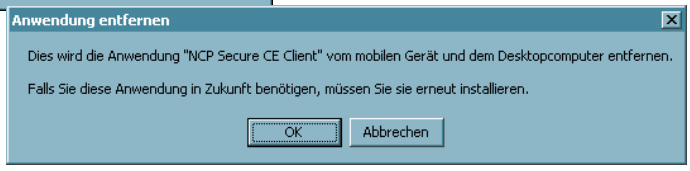
→
2.4 Übertragen des Telefonbuchs und der Zertifikate

2.8 Deinstallation der PDA-Komponente

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

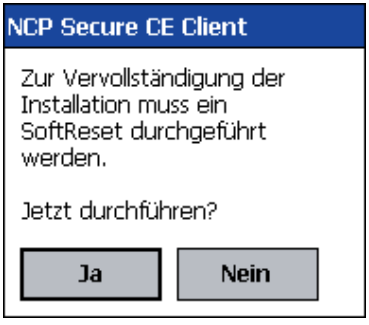
2.8.1 Deinstallation vom PC aus





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.



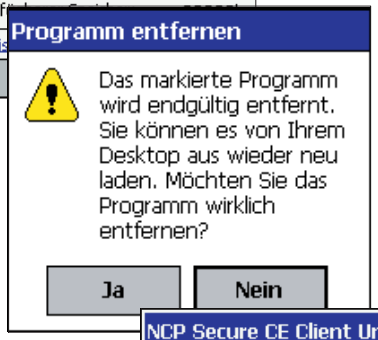
Am PDA erscheint kurzzeitig nebenstehende Meldung und anschließend die Aufforderung zu einem Soft-Reset.

Klicken Sie OK und führen Sie einen Soft-Reset durch!

Das Telefonbuch wird automatisch gelöscht. Sollten noch Zertifikate auf dem PDA vorhanden sein, so müssen diese per Hand entfernt werden. Damit ist die Deinstallation beendet.

2.8.2 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 ...

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

Klicken Sie OK, führen Sie einen Soft-Reset durch

Das Telefonbuch wird automatisch gelöscht. Sollten noch Zertifikate auf dem PDA vorhanden sein, so müssen diese per Hand entfernt werden. Damit ist die Deinstallation beendet.

2.9 Erweiterte Installation und Konfiguration

2.9.1 Autostart des NCP Client Service am PDA

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

2.9.2 Kommandozeilen-Optionen von ncpmon.exe

Der NCP Monitor am PDA versteht u. a. folgende Kommandozeilen-Optionen:

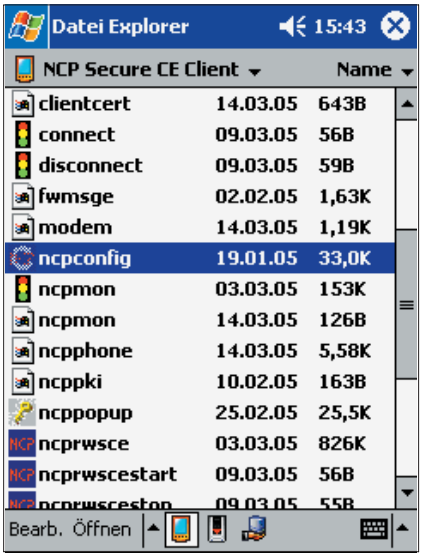
`-l license_key serialnumber`
Danach können die Lizenz-Codes eingegeben werden. Dabei wird der Lizenzschlüssel mit 20 Stellen ohne "-" als Trennung zwischen den Vierergruppen eingegeben. Die Seriennummer muss 8-stellig eingegeben werden.
`-hide`
Damit kann die Oberfläche des Monitors versteckt werden. Der Monitor ist damit nicht geschlossen, sodass weiterhin PIN- und Passwort-Abfeagen stattfinden können.
`-minimized`
Damit wird der Monitor minimiert gestartet, sodass weiterhin PIN- und Passwort-Abfeagen stattfinden können.
`-start`
Mit diesem Kommando kann eine Verknüpfung im (anzulegenden) Autostart-Verzeichnis angelegt werden, sodass der NCP Client Service und der NCP Client Monitor automatisch gestartet werden (ncpmon start minimized.lnk wird mit ausgeliefert), ggf. auch minimiert mit:
`-minimized\-start\`

2.9.3 Kaltstart-Installation

Mit einem eigenen Programm (Admin Pack) kann eine Neuinstallation inklusive des Telefonbuchs ohne PC vorgenommen werden. Dazu wird die Software im Flash-ROM des Geräts oder auf Flashcard hinterlegt. Nach einem Kaltstart wird sie dann automatisch installiert. Damit gleichzeitig Telefonbuch und Lizenzierung übernommen werden können, werden drei Dateien benötigt:
– die CAB-Datei der Software vom PC
– ein Installationsprogramm (Admin Pack) mit Anleitung
– ein Konfigurationsprogramm (Script)
Das Installationsprogramm wird durch die Autostart-Mechanismen des Systems gestartet. Im Konfigurationsprogramm ist angegeben um welche Software es sich handelt (Enterprise), ob und wo ein Telefonbuch vorhanden ist, sowie Informationen über die Lizenz. Zudem ist vermerkt, ob weitere Einstellungen vor bzw. nach der Installation in der Registry vorgenommen werden sollen. Das Admin Pack ist nicht Bestandteil der Software und nur auf Nachfrage direkt bei NCP erhältlich.

2.10 Konfigurationsprogramm NCPCONFIG am PDA

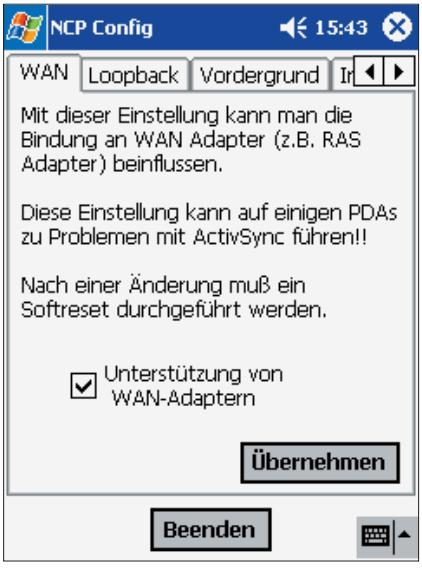
Die Basiskonfiguration erfolgt über die Profil-Einstellungen am Configurator der PC-Komponente. Am PDA können jedoch darüber hinaus weitere Einstellungen vorgenommen werden, die gerätespezifisch von Bedeutung sind. Dafür steht das Konfigurationsprogramm NCPCONFIG.EXE und ein Popup-Menü in der Monitor-Oberfläche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



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.

2.10.1 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.

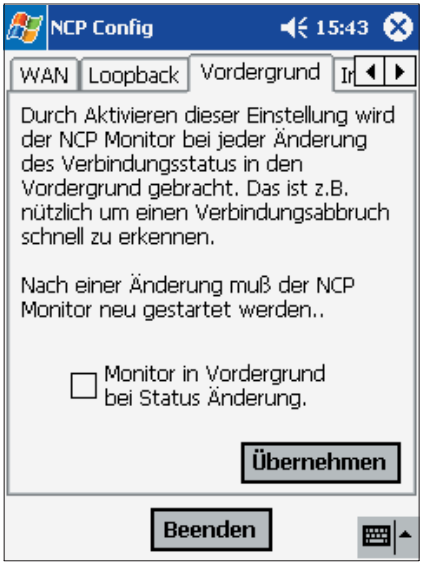
Ist dies nicht der Fall, so funktioniert der WAN-Support nicht und muss mit NCPCONFIG.EXE abgeschaltet werden. Nach einem erneuten Softreset sollte ActiveSync wieder funktionsfähig sein. NCP empfiehlt den WAN-Support nur dann zu deaktivieren, wenn Probleme auftreten.

2.10.2 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 allen neueren Geräten (PocketPC 2003 Phone Edition und neuer) zu empfehlen.

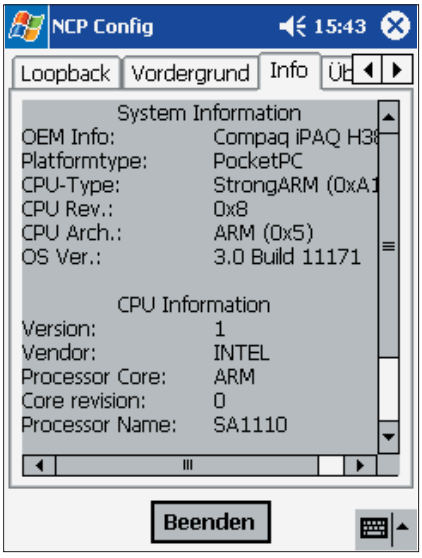
2.10.3 Vordergrund



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.

2.10.4 Info



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

2.10.5 Über

In diesem Feld werden Informationen zum Konfigurationsprogramm NCPCONFIG gezeigt.

2.11 Monitor-Oberfläche und Symbole

Im grafischen Feld des Monitors werden folgende Statusanzegen und Symbole je nach Konfiguration von links nach rechts dargestellt:

- **Endpoint Policy**

  Werden zwischen Client und VPN Gateway Endpunkt-Sicherheitsrichtlinien eingesetzt, so wird bei einem Verbindungsaufbau das Policy-Symbol dargestellt. Während der Prüfung der Policy, nachdem die Verbindung aufgebaut wurde, erscheint es mit gelben Haken, wenn die Richtlinien erfüllt werden mit grünen Haken, wenn die Richtlinien nicht erfüllt werden mit roten Haken, wonach die Verbindung zum Gateway wieder abgebaut wird.

- **Chipkarte**

  Wurde ein Chipkartenleser installiert, so wird das Symbol einer Chipkarte dargestellt. Es erscheint hellblau wenn der Chipkartenleser konfiguriert wurde, aber die Chipkarte nicht gesteckt ist, grün wenn die Chipkarte gesteckt und erkannt wurde. (Mit einem Tap-and-Hold über dem Symbol öffnet sich das Popup-Menü mit PIN-Dialog; siehe weiter unten “Popup-Menüs des Monitors”.)

- **PIN-Status**

  Die korrekte PIN-Eingabe wird immer mit einem grünen Haken versehen. Falsche PIN-Eingaben werden mit Fehlermeldungen quittiert. Der grüne PIN-Haken zeigt an, dass die eingegebene PIN gültig ist, auch wenn keine Verbindung aufgebaut ist. (Mit einem Tap-and-Hold über dem Symbol öffnet sich das Popup-Menü mit PIN-Dialog; siehe weiter unten “Popup-Menüs des Monitors”.)

- **Firewall**

  Das Firewall-Symbol ist immer dann sichtbar, wenn eine Firewall aktiviert ist. Ist die globale Firewall (Personal Firewall) mit definierten Regeln aktiv und die link-spezifische Firewall nicht aktiv, so wird das Symbol ohne Pfeile dargestellt. Bei aktivierter Link Firewall wird das Symbol mit Pfeilen dargestellt, gleich ob die globale Firewall aktiv oder inaktiv ist.

Wird die Link Firewall im Telefonbuch “immer” aktiv geschaltet und wird konfiguriert, dass eine Kommunikation ausschließlich im Tunnel zugelassen wird, so wird das Firewall-Symbol mit zwei roten Pfeilen dargestellt. Wird die Option “Ausschließlich Kommunikation im Tunnel zulassen” ausgeschaltet, so wird das Symbol mit einem grünen und einem roten Pfeil dargestellt. Wird Stateful Inspection nur für bestehende Verbindungen aktiviert, so erscheinen die Symbole nur nach dem Verbindungsaufbau.

Friendly Net Detection

Wurde vom Administrator ein Friendly Net (z.B. Firmennetz) festgelegt, und greift der Secure Client darauf zu, so färbtsich das Firewall-Symbol grün. Die Friendly Net Detection wird im Monitor-Konfigurationsmenü unter “Firewall-Einstellungen / Bekannte Netze” vorgenommen, entweder indem statische Netzwerk-Routen angegeben werden, oder indem die automatische Erkennung der bekannten Netze aktiviert wird. Siehe dazu die Beschreibung unter “Firewall-Einstellungen / Bekannte Netze”.

EAP-Status

Eine erweiterte Authentisierung mit MD5 oder TLS vor dem Tunnelaufbau wird mit “EAP” symbolisiert. Die Farbe Gelb symbolisiert die EAP-Verhandlungsphase, Grün die erfolgreiche Authentisierung mit EAP, Rot eine fehlgeschlagene Authentisierung. Bei erfolgreicher Authentisierung gegenüber einer Netzwerkkomponente, gibt die Gegenstelle zurück, welches Protokoll (MD5 oder TLS) verwendet wurde. (Mit einem Tap-and-Hold über dem Symbol öffnet sich ein kleines Popup-Menü; siehe weiter unten “Popup-Menüs des Monitors”.)

Erweiterte Authentisierung kann im Telefonbuch (für LAN- oder WLAN-Verbindungen) unter “Authentisierung vor VPN” konfiguriert werden. Wird EAP-Authentisierung gewählt, so muss im Configurator-Menü unter “Konfiguration / EAP-Optionen” das EAP für LAN aktiviert werden, sowie Benutzername und Passwort eingegeben werden. Erst dann ist das EAP-Symbol sichtbar.

Symbole des Verbindungsaufbaus

Die Symbole des Verbindungsaufbaus erscheinen bei erfolgreicher Abhandlung in grün. Sie bedeuten von links nach rechts: Einwahl ins Internet, Authentisierung beim ISP, Entschlüsselung am Gateway (wenn Verschlüsselung konfiguriert wurde), Kompression (wenn sie konfiguriert wurde). Die Verbindung wurde erfolgreich aufgebaut, wenn der Balken von gelb zu grün gewechselt hat.

Vergleiche dazu auch das Kapitel “Eine Verbindung herstellen”.

2.12 Popup-Menüs des Monitors

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

Bitte beachten Sie im folgenden:
Auf der HandheldPC-Platform (und auch bei Platformbuilder-WinCE-Versionen) ist zur Auswahl in List-Boxen immer ein Doppelklick nötig! Die Möglichkeit der Auswahl mit einfachem Klick ist von Microsoft nur für die PocketPC-Platform implementiert.)

Nebenstehende Menüpunkte können je nach Bedarf auch während einer stehenden Verbindung angewählt werden.

Bitte beachten Sie jedoch, dass bei Konfigurationsänderungen, die auch gespeichert werden (unter den Menüpunkten “WLAN-Manager” und “ActiveSync erlauben”), die Einstellungen am PDA gegenüber denen, die mit dem Telefonbuch des Configurators vorgegeben wurden, verändert werden. Soll ein Gleichstand der Konfigurationen wieder hergestellt werden, muss in diesem Fall zunächst ein Upload oder Download des Telefonbuchs über ActiveSync erfolgen.

Außerdem ist zu beachten, dass beim Speichern von Konfigurationsänderungen während einer bestehenden Verbindung, die Verbindung abbrechen kann.

2.12.1 Lizenzierung

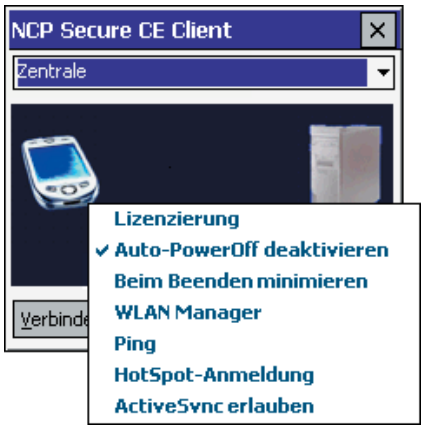
Selektieren Sie den Menüpunkt “Lizenzierung”, so öffnet sich nebenstehendes Fenster, worin die installierte und gegebenenfalls lizenzierte Software-Version angezeigt wird.

Handelt es sich bei der Software noch nicht um eine Voll-Version und soll die Test-Version lizenziert werden, so kann über den Button “Pfeil nach rechts” das Eingabefenster für die Lizenz-Codes geöffnet werden.

Nach Eingabe von Lizenz-Schlüssel und Seriennummer tippen Sie auf den Button “Pfeil nach rechts”. Damit werden die Codes gespeichert und die Software zur Voll-Version freigeschaltet. Ein Tippen auf die Pfeiltaste nach links verwirft die eingegebenen Codes und führt zum oberen Fenster zurück.

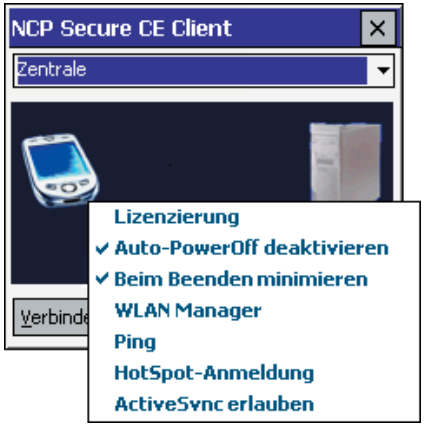
Nach korrekter Eingabe der Codes erscheinen die Lizenzierungsdaten wie in nebenstehendem Bild.

2.12.2 Auto-PowerOff



Standardmäßig ist die Auto-PowerOff-Funktion deaktiviert wie in nebenstehender Abbildung, d. h. der PDA versetzt sich nicht automatisch in den Stromsparmodus, wenn eine VPN-Verbindung steht.

2.12.3 Beim Beenden minimieren



Normalerweise wird der Monitor mit dem Button [x] rechts oben beendet, d. h. geschlossen. ird die Funktion “Beim Beenden minimieren” aktiviert, so wird der Monitor mit einem Tipp auf den [x]-Button nicht beendet, sondern nur verkleinert und in der Taskleiste als Icon dargestellt.

Der Monitor kann nur dann über den [x]-Button beendet werden, wenn die Funktion “Beim Beenden minimieren” deaktiviert ist.

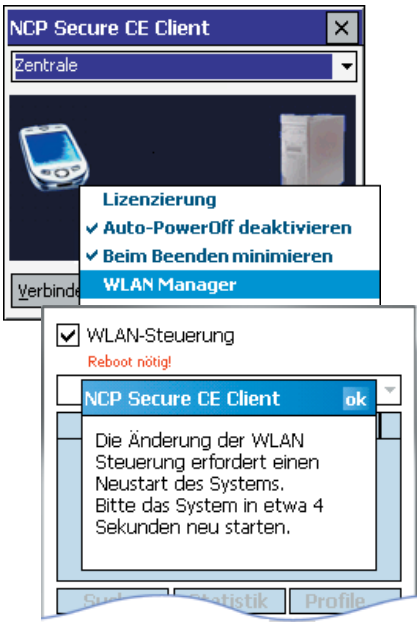
2.12.4 WLAN Manager (Konfiguration)

Die Konfigurationsmöglichkeiten des WLAN-Managers entsprechen denen, die über das Configurator-Menü “Konfiguration / WLAN-Einstellungen” ausgeführt werden können. Beachten Sie dazu die Beschreibung zum Configurator-Menü unter “Konfiguration / WLAN-Einstellungen”.

Soll ein Gleichstand der Konfigurationen von PDA und Confiurator am PC wieder hergestellt werden, so muss ein Upload oder Download des Telefonbuchs über ActiveSync erfolgen.

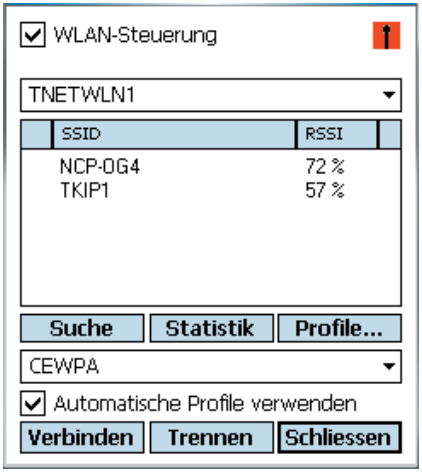
Ab Windows Mobile 2003 kann der WLAN-Adapter mit der Verbindungsart “WLAN” betrieben werden. Die Konfiguration, worin die Zugangsdaten zum Funknetz festgelegt werden, kann alternativ über den Configurator oder den WLAN-Managers am PDA erfolgen.

WLAN-Manager



Im folgenden ist die WLAN-Steuerung mit dem WLAN-Manager und auf den nächsten Seiten die Konfiguration mit dem Profil-Manager des PDAs kurz beschrieben.

Wird die WLAN-Steuerung aktiviert, so muss das Management-Tool bzw. das Microsoft-Tool der WLAN-Karte deaktiviert werden. Dies erfolgt über einen Soft-Reset oder über einen Neustart der WLAN-Karte. (Die jeweils nicht eingesetzten Tools müssen deaktiviert werden.)



WLAN-Steuerung / Übersichtsfenster

Unter der aktivierten WLAN-Steuerung wird der vom System gefundene WLAN-Adapter angezeigt (hier: TNETWLN1). Darunter werden die aktuellen WLAN-Netze mit SS-ID und Feldstärke (RSSI) angezeigt.

Mit dem [Suche]-Button wird der Scan nach WLANs angestoßen. Ein Statistikfenster zeigt den Status der Verbindung zum Access Point. Der [Profile]-Button öffnet den Profil-Manager zur Konfiguration der WLAN-Profile (siehe nächste Seite oben). Über den Auswahl-Button kann das gewünschte Profil selektiert werden.

Die Verbindung wird mit den entsprechenden Buttons aufgebaut und beendet. [Schließen] beendet das Menü des WLAN-Managers.

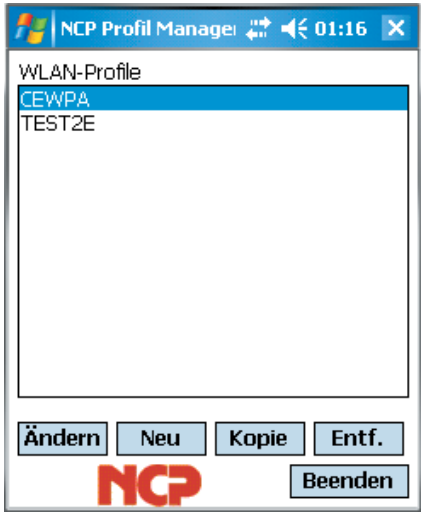
“Automatische Profile verwenden” bedeutet, dass für den Verbindungsaufbau Profile mit automatischer Verbindungsart verwendet” werden. Sie kann für jedes Profil einzeln in der WLAN-Konfiguration unter “Allgemein” eingestellt werden (siehe nächste Seite).

Profil-Manager

Der [Profile]-Button des WLAN-Managers (siehe Seite vorher) öffnet den Profil-Manager zur Konfiguration der WLAN-Profile.

Bitte beachten Sie: Wenn Sie den Profil-Manager über den [x]-Button rechts oben schließen, wird er nur minimiert, nicht beendet! Nur wenn er mit dem [Beenden]-Button beendet wurde, wird er als Task beendet und eine Verbindung mit dem gewünschten Profil kann hergestellt werden.

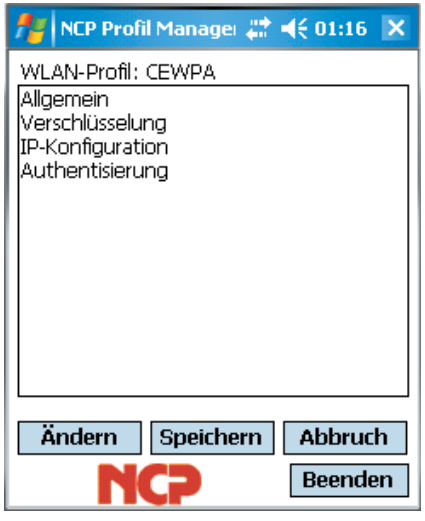
Nur im Fenster mit der Liste der Konfigurationsrubriken (Bild unten auf dieser Seite) kann mit dem [Speichern]-Button die Einstellung für ein Profil gespeichert werden.



WLAN-Profile / Auswahl

Zur Konfiguration wird ein WLAN-Profil mit dem Button [Neu] erstellt oder mit den Buttons [Ändern] oder [Kopie] selektiert. Mit einem Tipp auf diese Buttons gelangen Sie in das nächste Konfigurationsfeld, in dem die vier Parameterfelder für das WLAN-Profil gelistet sind. Der Button [Entf.] löscht ein Profil.

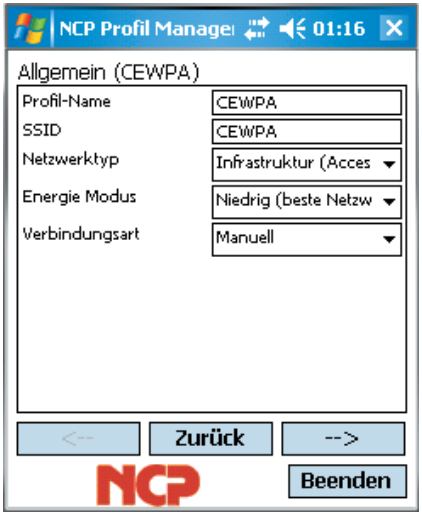
Der Button [Beenden] beendet immer die Konfiguration im jeweiligen Parameterfeld und Führt ohne zu speichern zum Übersichtsfenster zurück.



WLAN-Profil / Konfigurationsrubriken

Unter dem angezeigten Profil-Namen werden in diesem Fenster die vier Konfigurationsrubriken aufgeführt. Nach Auswahl einer Rubrik und Tipp auf [Ändern] wird das selektierte Parameterfeld geöffnet. [Abbruch] führt auf die höhere Ebene (WLAN-Profile / Auswahl) zurück.

Nur mit diesem [Speichern]-Button können die Einstellungen in den Konfigurationsrubriken (der folgenden Fenster) gespeichert werden.



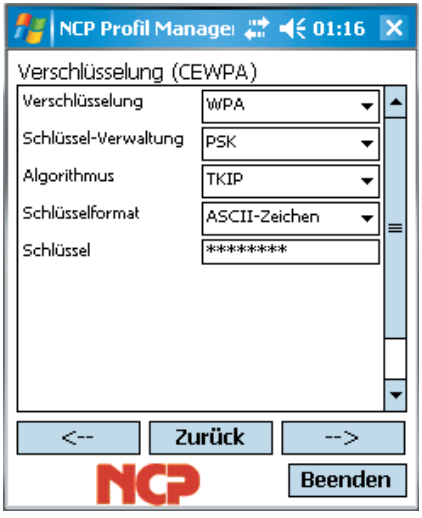
WLAN-Konfiguration / Allgemein

Mit den Pfeil-Buttons gelangen Sie in eine benachbarte Konfigurationsrubrik, mit [Zurück] gelangen sie in das Rubrikenfenster.

Der Name kann frei vergeben werden und muss eindeutig sein. Der Netzwerktyp muss mit dem des Funknetzes identisch sein. Der Netzwerktyp muss dann manuell umgestellt werden auf “Ad-Hoc”, wenn ein Profil für eine Direktverbindung von PDA zu PDA hergestellt werden soll. Sofern der WLAN- Adapter dies gestattet, kann der Energie-Modus für ihn ausgewählt werden. Mit der Verbindungsart kann angegeben werden, ob über dieses Profil die Verbindung zum Access Point automatisch aufgebaut wird oder manuell. Wird “automatisch” eingestellt, so kann dieses und andere mit “automatisch” konfigurierte Profile für die WLAN-Automatik verwendet werden.

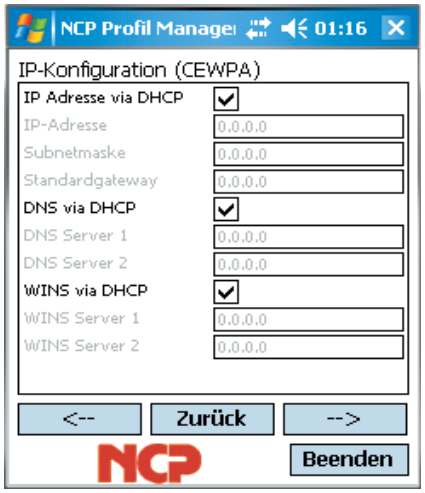
WLAN-Automatik

Im Übersichtsfenster kann konfiguriert werden, dass “Für den Verbindungsaufbau Profile mit automatischer Verbindungsart verwendet” werden. Anschließend kann in der WLAN-Konfiguration unter “Allgemein” für die gewünschten Profile die automatische Verbindungsart gesetzt werden. Alle diese Profile gelangen dann automatisch zum Einsatz, wenn eine Verbindung zum Access Point hergestellt werden soll. D. h. zunächst wird das zuletzt selektierte Profil für einen möglichen Verbindungsaufbau herangezogen. Ist die SSID nicht passend, sodass mit diesem Profil keine Verbindung zum Access Point hergestellt werden kann, so werden anschließend die als “automatisch” konfigurierten Profile abgearbeitet und das erste mit der passenden SSID verwendet.



WLAN-Konfiguration / Verschlüsselung

Der Verschlüsselungsmechanismus wird vom Access Point (WLAN Router) vorgegeben und über den Administrator mitgeteilt.



WLAN-Konfiguration / IP-Konfiguration

In diesem Fenster wird die IP-Adress-Konfiguration der WLAN-Karte vorgenommen.

Die hier gemachten Einstellungen werden dann wirksam, wenn die WLAN-Konfiguration wie oben beschrieben aktiviert wurde. In diesem Fall wird die hier eingetragene Konfiguration in die Microsoft-Konfiguration der Netzwerkverbindungen übernommen.

Authentisierung

In diesem Fenster können die Zugangsdaten für eine automatische Anmeldung am HotSpot eingetragen werden. Diese Benutzerdaten werden nur für dieses WLAN-Profil verwendet.

Konfiguration speichern

Klicken sie nach der Konfiguration einer der Rubriken auf den [Beenden]-Button, so erscheint nebenstehende Warnung.

Nur im Fenster mit der Liste der Konfigurationsrubriken kann mit dem [Speichern]-Button die Einstellung für ein Profil gespeichert werden. Tippen Sie daher zunächst auf den [Zurück]-Button, um in dieses Fenster zu gelangen und speichern Sie dann das Profil.

2.12.5 HotSpot-Anmeldung

Mit einem Tipp auf diesen Menüpunkt erfolgt eine automatische HotSpot-Anmeldung. Damit der remote Client in jeder Phase des Verbindungsaufbaus auch in WLANs mit Hot-Spots 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.

Nachdem dieser Menüpunkt angeklickt wurde, können verschiedene Verbindungsmeldungen am Bildschirm erscheinen:

– Wenn sich der Benutzer bereits im Internet befindet, wird er mit der Startseite http://www.ncp.de verbunden. Es erscheint ein Fenster mit folgender Meldung: “Sie befinden sich bereits im Internet. Eine Anmeldung am HotSpot ist nicht notwendig oder wurde bereits durchgeführt.” Dieser Text kann vom Administrator ausgetauscht werden, indem die Adresse einer anderen HTML-Startseite in der Form angegeben wird “http://www.mycompagnie.de/error.html” und der Text von error.html entsprechend geändert wird.
– Wenn der Benutzer noch nicht angemeldet ist, erscheint ein Fenster mit der Aufforderung Benutzername und Passwort für die Anmeldung am HotSpot-Betreiber einzugeben.
– Wenn der Benutzer keine Website erreicht, erscheint die Microsoft-Fehlermeldung “... not found”.

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).

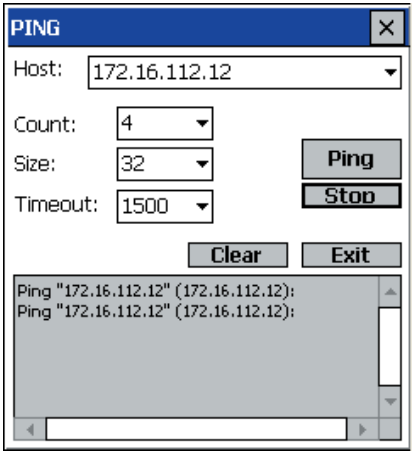
Funktionsbeschreibung

Die Konfiguration zur HotSpot-Anmeldung erfolgt im Configurator unter “Konfiguration / HotSpot”. Folgende Einstellungen sind möglich:

– “Standard-Browser für HotSpot-Anmeldung verwenden” ist die Standardeinstellung. Wird der Haken in der Checkbox entfernt, kann ein anderer Browser angegeben werden (Dieser alternative Browser ist nicht Bestandteil der Client Software!). Darüber hinaus kann der MD5-Hash-Wert der Browser-Exe-Datei ermittelt und in das Feld “MD5-Hash” eingetragen werden. Auf diese Weise wird sichergestellt, dass nur mit diesem Browser eine HotSpot-Verbindung zustande kommt.

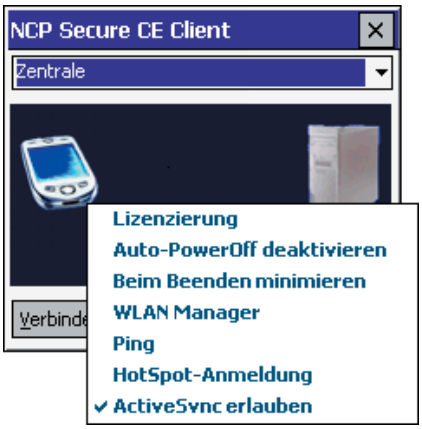
– Unter “Startseite / Adresse” wird die oben beschriebene Startseite eingegeben in der Form: http://www.mycompagnie.de/error.html.

2.12.6 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.

2.12.7 ActiveSync erlauben



Die (globale) Firewall, die im Configurator-Menü unter “Konfiguration / Firewall-Einstellungen” aktiv geschaltet wurde, muss bei einer Direktverbindung (über USB, seriell oder Infrarot) für ActiveSync freigeschaltet werden. Dies erfolgt in den Firewall-Einstellungen am Configurator unter “Optionen / ActiveSync-Verbindungen 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), muss zusätzlich manuell eine eigene Firewall-Regel für die Namensauflösung (DNS/WINS) erstellt werden.

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

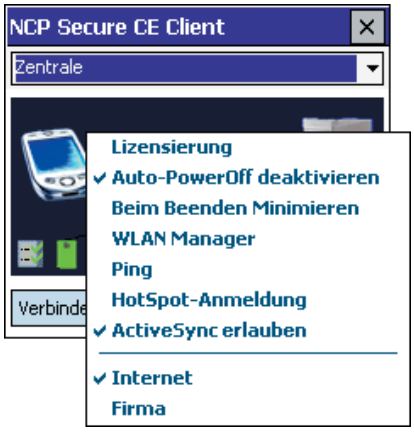
Diese globale Definition erspart die Einrichtung dezidierter Einzelregeln für die jeweilige VPN-Variante.

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.

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.

2.12.8 PocketPC Connection Manager



In den Profil-Einstellungen des Telefonbuchs 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.

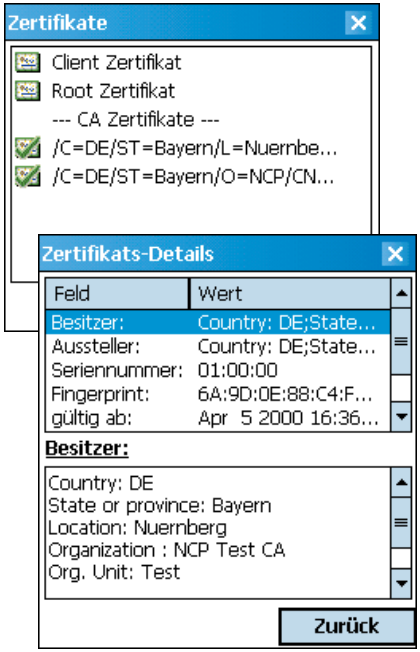
2.12.9 EAP

Mit einem Tap-and-Hold über dem EAP-Symbol öffnet sich ein kleines Popup-Menü: Mit “EAP verhandeln” kann das EAP zurückgesetzt werden. Unmittelbar anschließend erfolgt automatisch eine erneute EAP-Verhandlung. Bei erfolgreicher Authentisierung gegenüber einer Netzwerkkomponente, gibt die Gegenstelle zurück, welches Protokoll (MD5 oder TLS) verwendet wurde. Mit “EAP beenden” wird in EAP-Logoff gesendet. Um die EAP-Verhandlung wieder anzustoßen, muss erneut “EAP verhandeln” geklickt werden.

Erweiterte Authentisierung kann im Telefonbuch (für LAN- oder WLAN-Verbindungen) unter “Authentisierung vor VPN” konfiguriert werden. Wird EAP-Authentisierung gewählt, so muss im Configurator-Menü unter “Konfiguration / EAP-Optionen” das EAP für LAN aktiviert werden, sowie Benutzername und Passwort eingegeben werden. Erst dann ist das EAP-Symbol sichtbar.

2.12.10 Zertifikate

Mit einem Tap-and-Hold über dem PIN- oder Smart Card-Symbol öffnet sich das Popup-Menü zum Zertifikats-Informations-Dialog.



Zertifikats-Info

zeigt die verwendeten CA- und Benutzer-Zertifikate an.

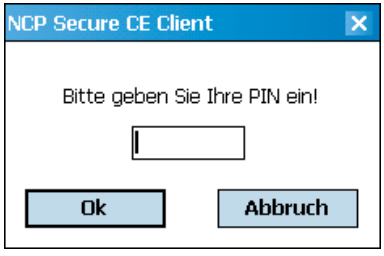
Zertifikats-Details

Ein weiterer Tipp auf das gewünschte Zertifikat zeigt dessen Inhalte (links) an.

PIN ändern

Unter dem Menüpunkt “PIN ändern” kann nur bei Verwendung einer Smart Card deren PIN geändert werden, wenn vorher die bisherige PIN eingegeben wurde. Ohne die vorherige Eingabe einer gültigen PIN wird dieser Menüpunkt nicht aktiv.

PIN eingeben



Die PIN-Eingabe kann bereits vor einem Verbindungsaufbau erfolgen. Wird dann zu einem späteren Zeitpunkt eine Verbindung aufgebaut, die ein Zertifikat erfordert, so kann die PIN-Eingabe unterbleiben, es sei denn in der Zertifikats-Konfiguration des Configurators wurde die Funktion “PIN-Abfrage nach jedem Verbindungsaufbau” eingeschaltet.

Der PIN-Dialog erscheint immer dann, wenn eine Verbindung aufgebaut werden soll, für die ein Zertifikat benötigt wird, dessen PIN noch nicht eingegeben wurde. Bei einem wiederholten manuellen Verbindungsaufbau kann die PIN-Eingabe unterbleiben.

Wird ein Soft-Zertifikat verwendet, muss die PIN mindestens 4-stellig sein, bei einer Chipkarte mindestens 6-stellig. Fehlerhafte Eingaben werden nach ca. 3 Sekunden mit einer Fehlermeldung quittiert. Ein Verbindungsaufbau ist dann nicht möglich.

Nach dreimaliger Falscheingabe (kann je nach Chipkarte variieren) wird die PIN gesperrt! Wenden Sie sich in diesem Fall an Ihren Administrator. Wenn die Chipkarte während des laufenden Betriebs entfernt wird, findet ein Verbindungsabbau statt, sofern dies nicht anders in der Zertifikats-Konfiguration des Configurators eingestellt wurde (siehe →Kein Verbindungsabbau nah gezogener Chipkarte).

PIN zurücksetzen

Dieser Menüpunkt kann gewählt werden, um die PIN zu löschen, d. h. um die aktuell gültige PIN für einen anderen Benutzer unbrauchbar zu machen. Dies kann dann sinnvoll sein, wenn der PDA vorübergehend aus der Hand gelegt wird oder wenn der Benutzer gewechselt wird. Danach muss erneut eine gültige PIN eingegeben werden, um eine Authentisierung durchführen zu können.

Bei einem Standby des PDAs wird die PIN aus Sichrheitsgründen automatisch zurückgesetzt.

ReInit PKI-Modul

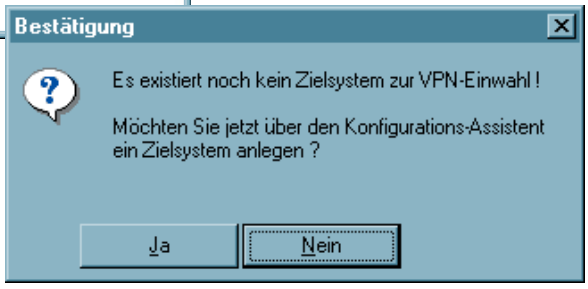
Bei einer fehlerhaften Verbindung zum Chipkartenleser kann mit dieser Funktion eine erneute Initialisierung angestoßen werden.

Diese Seite ist frei →

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 Enterprise 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 “4.2.1 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 Telefonbuch-Einstellungen auf das PDA-Gerät.

☑ das Herunterladen der Telefonbuch-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,

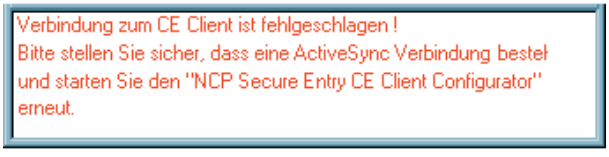
- einer Buttonleiste für “Upload” und “Download” des Telefonbuchs

- der Zielauswahl für bereits erstellte Zielsysteme,

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

- und 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.

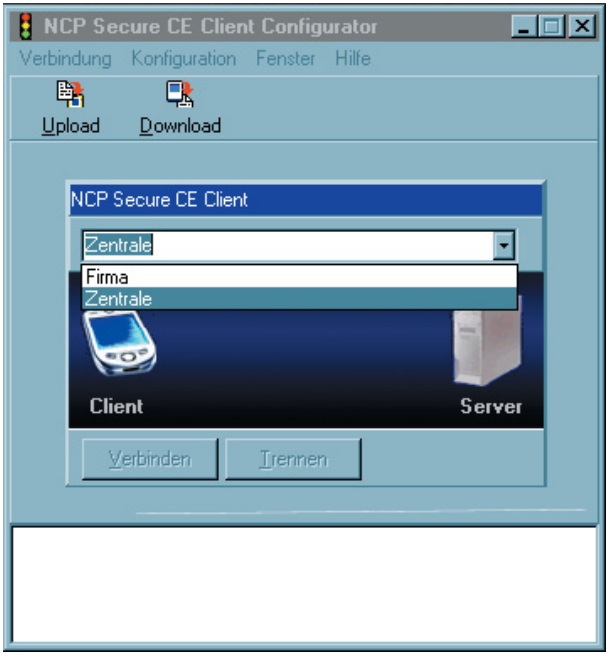


rote Meldungen: Fehler und missglückte Verbindungen
grüne Meldungen: OK-Meldungen bei Upload von Profil-Einstellung und Zertifikat
blaue Meldungen: Hinweise und Warnungen wegen inkompatibler Profile (WAN Support, virtueller Adapter am PDA - Upload auf den PDA)

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

3.1.1 Die Benutzung der Configurators

Sobald die Software installiert und eine Testverbindung korrekt konfiguriert wurde (siehe oben → Erstellen von Testverbindungen), kann dieses Zielsystem zu einer weiteren Modifikation ausgewählt werden (siehe →Telefonbuch / Konfigurationsparameter).



Das gewünschte Zielsystem wird über die Auswahl-Box unter dem Hauptmenü aus einer Liste gewählt (siehe nebenstehendes Bild).

Wurde noch kein Zielsystem angelegt, so fahren Sie mit Abschnitt “Konfiguration - Telefonbuch” weiter unten in diesem Kapitel fort.

4. Das Configurator-Menü

Die Beschreibung folgt den Menüpunkten in der Menüleiste.

Die Hauptmenüpunkte in der Menüleiste von links nach rechts sind:

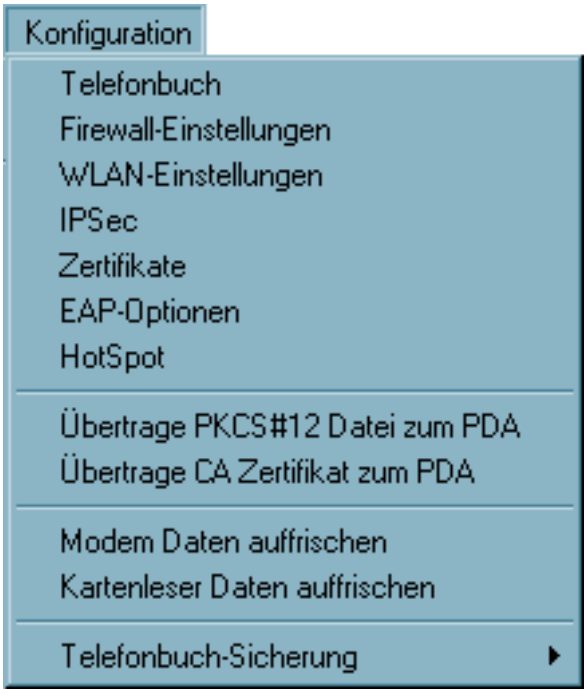
- ☐ Verbindung |Menü
- ☐ Konfiguration |Menü
- ☐ Fenster |Menü
- ☐ Hilfe |Menü

4.1 Verbindung

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

Die Kommandos zum Aufbau und Trennen einer Verbindung sind derzeit noch ohne Funktion.

4.2 Konfiguration



Unter diesem Menüpunkt werden die Einträge für das Telefonbuch erstellt, das heißt die Zielsysteme konfiguriert. (Die Beschreibung zu den einzelnen Parametern finden Sie unter "Konfigurationsparameter / Telefonbuch").

Soll IPSec genutzt werden, so finden Sie hier den Zugang zur IPSec-Konfiguration.

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

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

4.2.1 Telefonbuch

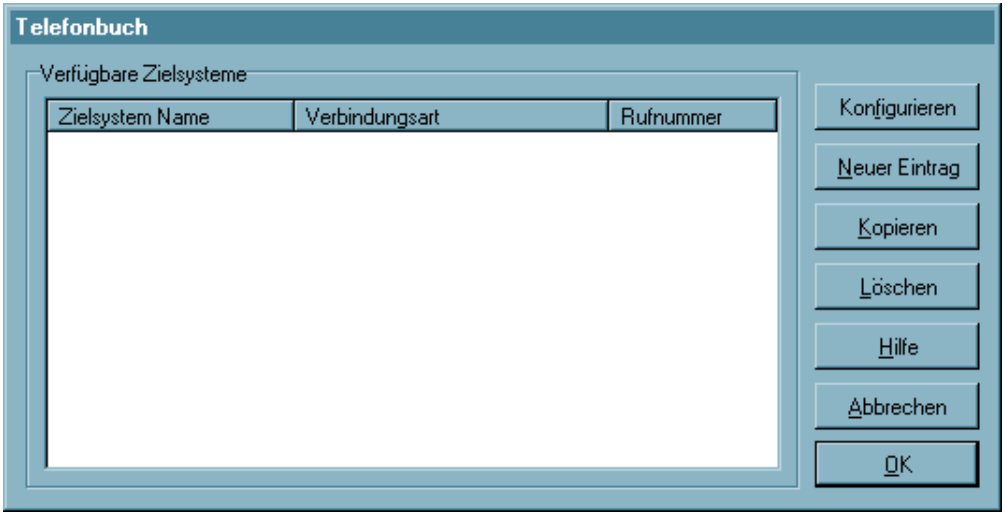
Die Einträge des Telefonbuchs

Bei einer Erstinstallation der PC-Komponente ist noch kein Telefonbuch vorhanden. Sie haben aber die Möglichkeit Testverbindungen nach den vorgegebenen Parametern (siehe → Installation, Erstellen von Testverbindungen) mit Hilfe des Konfigurations-Assistenten zu erstellen. Die Einträge zu den Testverbindungen können Sie später nach Belieben modifizieren.

Das Telefonbuch des Configurators ist besonders leistungsstark. Mit ihm können die Zielsysteme definiert und die Übertragungsart, den Benutzeranforderungen entsprechend, bis ins Detail konfiguriert werden.

Nachdem Sie auf “Telefonbuch” in der Menüleiste des Configurators geklickt haben, öffnet sich das Telefonbuch und zeigt in einer Liste der bereits verfügbaren Zielsysteme die Namen der definierten Zielsysteme und deren Rufnummern.

Ohne definiertes Zielsystem kann das PDA-Gerät keine Verbindung aufbauen. Ein Zielsystem ist definiert, wenn es als neuer Eintrag im Telefonbuch angelegt wird (siehe → Neuer Eintrag, Zielsystem).



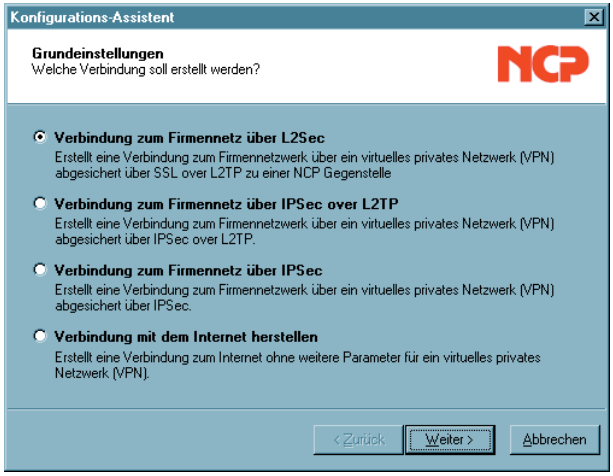
Auf der rechten Seite des Telefonbuchs sind Buttons angebracht zu folgenden Funktionen: Konfigurieren, Neuer Eintrag, Kopieren, Löschen, OK, Hilfe und Abbrechen.

Zur Konfiguration beachten Sie bitte die Beschreibung der “Konfigurationsparameter”.

Neuer Eintrag – Zielsystem (Konfigurations-Assistent)

Um ein neues Zielsystem zu definieren, klicken Sie in der Menüleiste auf “Telefonbuch”. Das Fenster des Telefonbuchs öffnet sich nun und zeigt die bereits definierten Zielsysteme.

Klicken Sie jetzt auf “Neuer Eintrag”. Jetzt legt der “Konfigurations-Assistent” mit Ihrer Hilfe ein neues Zielsystem an. Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Zielsystem angelegt. Für alle weiteren Parameterfelder des Telefonbuchs werden Standardwerte eingetragen, die Sie unter dem Menüpunkt “Konfigurieren” (siehe → Konfigurieren, Zielsystem) auch ändern können.



Mit dem Konfigurations-Assistenten können Verbindungen mit dem Internet oder, je nach erforderlichem VPN-Übertragungsprotokoll, zum Firmennetz rasch hergestellt werden. Je nach Auswahl der gewünschten Grundeinstellung wird das Zielsystem nach wenigen Konfigurationsabfragen im Telefonbuch angelegt.

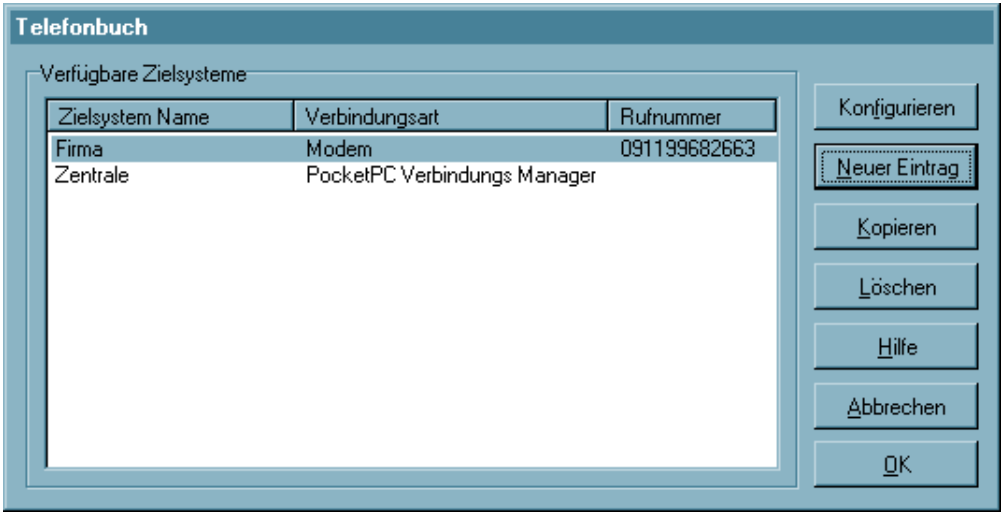
Im folgenden die jeweils nötigen Daten zur Konfiguration:

Verbindung zum Firmennetz über L2Sec:
→ Name des Zielsystems
→ Verbindungsart
→ Zugangsdaten für Internet-Dienstanbeiter (Benutzername, Kennwort, Rufnummer)
→ VPN-Gateway-Parameter (VPN-Gateway, Tunnelsecret, Kompression)
→ Nutzung von Zertifikaten
→ Zugangsdaten für VPN-Gateway (VPN-Benutzer, VPN-Passwort)
→ Statischer Schlüssel (Preshared Key) sofern kein Zertifikat eingesetzt wird

Verbindung zum Firmennetz über IPSec over L2Sec:
→ Name des Zielsystems
→ Verbindungsart
→ Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)
→ VPN-Gateway-Parameter (VPN-Gateway, Tunnelsecret)
→ Nutzung von Zertifikaten
→ Zugangsdaten für VPN-Gateway (VPN-Benutzer, VPN-Passwort)
→ Statischer Schlüssel (Preshared Key) sofern kein Zertifikat eingesetzt wird

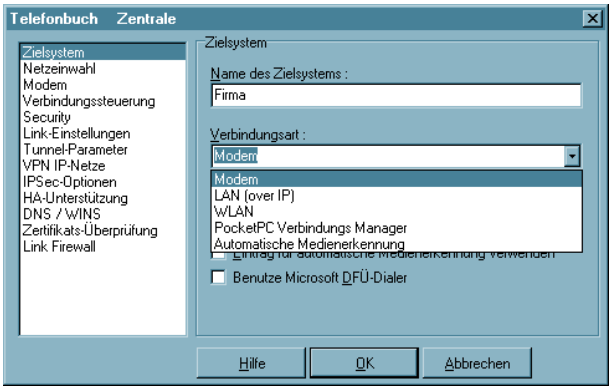
Verbindung zum Firmennetz über IPSec:
→ Name des Zielsystems
→ Verbindungsart
→ Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)
→ VPN-Gateway-Parameter (VPN-Gateway, Tunnelsecret)
→ Nutzung von Zertifikaten
→ Zugangsdaten für VPN-Gateway (VPN-Benutzer, VPN-Passwort)
→ Statischer Schlüssel (Preshared Key), ohne Zertifikat (IKE ID-Typ, IKE ID)

Verbindung mit dem Internet herstellen:
→ Name des Zielsystems
→ Verbindungsart
→ Zugangsdaten für 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 – Zielsystem



Um die (Standard-)Werte eines Zielsystems zu editieren, d. h. Parameter so abzuändern, wie es den Verbindungsanforderungen zum definierten Zielsystem entspricht, wählen Sie das Zielsystem, dessen Werte Sie ändern möchten, aus dem Telefonbuch aus und klicken anschließend auf “Konfigurieren”.

Das Telefonbuch zeigt nun in seinem linken Fenster eine Liste von Begriffen, denen jeweils ein Parameterfeld zugeordnet ist.

Je nachdem, welchen Begriff Sie markieren, zeigt sich das entsprechende Feld mit den zugehörigen Parametern (siehe → Konfigurationsparameter), oben das “Zielsystem”.

Ok – Zielsystem

Die Konfiguration eines Zielsystems ist abgeschlossen, wenn Sie das Konfigurationsfenster des Telefonbuchs mit OK schließen. Das neue oder geänderte Zielsystem ist nach einem Download auf das PDA-Gerät sofort verfügbar. Es kann über den Verbinden-Button sofort angewählt werden.

Bitte beachten Sie wenn Sie das TCP/IP-Protokoll benutzen und nicht IP Network Address Translation verwenden, dass es nötig sein kann, die Einstellungen Ihres Windows CE-Systems zu ändern (siehe → Link-Einstellungen, IP Network Address Tranlation).

Kopieren – Zielsystem

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

Ein kopiertes Zielsystem muss einen neuen, noch nicht vergebenen, Namen erhalten. Nur so kann es im Telefonbuch abgelegt werden.

Löschen – Zielsystem

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

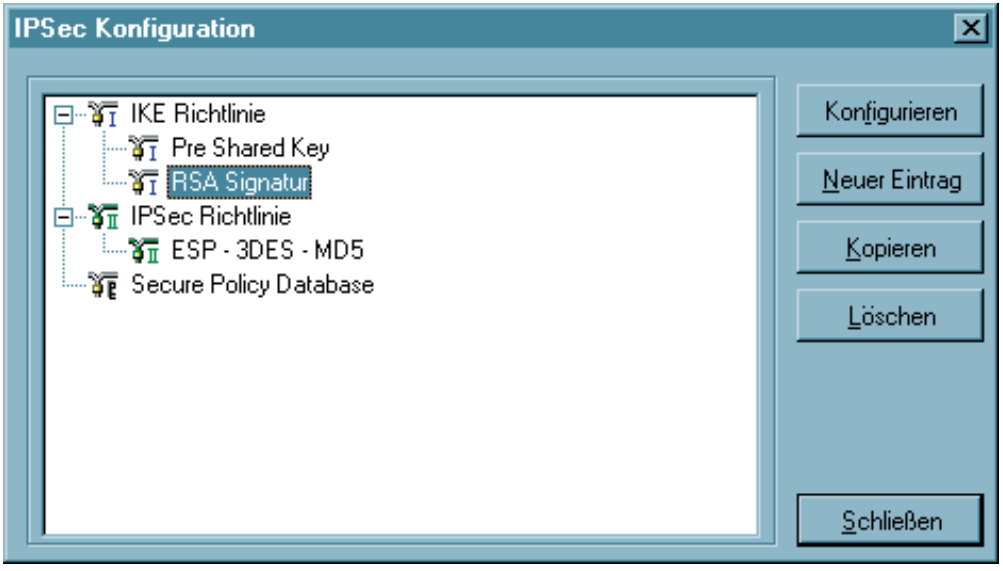
4.2.2 IPSec

■ Die Einträge der IPSec-Konfiguration

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 Konfiguratiosnfensters.

Der Secure Client wird mit vorkonfigurierten IKE-Richtlinien (Pre-shared Key / RSA-Signatur) und einer IPSec-Richtlinie (ESP-3DES-MD5) ausgeliefert.

Um die (Standard-)Werte der Richtlinien zu editieren, d.h. Parameter so einzustellen oder abzuändern, wie es den Verbindungsanforderungen zum definierten Zielsystem entspricht, wählen Sie mit der Maus die Richtlinie, deren Werte Sie ändern möchten – die Buttons zur Bedienung werden dann aktiv.



Auf der rechten Seite der IPSec Konfiguration sind Buttons angebracht zu folgenden Funktionen: Konfigurieren, Neuer Eintrag, Kopieren, Löschen, Schließen.

Zur Konfiguration beachten Sie bitte die Beschreibung der "Konfigurationsparameter"! (Siehe → Konfigurationsparameter, IPSec)

Konfigurieren – IPSec

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 – IPSec

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 – IPSec

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 – IPSec

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.

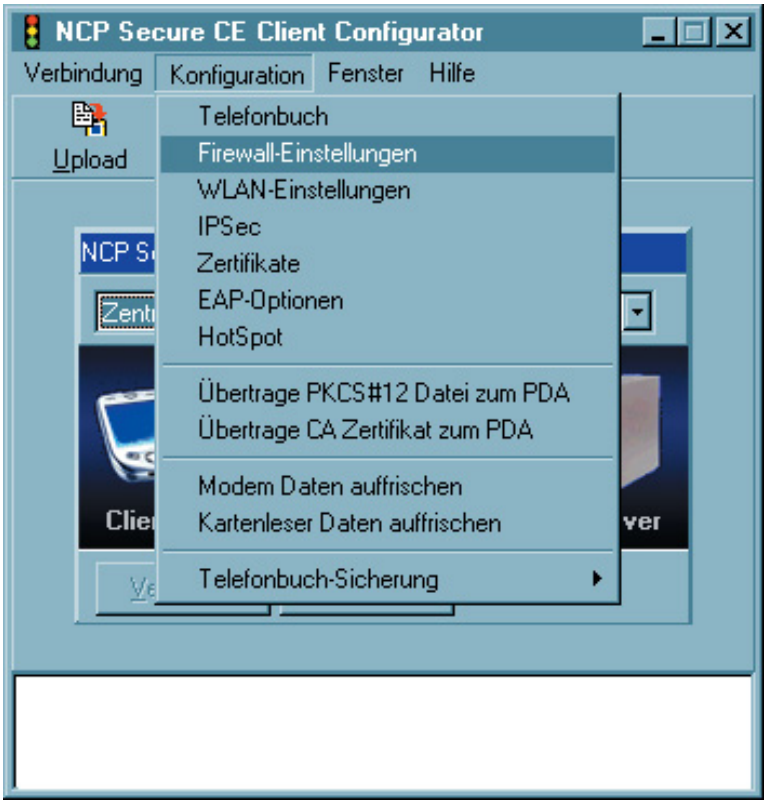
Schließen – IPSec

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

4.2.3 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.

ActiveSync mit Firewall

Unter Windows Mobile 5.0 wird eine ActiveSync-Verbindung über USB unabhängig von den Einstellungen der Firewall (sowohl der Link-Firewall als auch der erweiterten Firewall) zugelassen.

Bei aktiver Link-Firewall:

ActiveSync-Verbindungen über Bluetooth, serielle oder Infrarot-Schnittstelle etc. 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 ein Datenverkehr zugelassen. Die Verbindung wird nur dann gesperrt, wenn in der Link-Firewall “Ausschließlich Kommunikation im Tunnel zulassen” aktiviert ist.

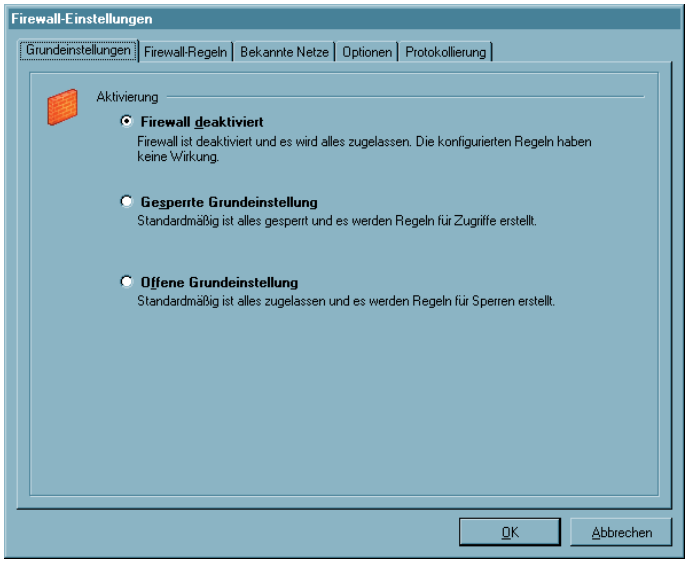
Sollte diese Konfiguration so genutzt werden, muss der Parameter “ActiveSync-Verbindungen zulassen” aktiviert sein, damit ein Verbindung über ActiveSync zustande kommt.

Bei aktiver globaler Firewall:

Die globale Firewall muss bei einer Direktverbindung (über Bluetooth, serielle oder Infrarot-Schnittstelle) für ActiveSync freigeschaltet werden. Dies erfolgt in den Firewall-Einstellungen des Configurators unter “Optionen - ActiveSync-Verbindungen zulassen”. Diese Einstellung kann auch am PDA über das Popup-Menü vorgenommen werden, wenn die 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.

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.

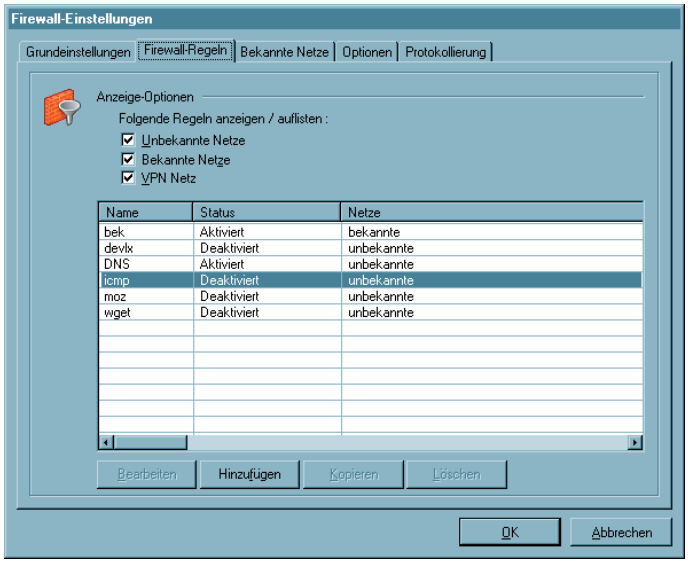
Dazu kann im Konfigurationsfeld “Optionen” der Datenverkehr über VPN-Protokolle (L2Sec, IPSec) global zugelassen werden.

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

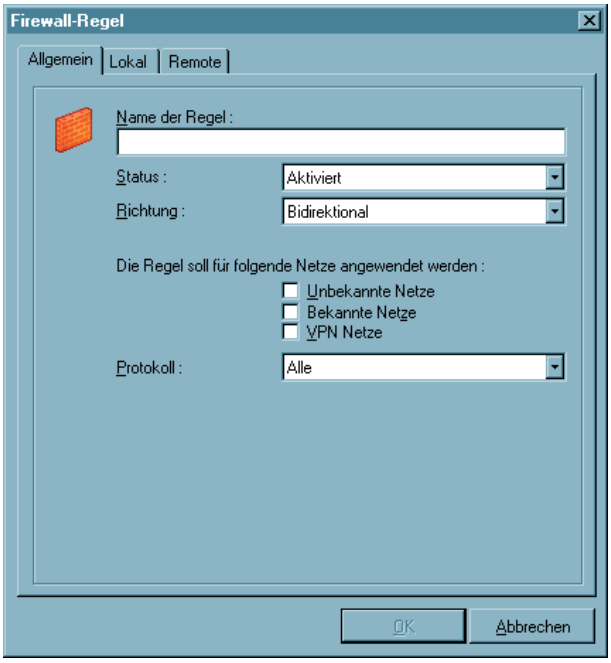
Durch Klick auf diese Eigenschafts-Buttons können die eingeblendeten Regeln sortiert werden.

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 vier 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

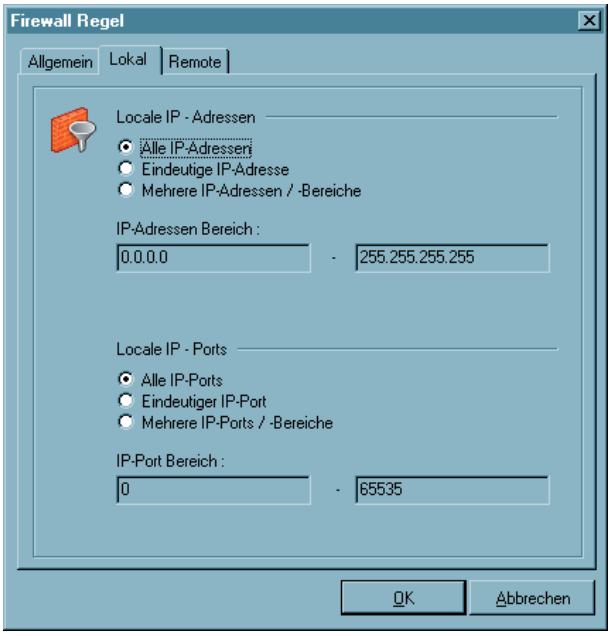
Verbindungssteuerung

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.

Bitte beachten Sie: Auf Windows CE-Geräten der PocketPC Plattform 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.

Ist der virtuelle Netzwerkadapter "NCP Loopback" deaktiviert – was bei einer Neuinstallation standardmäßig der Fall ist – so muss bei der Erzeugung einer "Filter-Regel / lokal" folgendes beachtet werden:

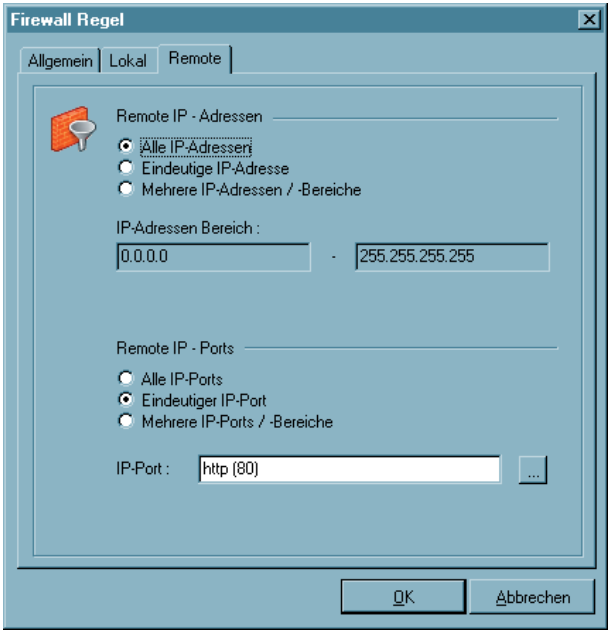
– Da die IP-Adress-Umsetzung für das VPN hinter der Firewall erfolgt, darf bei der Regelerstellung kein IP-Adress-Bereich aus dem VPN verwendet werden. Dies gilt für alle programminternen Adress-Umsetzungen, wie z. B. auch DNS-Adresse, eigene IP-Adresse usw.

– Die Firewall blockiert die Kommunikation, sofern nicht “Alle IP-Adressen”, unabhängig vom lokalen Netzwerkadapter, zugelassen werden. Eine “Eindeutige IP-Adresse” oder “Mehrere IP-Adressen” aus dem lokalen Bereich kann nur verwendet werden, wenn der Loopback-Adapter aktiviert wird. Dies erfolgt über das Konfigurationsprogramm NCPCONFIG.EXE am PDA. Das Konfigurationsprogramm befindet sich normalerweise im Installationsverzeichnis:
`\Programme\NCP Secure CE Client\`

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.

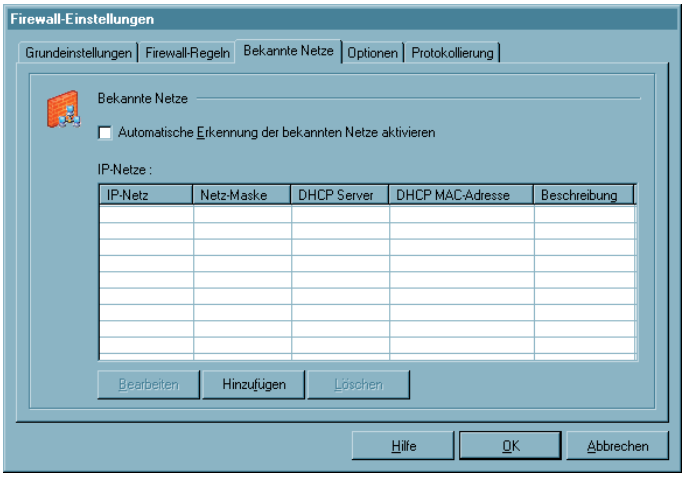
Alle IP-Adressen
– erlaubt die Kommunikation mit beliebigen IP-Adressen der Gegenseite, ohne Einschränkung.
Eindeutige IP-Adresse
– lässt nur Kommunikation mit der hier angegebenen IP-Adresse auf der Gegenseite zu.
Mehrere IP-Adressen /-Bereiche
– gestattet die Kommunikation mit verschiedenen IP-Adressen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



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;

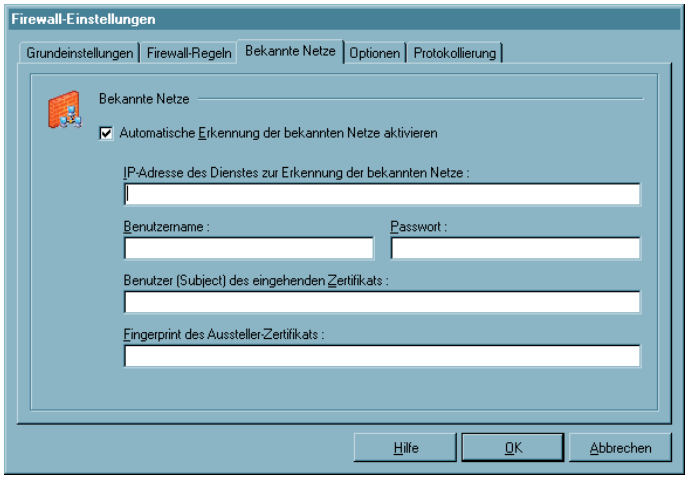
[DHCP MAC-Adresse]

– 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.

Automatische Erkennung der bekannten Netze

Zur autimatischen Friendly Net Detection beachten Sie bitte das Parameterfeld auf der folgenden Seite.

Automatische Erkennung der bekannten Netze



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 IP-Adresse hier eingetragen werden.

Benutzername, Passwort (FNDS)

Die Authentisierung des Friendly Net Detection 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.

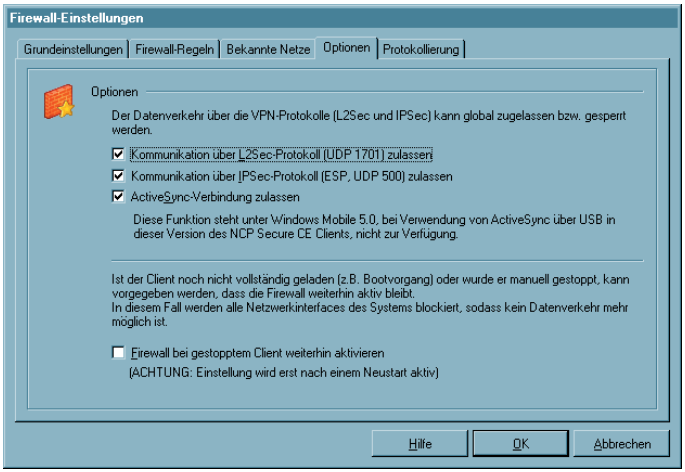
Fingerprint des Aussteller-Zertifikats

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, 26675, 5721

Die (globale) Firewall 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.

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

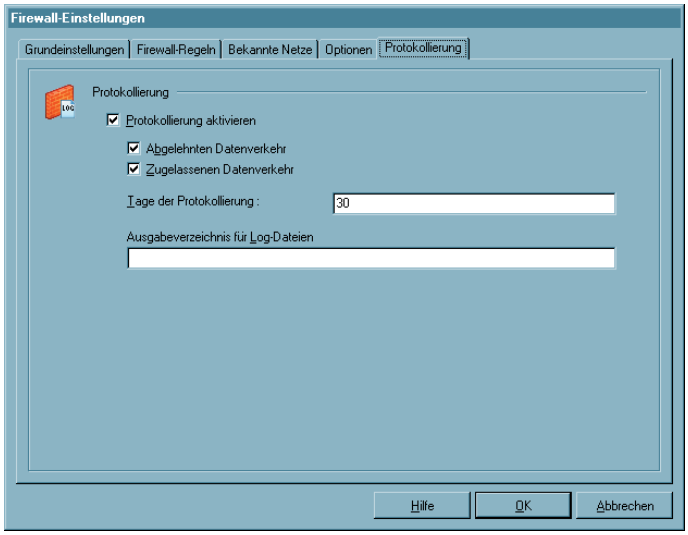
Die globale Definition erspart die Einrichtung dedizierter Einzelregeln für die jeweilige VPN-Variante.

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, auch wenn das Eingabefeld leer bleibt, unter:

```
\Programme\NCP Secure CE Client\log
```

Wird per Hand ein alternativer Pfad eingetragen, so muss dieser Pfad auch am PDA existieren, da ansonsten keine Log-Dateien geschrieben werden.

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.

Bitte beachten Sie, dass es bei aktivierter Protokollierung zu Performance-Einbußen kommen kann, da für jedes Paket, für welches diese Einstellung gilt, ein entsprechender Protokolltext ausgegeben werden muss.

4.2.4 WLAN-Einstellungen

Integrierte WLAN-Konfiguration ab Windows Mobile 2003

Ab Windows Mobile 2003 kann der WLAN-Adapter mit der Verbindungsart “WLAN” betrieben werden. Im Configurator erscheint eigens der Menüpunkt “WLAN-Einstellungen”, worin die Zugangsdaten zum Funknetz in einem Profil hinterlegt werden können. Alternativ kann die Konfiguration auch über da Popup-Menü des WLAN-Managers am PDA erfolgen.

WLAN-Automatik

Über eine intelligente WLAN-Automatik kann im Hintergrund das passende Profil für das aktuell vorliegende WLAN eingesetzt werden.

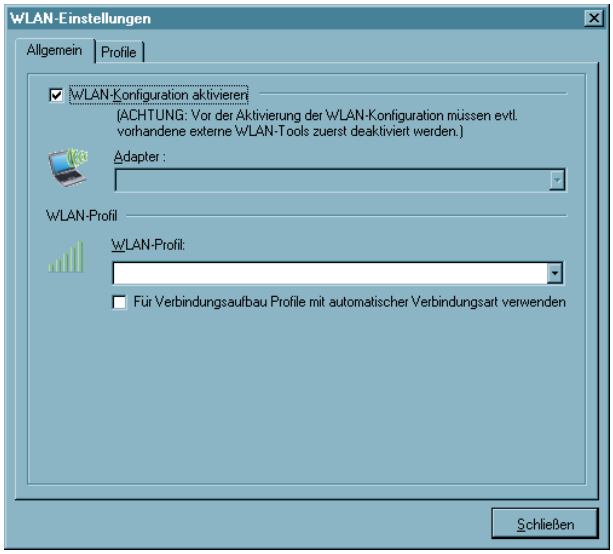
Die Konfiguration erfolgt entweder über die “WLAN-Einstellungen” des Configurators im Konfigurationsmenü oder über den WLAN-Manager des Popup-Menüs in der “WLAN-Steuerung” auf die gleiche Weise. Die Parameter und Konfigurationsfelder entsprechen sich jeweils. Dabei ist lediglich darauf zu achten, dass bei einem Konfigurations-Download vom PC auf den PDA die Einstellungen im WLAN-Manager des Popup-Menüs überschrieben werden.

Unter “Allgemein” kann konfiguriert werden, dass “Für den Verbindungsaufbau Profile mit automatischer Verbindungsart verwendet” werden. Die Verbindungsart “automatisch” kann für jedes Profil einzeln unter “WLAN-Profile / Allgemein” eingestellt werden.

Anschließend wird ein WLAN-Profil selektiert, über das eine Verbindung zum Access Point hergestellt werden soll. Weitere Profile gelangen automatisch dann zum Einsatz, wenn diese mit Verbindungsart “automatisch” konfiguriert wurden und die Funktion “Für Verbindungsaufbau Profile mit automatischer Verbindungsart verwenden” aktiviert wurde.

D. h., wurden mehrere Profile mit der Verbindungsart “automatisch” angelegt und wird die Funktion “Für Verbindungsaufbau Profile mit automatischer Verbindungsart verwenden” genutzt, so wird zunächst das zuletzt selektierte Profil für einen möglichen Verbindungsaufbau herangezogen. Ist die SSID nicht passend, sodass mit diesem Profil keine Verbindung zum Access Point hergestellt werden kann, so werden anschließend die als “automatisch” konfigurierten Profile für den Verbindungsaufbau herangezogen und das mit der passenden SSID verwendet.

Allgemein



Wird über den WLAN-Manager die “WLAN-Konfiguration aktiviert” geschaltet, so muss das Management-Tool bzw. das Microsoft-Tool der WLAN-Karte deaktiviert werden. Dies erfolgt über einen Soft-Reset oder über einen Neustart der WLAN-Karte. (Die jeweils nicht eingesetzten Tools müssen deaktiviert werden.)

Adapter

Sofern ein WLAN-Adapter installiert ist, wird dieser angezeigt.

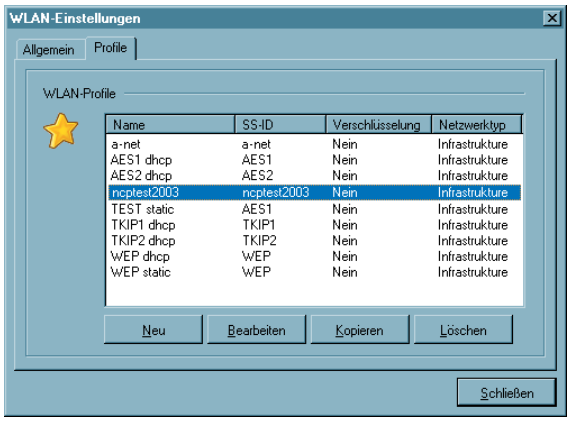
WLAN-Profil

Ein bereits erstelltes WLAN-Profil kann hier für das gewünschte Netz ausgewählt werden. (Bei einem MDA wird mit Klick auf den Verbinden-Button der Verbindungsaufbau initialisiert.)

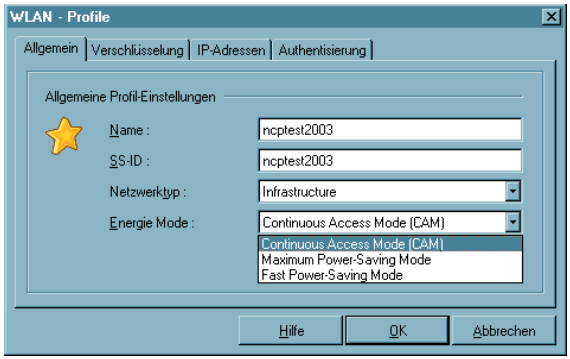
Für Verbindungsaufbau Profile mit automatischer Verbindungsart verwenden

Wurden mehrere Profile mit der Verbindungsart “automatisch” angelegt und wird die Funktion “Für Verbindungsaufbau Profile mit automatischer Verbindungsart verwenden” genutzt, so wird zunächst das zuletzt selektierte Profil für einen möglichen Verbindungsaufbau herangezogen. Ist die SSID nicht passend, sodass mit diesem Profil keine Verbindung zum Access Point hergestellt werden kann, so werden anschließend die als “automatisch” konfigurierten Profile für den Verbindungsaufbau herangezogen und das mit der passenden SSID verwendet.

WLAN-Profile

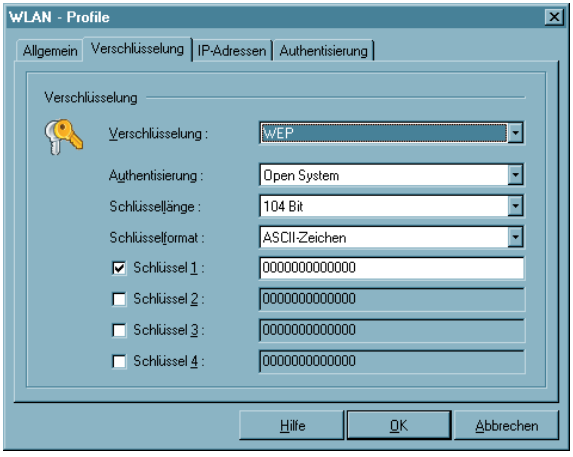


Bereits erstellte Profile zum oben selektierten Adapter werden in einer Liste dargestellt. Netzwerktyp, Verschlüsselung und SS-ID müssen mit den obigen Netzwerkparametern übereinstimmen.
Ein neues Profil wird erzeugt, indem der Button “Neu” gedrückt wird oder im vorigen Fenster auf das zugehörige Netz ein Doppelklick ausgeübt oder die rechte Maustaste geklickt wird. Über die Buttons können Profile auch bearbeitet oder gelöscht werden.



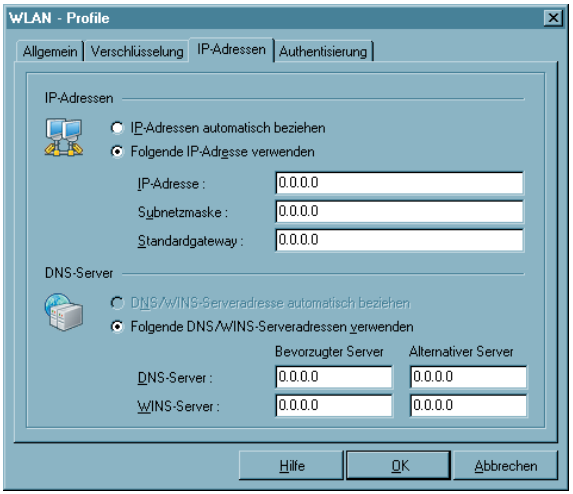
Allgemeine Profil-Einstellungen

Der Name kann frei vergeben werden. Der Name für die SS-ID (Standard Security) wird vom Netzbetreiber vergeben bzw. am WLAN-Router eingegeben. Der Netzwerktyp muss dann manuell auf “Ad-Hoc” umgestellt werden, wenn ein Profil für eine Direktverbindung von PC zu PC hergestellt werden soll. Sofern der WLAN-Adapter dies gestattet, kann der Energie Mode für ihn ausgewählt werden. Mit der Verbindungsart kann angegeben werden, ob dieses Profil für die WLAN-Automatik (automatisch) verwendet wird, oder ob das Profil “manuell” ausgewählt werden muss.



Verschlüsselung

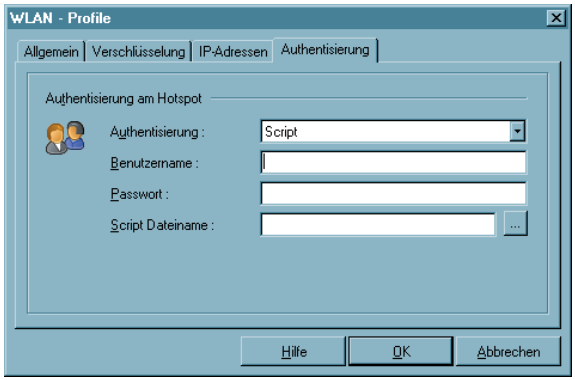
Der Verschlüsselungsmechanismus wird vom Access Point (WLAN Router) vorgegeben und über den Administrator mitgeteilt.



IP-Adressen

In diesem Fenster wird die IP-Adress-Konfiguration der WLAN-Karte vorgenommen.

Die hier gemachten Einstellungen werden dann wirksam, wenn die WLAN-Konfiguration wie oben beschrieben aktiviert wurde. In diesem Fall wird die hier eingetragene Konfiguration in die Microsoft-Konfiguration der Netzwerkverbindungen übernommen. (Siehe dort → Netzwerkverbindungen / Eigenschaften von Internetprotokoll (TCP/IP)).



Authentisierung

In diesem Fenster können die Zugangsdaten für eine automatische Anmeldung am HotSpot eingetragen werden. Diese Benutzerdaten werden nur für dieses WLAN-Profil verwendet.

Die Authentisierung kann durch Eintragen von Benutzername und Passwort in die Eingabemaske des HotSpot-Betreibers erfolgen oder über Script. Das Script automatisiert die Anmeldung beim HotSpot-Betreiber.

Beachten Sie dabei, dass die Verbindung über einen HotSpot-Betreiber gebührenpflichtig ist. Sie müssen den Geschäftsbedingungen des HotSpotbetreibers zustimmen, wenn die Verbindung aufgebaut werden soll.

4.2.5 Zertifikate |Konfiguration

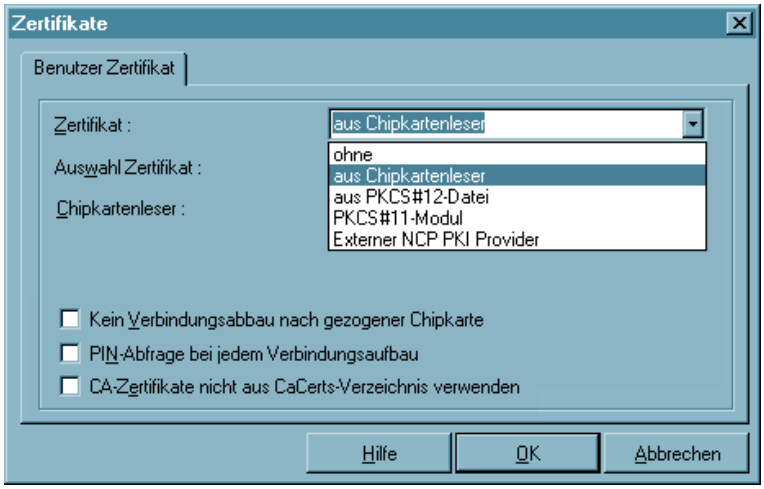
Unter diesem Menüpunkt wird konfiguriert, welche Art von Zertifikaten eingesetzt werden – ob Soft-Zertifikate oder Zertifikate auf Chipkarten (Smart Cards) – und wo diese Zertifikate auf dem PDA zu finden sind.

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.

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

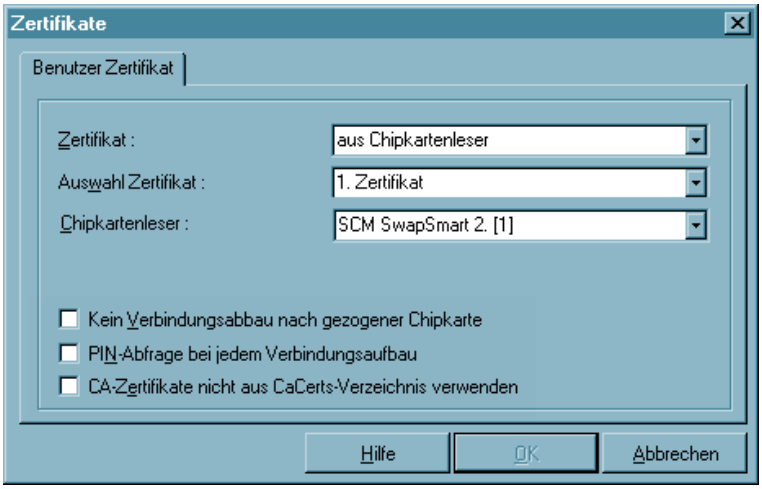


Zertifikat

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 Driver am PDA mindestens einmal gestartet wurde. (Siehe → Voraussetzungen für die Strong Security-Version)

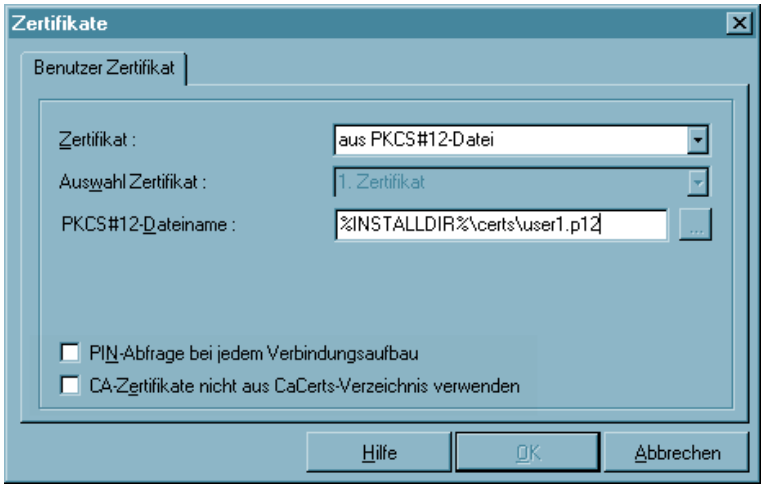
Der Name eines Chipkarten-Lesers kann hier selektiert oder editiert werden. Verwendet man nun am PDA einen anderen Leser so unterscheidet sich der Name und der Leser wird nicht gefunden. Bei zwei Lesern, die sich lediglich in der Firmware unterscheiden, deswegen jedoch einen anderen Namen haben, kann 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**

(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)

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.

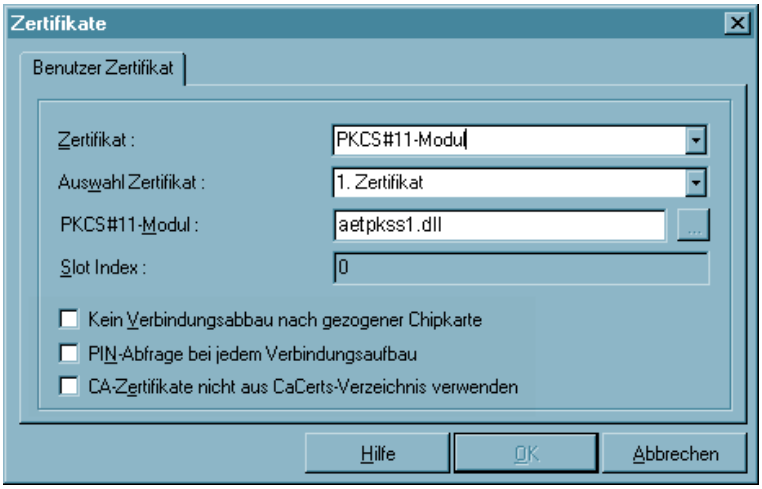
■ **PKCS#12-Dateiname**

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.

Verbindungsabbau bei gezogener Chipkarte

Beim Ziehen der Chipkarte wird nicht unbedingt die Verbindung abgebaut. Ob “Kein Verbindungsabbau bei gezogener Chipkarte” erfolgt, wird an dieser Stelle eingestellt.

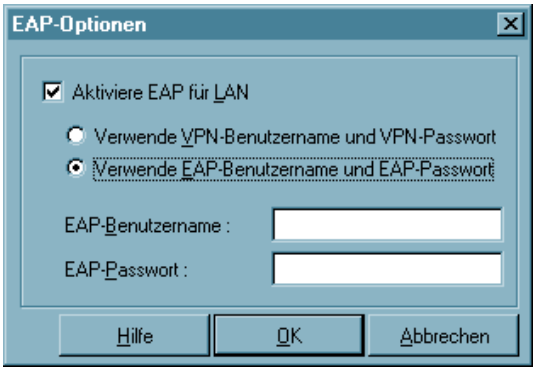
PIN-Abfrage bei jedem Verbindungsaufbau

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

4.2.6 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.

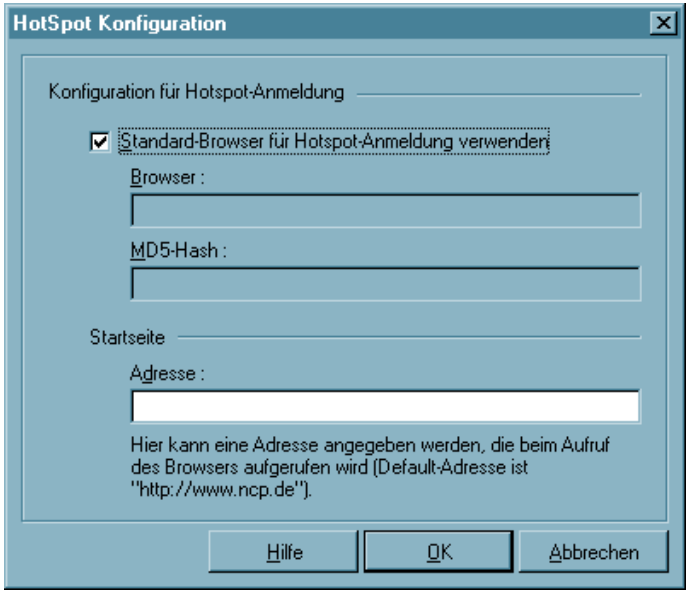
Zur Authentisierung kann wahlweise “VPN-Benutzername” mit “VPN-Passwort” verwendet werden oder ein eigener “EAP-Benutzername” mit einem “EAP-Passwort”.

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%
```

4.2.7 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.

4.2.8 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.

4.2.9 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.

4.2.10 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.

4.2.11 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.

4.2.12 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.

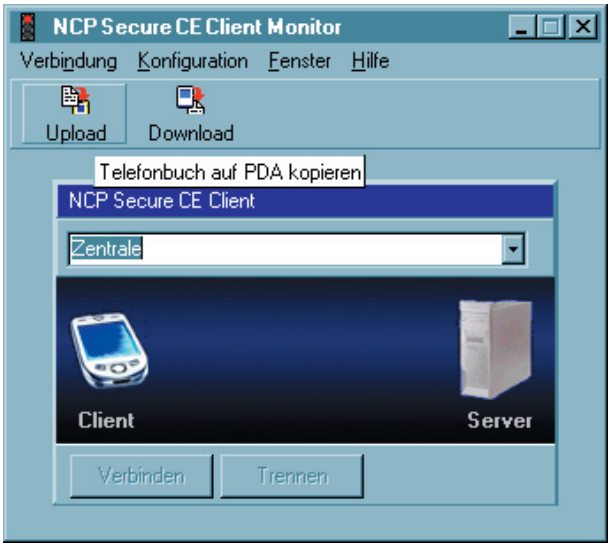
4.3 Fenster – Sprache

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 des Telefonbuchs



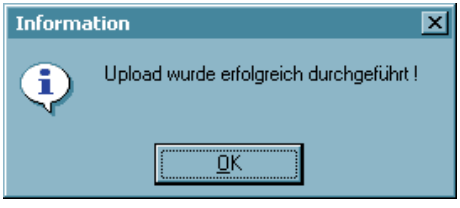
Nachdem die Konfiguration eines Zielsystems abgeschlossen wurde und dieTelefonbucheinträge komplettiert wurden, muss das Telefonbuch auf den PDA kopiert werden.

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.

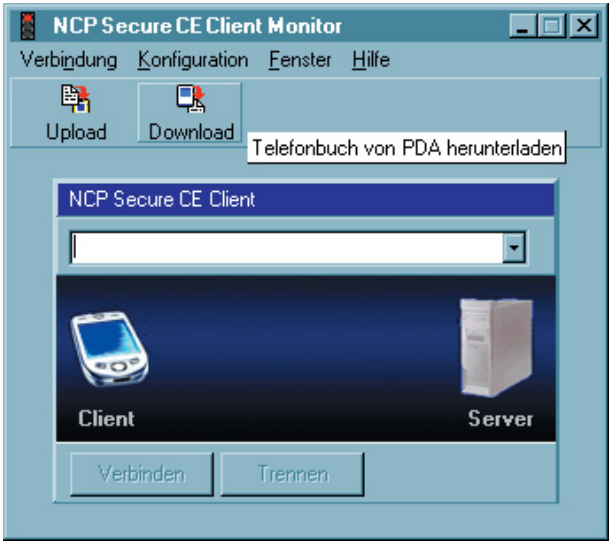


Nachdem der Upload erfolgreich durchgeführt wurde, ...

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

Bitte beachten Sie dass ein eventuell bereits vorhandenes Telefonbuch auf dem PDA ohne Rückfrage überschrieben wird.

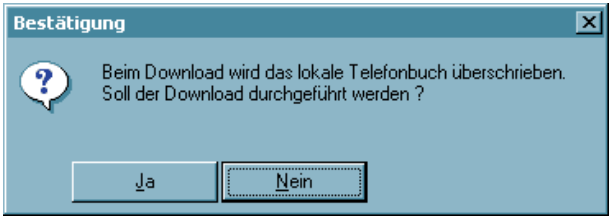
4.6 Download des Telefonbuchs



Ein Download des Telefonbuchs vom PDA auf den PC ist immer dann nötig, wenn Änderungen in der Konfiguration eines 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 des Telefonbuchs vom PDA wird das Telefonbuch auf dem PC überschrieben.

Um ein vorhandenes Telefonbuch auf dem PC zu erhalten, muss es eigens gesichert werden. Es befindet sich in dem Verzeichnis:

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

Diese Seite ist frei

5. Konfigurationsparameter

Mit dem Telefonbuch des NCP Secure CE Client Configurator, kurz “Client Configurator” oder “Configurator”, wird die Software für den Einsatz am PDA konfiguriert und die Konfiguration auf das Gerät übertragen.

Wie oben unter “Client Configurator” beschrieben, können neue Zielsysteme mit dem Konfigurations-Assistenten angelegt werden. Mit Hilfe dieses Assistenten werden die Zielsysteme so weit wie möglich vorkonfiguriert. Um Modifikationen oder Erweiterungen vornehmen zu können, ist es aber unumgänglich, dass einzelne Parameter, die nicht vom Konfigurations-Assistenten abgefragt werden, über das Telefonbuch- oder das IPSec-Menü gesetzt werden.

Zur Bedienung des Telefonbuch- und des IPSec-Menüs beachten Sie bitte die Beschreibung in diesem Handbuch unter “Configurator-Menü / Konfiguration / Telefonbuch / IPSec”.

Im folgenden sind alle Parameter mit Beschreibungen aufgeführt, und sie sind so angeordnet, wie sie auf der Oberfläche des Configurators erscheinen. Beschreibungen der funktionalen Zusammenhänge in PKI-, VPN- oder IPSec-Architekturen finden Sie in den Beispiel-Texten des Handbuchs (siehe → Beispiele und Erklärungen).

Ordnungsprinzip der Parameter

Die Parameter sind in verschiedenen Parameterfeldern gesammelt. In der Kopfzeile steht der Name des Zielsystems (im Telefonbuch-Menü) oder der Name der Richtlinie (im IPSec-Menü). Sie erreichen die Konfigurationsparameter über die Untermenüs

Konfiguration / Telefonbuch (5.1)

Konfiguration / IPSec (5.2)

Die Beschreibung der einzelnen Parameter folgt der Reihenfolge ihres Erscheinens in den einzelnen Parameterfeldern wie sie von oben nach unten angeordnet sind.

Zum schnellen Auffinden eines Parameters kann die Überschrift eines Parameterfelds oder der Index herangezogen werden.

Um Verwechslungen bei gleichlautenden Parametern vorzubeugen, wurden die Namen der übergeordneten Parameterfelder dahinter gesetzt. Diese Begriffe haben nur die Funktion, die Orientierung zu erleichtern!

5.1 Telefonbuch

Parameterfelder:

1 *Zielsystem*

2 *Netzeinwahl*

3 *Modem*

4 *Verbindungssteuerung*

5 *Security*

6 *Authentisierung vor VPN*

7 *HTTP-Anmeldung*

8 *Link-Einstellungen*

9 *Tunnel-Parameter*

10 *VPN IP-Netze*

11 *IPSec-Optionen*

12 *HA-Unterstützung*

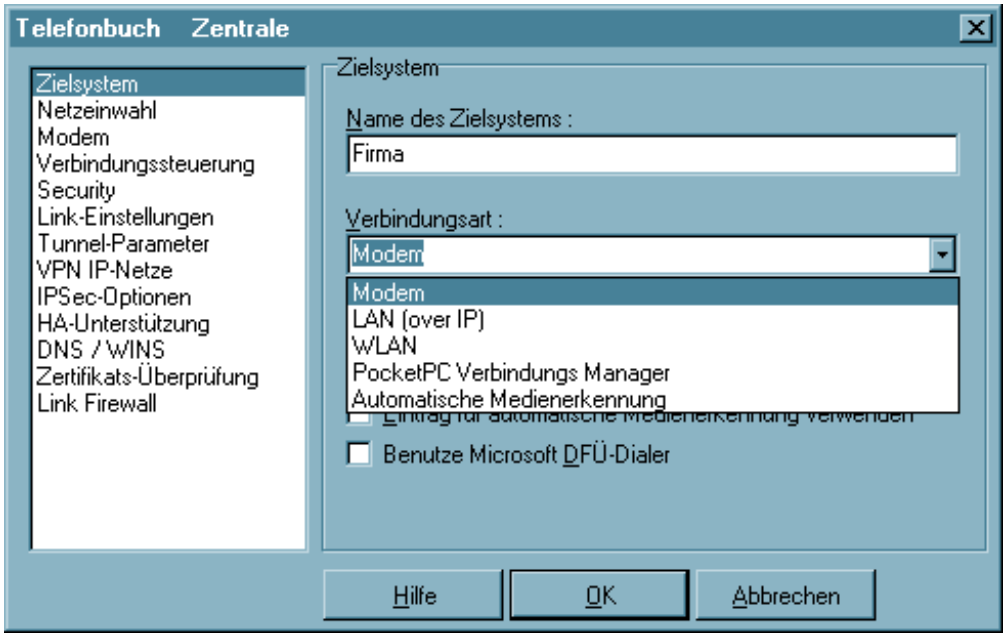
13 *DNS/WINS*

14 *Zertifikats-Überprüfung*

15 *Link Firewall*

Parameter und Parameterfelder werden nach der jeweils gewählten Verbindungsart automatisch ein- oder ausgeblendet (z.B. Modem). Einzelne Parameterfelder oder Parameter, die Sie für Ihre Arbeit mit dem Client nicht benötigen, können von Ihrem Systemadministrator ausgeblendet worden sein.

5.1.1 Zielsystem



Die Client Software gestattet die Einrichtung individueller Ziele bzw. Zielsysteme (auch Profile), die den Benutzeranforderungen entsprechend konfiguriert werden können. Um sie voneinander wie in einem Telefonbuch unterscheiden zu können, muss in diesem Parameterfeld zunächst ein Name für das Zielsystem vergeben werden. Danach kann die Verbindungsart zum Zielsystem genauer definiert werden.

Parameter:

☐ Name Zielsystem

☐ Verbindungsart

☐ Zielnetzwerk

☐ Eintrag für automatische Medienerkennung verwenden

☐ Benutze Microsoft DFÜ-Dialer

■ Name des Zielsystems

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

■ Verbindungsart

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

Folgende Verbindungsarten können eingestellt werden:

Modem

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

LAN (over IP)

Hardware: LAN-Adapter;
Netze: WLAN mit Ethernet;
Gegenstellen: Die Gegenstellen des lokalen Multiprotokoll-Routers im LAN;

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 genügend 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.

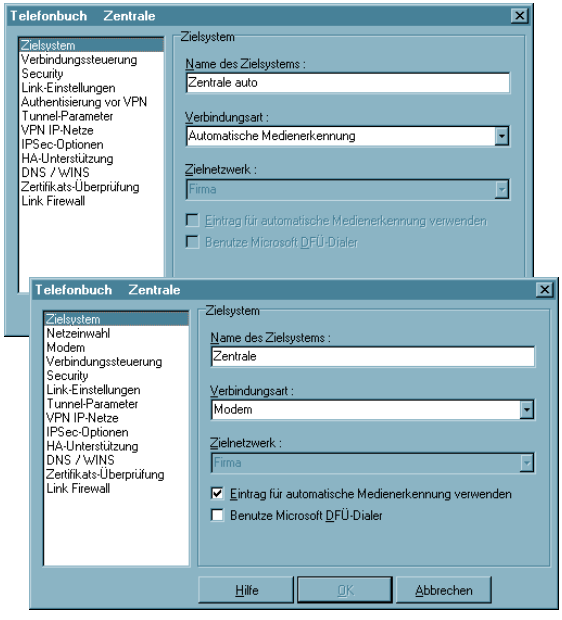
WLAN

Hardware: WLAN-Adapter;
Netze: Funknetz;
Gegenstellen: Access Point;

Die Verbindungsart WLAN kann nur ab Windows Mobile 2003 genutzt werden. Wird diese “WLAN-Konfiguration aktiviert”, so muss das Management-Tool der WLAN-Karte deaktiviert werden. (Alternativ kann auch das Management-Tool der WLAN-Karte genutzt werden, dann muss die WLAN-Konfiguration im Monitormenü deaktiviert werden.)

Automatische Medienerkennung

Werden wechselweise unterschiedliche Verbindungsarten genutzt, wie zum Beispiel Modem und ISDN, so kann die manuelle Auswahl des Zielsystems mit der jeweils zur Verfügung stehenden Verbindungsart 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 (links oben) mit allen für die Verbindung zum VPN Gateway nötigen Parametern (insbesondere der IP-Adresse des VPN Gateways) konfiguriert ist, wohingegen die Zielsysteme mit den alternativen Verbindungsarten (links unten) so konfiguriert sein müssen, dass die jeweils gewünschte Verbindungsart (evtl. auch die Modemparameter) eingestellt ist und die Funktion “Eintrag für automatische Medienerkennung verwenden” aktiviert ist.

Außerdem müssen für die jeweilige Verbindungsart 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. MODEM. Die Eingangsdaten für die Verbindung zum ISP werden aus den Telefonbucheinträgen übernommen, die für die automatische Medienerkennung konfiguriert wurden.

■ Eintrag 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.

■ Benutze Microsoft DFÜ-Dialer

Zur Einwahl am ISP (Internet Service Provider) kann der Microsoft RAS-Dialer genutzt werden. Dies ist immer dann nötig, wenn der Einwahlpunkt ein Einwahl-Script benötigt. Der RAS-Dialer unterstützt dieses Script. Beachten Sie zudem, dass RAS-Dialing nur für VPN-Verbindungen genutzt werden kann.

Im Parameterfenster “Netzeinwahl” wird anschließend die RAS Script-Datei unter Eingabe von Pfad und Namen zur eingespielten Script-Datei eingetragen (siehe → RAS Script-Datei).

NCP-Dialer und Microsoft DFÜ-Dialer

Der CE Client kann sowohl den Microsoft RAS-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 Telefonbuch unter “Zielsystem” eingestellt werden. Wird für das Zielsystem die Verbindungsart “Modem” gewählt, so kann die Option “Benutze Microsoft RAS-Dialer” 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.

Amtsholung

Eine eventuell notwendige Amtsholung muss bei Verwendung des NCP-Dialers der “Rufnummer Ziel”, im Telefonbuch unter “Netzeinwahl”, vorangestellt werden. Dies muss bei der Erstellung des Telefonbuchs 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” in der Liesmich-Datei oder in der Broschüre “PDA-Monitor”.

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. Der Name für den Benutzer kann bis zu 256 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Benutzername vom Zielsystem zugewiesen, da Sie vom Zielsystem auch 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 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.

Hinweis: Für den Fall, dass Sie den Parameter “Passwort speichern” nicht aktiviert haben, gilt: Auch wenn Sie für den Verbindungsmodus “automatisch” gewählt haben, müssen Sie die Verbindung beim ersten Mal manuell aufbauen. Dabei werden Sie nach dem Passwort gefragt. Für jeden weiteren automatischen Verbindungsaufbau wird dieses Passwort selbständig übernommen, bis Sie den PC erneut booten oder Sie das Zielsystem wechseln.

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 PDA 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 Telefonbuch gespeichert und für die Anwahl verwendet: 00441711234567
Die Rufnummer des Ziels kann bis zu 30 Ziffern beinhalten.

■ Alternative Rufnummern

Möglicherweise ist das Zielsystem ein Network Access Server (NAS), der mit mehreren S0-Anschlüssen für verschiedene Rufnummern ausgestattet ist. In diesem 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 : 000441711234567:000441711234568
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.

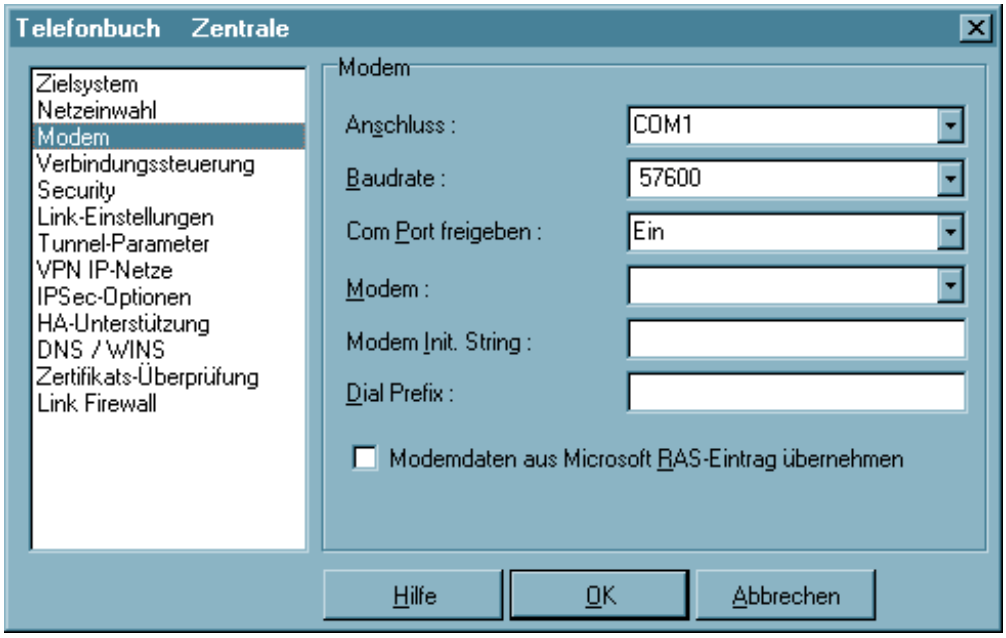
Wichtig: Bitte beachten Sie, dass der Verbindungsaufbau nur funktionieren kann, wenn die Protokoll-Eigenschaften für die Anschlüsse der alternativen Rufnummern die gleichen sind.

■ Script-Datei

Wenn Sie den Microsoft RAS-Dialer benutzen, tragen Sie hier die Script-Datei unter Eingabe von Pfad und Namen ein.

(Siehe → Zielsystem, Benutze Micosoft RAS-Dialer)

5.1.3 Modem



Dieses Parameterfeld erscheint ausschließlich, wenn Sie als "Verbindungsart" "Modem" gewählt haben. Alle nötigen Parameter zu dieser Verbindungsart sind hier gesammelt. Bei Einsatz des Microsoft RAS-Dialers sind nur die Parameter "Baudrate" und "Modem" konfigurierbar. Je nach Einsatz des vorher unter "Zielsystem" festzulegenden Dialers werden zum Modem die zugehörigen Treibernamen zur Auswahl gelistet.

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:

- ☐ Anschluss
- ☐ Baudrate
- ☐ Com Port freigeben
- ☐ Modemdaten aus RAS-Eintrag übernehmen
- ☐ Modem
- ☐ Modem Init. String
- ☐ Dial Prefix

■ 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. In diesem Fall stellen Sie den Parameter auf “Ein”. Solange der Parameter in der Standardstellung auf ”Aus” bleibt, wird der Com Port ausschließlich von der Client Software genutzt.

■ Modem

Die Modemliste wird aus der Registry des PDA gewonnen und für dieses Konfigurationsfeld des Telefonbuchs zur Auswahl gestellt. Je nachdem, welches Modem Sie wählen, wird der zugehörige Parameter ”Com Port” automatisch in das Konfigurationsfeld des Telefonbuchs aus der Treiberdatenbank des Systems übernommen.

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

■ 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.

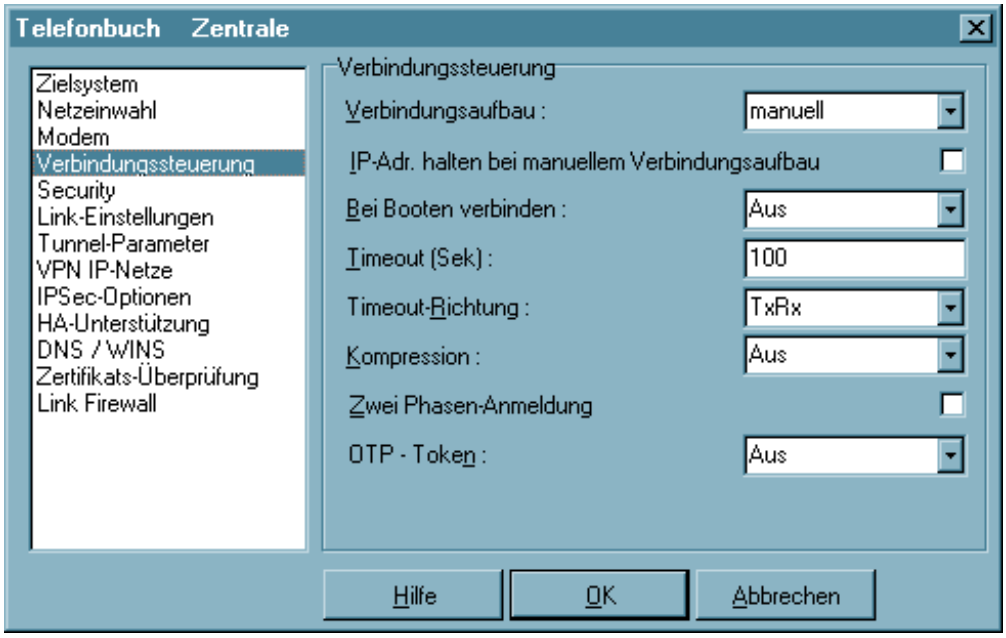
Neuer Telefonbucheintrag mit Modem-Verbindung

Wird ein neuer Telefonbucheintrag mit Modem-Verbindung erzeugt indem der Button “Neuer Eintrag” im Telefonbuch 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 PDA-Hersteller 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 Telefonbucheintrag 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.

5.1.4 Verbindungssteuerung



In diesem Parameterfeld bestimmen Sie, wie der Verbindungsaufbau erfolgen soll und stellen die Timeout-Werte ein. Zudem können Sie Kompression aktivieren und die Art der Kompression bestimmen. Mit Kompression kann der Datendurchsatz um den Faktor 3 bis 5 erhöht werden, je nachdem um welche Daten es sich handelt.

Parameter:

☐ Verbindungsaufbau

☐ IP-Adr. halten bei manuellem Verbindungsaufbau

☐ Bei Booten verbinden

☐ Timeout

☐ Timeout-Richtung

☐ Kompression

☐ Zwei Phasen-Anmeldung

☐ OTP-Token

■ Verbindungsaufbau

Hier definieren Sie, wie die Verbindung zu einem, im Telefonbuch eingetragenen Zielsystem, aufgebaut werden soll. Drei Modi stehen zur Wahl:

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 Telefonbuch.

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.

Ist der Timeout auf Null (0) gesetzt, d.h. kein Timeout eingestellt, müssen Sie in jedem Fall die Verbindung manuell trennen.

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.

■ IP-Adr. halten bei manuellem Verbindungsaufbau

Wird eine Verbindung getrennt – auch durch Timeout – so verliert der Client standardmäßig die IP-Adresse, die ihm das VPN Gateway aus dem Firmennetz für die Session zugewiesen hatte. Ist die Funktion “IP-Adr. halten bei manuellem Verbindungsaufbau” aktiviert, so behält der Client die IP-Adresse nach Beendigung der Verbindung bis zum nächsten manuellen Verbindungsaufbau, sodass die logische Verbindung ununterbrochen bestehen bleibt.

Hinweis: Diese Funktionalität kann nur für manuellen oder wechselnden Verbindungsmodus genutzt werden.

■ Bei Booten verbinden

Wenn Sie “Bei Booten verbinden” aktivieren wollen, schalten Sie dieses Feature auf ”Ein”. Die Standardeinstellung ist “Aus”.

Dieser Funktions-Parameter wirkt nur nach einem Soft-Reset.

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".

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.

Timeout-Richtung

Mit diesem Parameter bestimmen Sie, für welche Übertragungsrichtung der Timeout gelten soll. Drei verschiedene Einstellungen sind möglich:

TxRx	(standard) in diesem Fall achtet der Client sowohl auf das Ende der gesendeten (out) als auch der empfangenen (in) Daten, bevor der Timer angestoßen wird.
Tx	nur die Senderichtung (out) wird beobachtet.
Rx	nur die Empfangsrichtung (in) wird beobachtet.

Hinweis: Um die Timeout-Richtung zur Geltung kommen zu lassen, muss der Wert für den Timeout zwischen 1 und 65356 gewählt sein.

Kompression

Mit diesem Parameter bestimmen Sie den Typ der eingesetzten Kompression. Drei Einstellungen sind möglich:

Aus	(standard), d.h. ohne Kompression
STAC	(without History)
STAC mit History	Cisco-kompatibel

Wichtig: Der hier gewählte Typ der Kompression muss auch vom Network Access Server (NAS) unterstützt werden.

Ziehen Sie zu weiteren Informationen bitte Ihren Internet Provider oder Ihren Systemadministrator zu Rate.

■ 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.

■ OTP-Token

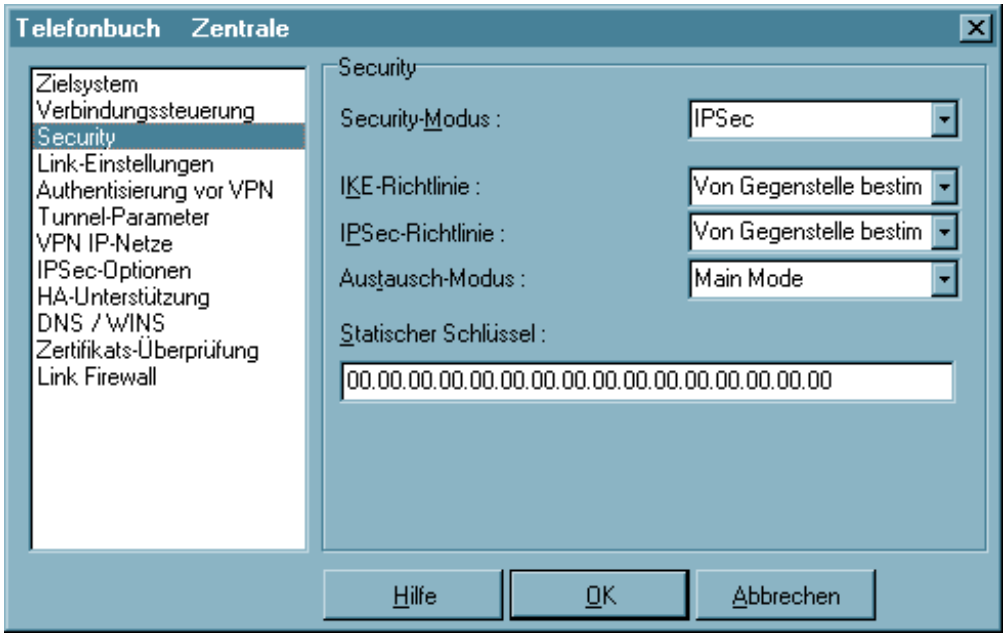
Wird ein OTP-Token verwendet, so kann statt “Benutzername” und “Passwort” für die Einwahl die PIN und das Onetime-Passwort des Tokens eingegeben werden. Wofür der OTP-Token genutzt wird, wird mit folgenden Einstellungen bestimmt:

Aus =	(standard) OTP wird nicht genutzt
NAS-Einwahl =	Wird ein OTP für die Einwahl an einem NAS geutzt, wird das Feld für “Passwort” unter “Netzeinwahl” inaktiv geschaltet.
VPN-Einwahl =	Wird ein OTP für die Einwahl zum VPN Gateway genutzt, wird entsprechend das Feld für “VPN-Passwort” unter “Tunnel-Parameter” inaktiv geschaltet.

Bei der Einwahl erscheint ein Dialogfenster für die Eingabe des “Einmalpassworts”, in welches PIN und Einmalpasswort des Tokens eingetragen werden müssen.

Werden vom ACE-Server auf Grund des RSA-Tokens Nachrichten versendet, werden diese am Monitor in einem Informationsfenster mit Eingabefeld angezeigt (z.B. “Ablauf der gültigen PIN” oder “Ablauf des OTP-Passworts”). Geben Sie die neue PIN oder das neue Passwort von Ihrem Token in das Eingabefeld ein.

5.1.5 Security



Im Parameterfeld "Security" sind die Konfigurationsparameter zu L2Sec und IPSec für den Einsatz in Remote Access-Umgebungen gesammelt. Je nach eingestelltem Sicherheits-Modus, L2Sec oder IPSec, kann eine weitergehende Parametrisierung vorgenommen werden.

Der Sicherheits-Modus "L2Sec" wurde in früheren Versionen der Secure Software standardmäßig immer eingesetzt, wenn eine der angebotenen Verschlüsselungsarten gewählt wurde! In früheren Versionen der Secure Software hieß das Parameterfeld "Security" "Verschlüsselung".

Sofern IPSec für Remote Access eingesetzt wird, wird die Secure Policy Database (SPD) nach Vorgabe der hier eingestellten Parameter dynamisch aufgebaut (siehe im Handbuch → IPSec für Remote Access – IPSec over L2TP). Alle IP-Pakete für dieses Ziel werden über die dynamische SPD abgearbeitet. In diesem Fall wird eine statische SPD-Konfiguration nicht benötigt – so dass eventuell im Konfigurationsbaum vorhandene statische SPDs "inaktiv" geschaltet werden können!

Sind statische SPDs aktiv geschaltet, so werden im IPSec-Prozess zunächst für jedes IP-Paket die Filter der statischen SPDs abgearbeitet.

Aus Sicherheitsgründen ist IPSec für Remote Access nur im Tunnelmodus nutzbar. Der Transportmodus mit Authentication Header ist in diesem Parameterfeld für eine dynamische SPD nicht konfigurierbar und kann nur für statische SPDs eingestellt weren (siehe → Beispiele und Erklärungen, IPSec, AH und ESP im Tunnel- und Transportmodus).

Mit der Verschlüsselung werden wichtige Datenbestände eines Computer-Netzwerks und -Systems geschützt. Vor allem bei der Übertragung sensibler Daten über öffentliche Netze, die jedermann nutzen kann, ist die Verschlüsselung von größter Bedeutung. In der Secure Client Software ist eine Reihe von Sicherheitsmechanismen implementiert, um den Zugriff unautorisierter Personen zu verhindern und eine unbefugte Nutzung auszuschließen. Obwohl Standards zur Verschlüsselung existieren (DES oder AES), sind bislang noch keine ausreichenden Sicherheits-Standards entwickelt worden, die auch für die Interoperabilität zwischen verschiedenen Systemen ähnlich hohe Sicherheit gewähren. Daher ist es unbedingt erforderlich, dass die Gegenstelle des Secure Clients die entsprechend gleichen Standards unterstützt. Weiterhin ist NCP bemüht jeden neu verfügbaren Verschlüsselungs-Standard zu implementieren.

Parameter:

☐ Security-Modus

☐ Verschlüsselung |Security

☐ Index |Security

☐ Statischer Schlüssel |Security

☐ Preshared Key |Security

☐ Dateiname |Security

☐ IKE-Richtlinie |Security

☐ IPSec-Richtlinie |Security

☐ Austausch-Modus |Security

☐ IKE ID-Typ

☐ IKE ID

■ Security-Modus

Hier legen Sie den Sicherheits-Standard für eine Verbindung fest, L2Sec oder IPSec. Bitte beachten Sie dabei, dass nur mit L2Sec neben IP-Paketen auch NetBios-, IPX- und SNA-Daten übertragen werden können.

inaktiv	=	Verschlüsselung und Authentisierung sind ausgeschaltet
L2Sec	=	NCP Standard. Alle Sicherheits-Verhandlungen erfolgen verschlüsselt und sicher in einem End to End-Tunnel (Layer 2) zwischen Client und Secure Server (siehe → Beispiele und Erklärungen, L2Sec – Layer 2-Verbindungen mit Security).
IPSec	=	Zusätzlich kann mit dieser Option über jeden Layer-2-Medientyp (siehe → verfügbare Verbindungsarten), wie ISDN oder L2TP, zwischen Client und Secure Server der Standard IPSec im Tunnel-Modus (Layer 3) eingesetzt werden (siehe → Beispiele und Erklärungen, IPSec für Remote Access – IPSec over L2TP).

■ Verschlüsselung |Security

In diesem Feld bestimmen Sie, ob eine Verschlüsselung eingesetzt wird, und welche Art der Verschlüsselung verwendet werden soll. In den meisten Fällen wird die Art der Verschlüsselung von der Gegenstelle bestimmt sein, d.h. vom Zentralsystem.

Aus	=	Verschlüsselung nicht aktiv (standard)
Von Gegenstelle bestimmt	=	Die Daten werden je nach Verschlüsselungstechnik des Zielsystems nach Blowfish 128 / 448 oder Triple DES verschlüsselt übertragen.
SSL mit Zertifikat	=	Mit dieser Verschlüsselung ist ein Verbindungsaufbau nur möglich, wenn vorher eine gültige PIN eingegeben wurde. Diese Verschlüsselungsart (wie auch Blowfish und 3DES unter “ Von Gegenstelle bestimmt”) wird vom Zentralsystem vorgegeben.

■ Statischer Schlüssel |Security

Der Schlüssel kann nur eingegeben werden, wenn vorher die Verschlüsselung aktiviert wurde. Der Schlüssel ist ein String mit 16 hexadezimalen Zahlen, die durch einen Punkt (.) getrennt sind.

Standard ist: 00.11.22.33.44.55.66.77.88.99.AA.BB.CC.DD.EE.FF

Wichtig: Der Schlüssel muss abgestimmt sein mit dem in der Konfiguration der Remote-Seite (Zielsystem).

■ **Preshared Key |Security**

Der Preshared Key ist ein String beliebiger Zeichen in einer maximalen Länge von 255 Zeichen. Der Preshared Key muss nur dann eingegeben werden, wenn eine Verbindung mit “IPSec-Tunneling” zu einem fremden IPSec Gateway aufgebaut werden soll und diese Gegenstelle als IKE-Richtlinie “Preshared Key” erwartet.

■ **IKE-Richtlinie |Security**

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

Funktional unterscheiden sich zwei IKE-Richtlinien, die standardmäßig vorkonfiguriert mit der Software ausgeliefert werden (siehe → Beispiele und Erklärungen, IPSec, IKE-Modi). Sie finden sie unter Konfiguration unter “IPSec – IKE-Richtlinie” als “Preshared 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 → IPSec, IKE-Richtlinie, Authentisierung, Verschlüsselung), 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.

Von Gegenstelle bestimmt:

In diesem Fall kann die Konfiguration der IKE-Richtlinie im IPSec-Menü entfallen.

Preshared Key:

Diese vorkonfigurierte Richtlinie kann ohne PKI-Unterstützung genutzt werden. Beidseitig wird der gleiche “Statische Schlüssel” verwendet (siehe oben → Statischer Schlüssel).

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 Smartcard oder eines Soft-Zertifikats.

■ IPSec-Richtlinie |Security

Die IPSec-Richtlinie wird aus der Listbox ausgewählt. In der Listbox werden alle IP-Sec-Richtlinien aufgeführt, die Sie unter “Konfiguration” unter der “IPSec – IPSec-Richtlinie” 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 eine IPSec-Richtlinie mit ESP-Protokoll standardmäßig vorkonfiguriert mit der Software ausgeliefert (siehe → Beispiele und Erklärungen, IPSec, AH und ESP). Sie finden sie unter “Konfiguration” unter “IPSec – IPSec-Richtlinie”. Inhalt und Name dieser Richtlinie können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu IPSec-Protokoll und Authentisierung auf (siehe → IPSec, IPSec-Richtlinie, Protokoll, Authentisierung), 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.

Von Gegenstelle bestimmt:

In diesem Fall kann die Konfiguration der IKE-Richtlinie im IPSec-Menü entfallen.

■ Austausch-Modus |Security

Der 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 (siehe → Beispiele und Erklärungen, IPSec, IKE-Modi).

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.

■ IKE ID-Typ |Security

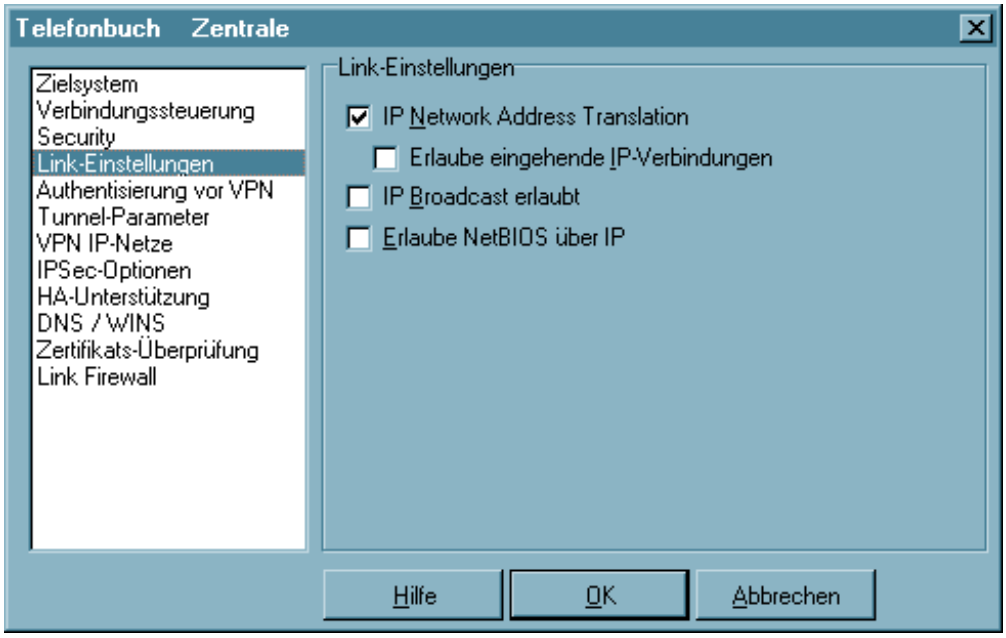
Bei “IPSec-Tunneling” (native IPSec) werden die Parameter “IKE ID-Typ” und “IKE ID” eingeblendet. Für den “IKE ID-Typ” stehen folgende Alternativen zur Auswahl:

– IP Address
– Fully Qualified Domain Name
– Fully Qualified Username
– IP Subnet Address
– ASN1 Distinguished Name
– ASN1 Group Name
– Free String used to identify Groups

■ IKE ID |Security

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

5.1.6 Link-Einstellungen



Die Einstellungen in diesem Parameterfeld hängen vom Network Access Server des jeweiligen Zielsystems ab. Wenn Ihnen diese Parameter nicht bekannt vorkommen, oder Sie unsicher bei der jeweiligen Einstellung sind, wird empfohlen sich an Ihren Systemadministrator oder Ihren Internet Service Provider zu wenden, um weitere Informationen zu bekommen.

Parameter:

☐ IP Network Address Translation

☐ Erlaube eingehende IP-Verbindungen

☐ IP Broadcast erlaubt

☐ Erlaube NetBios over IP

IP Network Address Translation

Wenn IP NAT aktiviert ist, werden alle übertragenen Frames mit der ausgehandelten (PPP) IP-Adresse verschickt. Wenn Sie IP Network Address Translation nutzen, können Sie jede beliebige IP-Adresse in Ihren Systemeinstellungen konfigurieren, da die Client Software die ausgehandelte (PPP) IP-Adresse in Ihre systemeigene übersetzt. Die DHCP Wartezeit wird in diesem Fall ignoriert. Wenn Sie die Eigenschaften des Protokolls ändern wollen, um DHCP zu nutzen oder eine feste IP-Adresse einzustellen, können Sie AUTOINSTALL nutzen oder Sie gehen auf dem PDA wie folgt vor:
→ Startmenü
→ Einstellungen
→ Verbindungen
→ Netzwerkadapter
→ Eigenschaften

Hinweis: Die meisten Internet Service Provider nutzen die Network Address Translation zur Kommunikation.

Erlaube eingehende IP-Verbindungen

Mit dem Schalter “Erlaube eingehende IP-Verbindungen” kann IP NAT modifiziert werden. Wenn dieser Schalter gesetzt ist, kann eine Verbindung aktiv von außerhalb aufgebaut werden, und die Gegenstelle kann auf den Rechner zugreifen.
Bitte beachten Sie, dass es nur sinnvoll ist, diesen Schalter zu setzen wenn der Zugriff von einer definierten Gegenstelle erfolgen, z.B. aus dem Firmennetz, da mit dem Setzen dieses Schalters der Schutzmechanismus von IP-NAT aufgehoben wird. D.h. potentiell kann jeder Teilnehmer aus dem eingewählten Netz auf den Rechner mit der Client Software zugreifen. Anders in einem Virtual Private Network (VPN). Nur die Teilnehmer dieses VPN haben die Möglichkeit zur Einwahl, der Tunnel blockt alle sonstigen Verbindungsversuche ab.

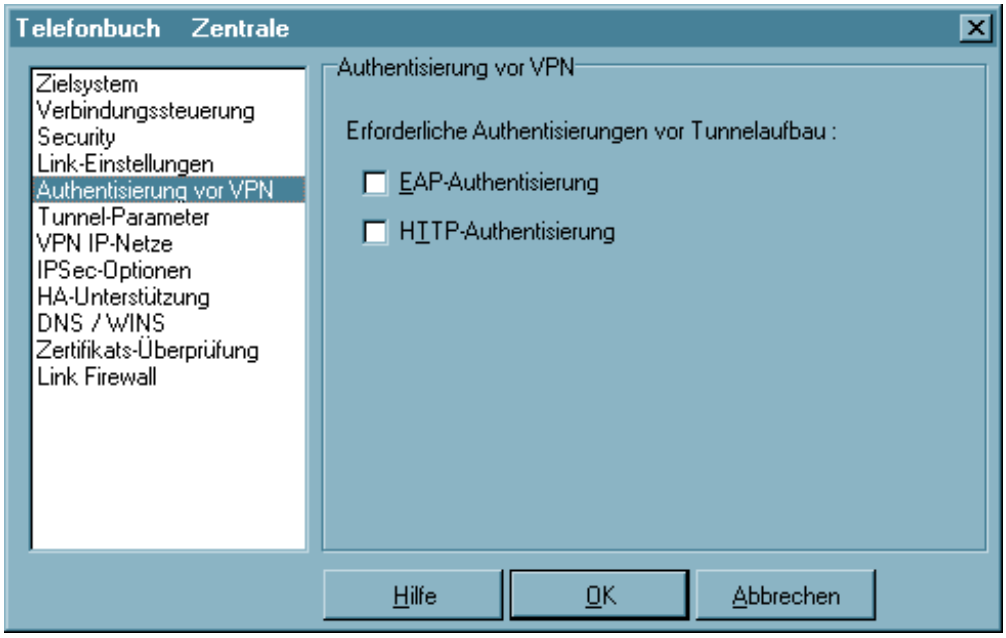
IP Broadcast erlaubt

Mit diesem Parameter entscheiden Sie, ob die Client Software die Übertragung von IP-Broadcasts zulassen soll. IP-Broadcasts werden z.B. dann eingesetzt, wenn ein LAN-Client (wie etwa die Client Software) im Netz nach einem File Server sucht. Im Fall des Clients wäre das Netz ein Remote-LAN, an welches der Client via ISDN angeschlossen ist. IP-Broadcasts werden unterdrückt, wenn das Feld nicht angeklickt ist (standard).
Hinweis: IP-Broadcasts müssen Sie zulassen, wenn Sie DHCP nutzen um eine IP-Adresse vom Zielsystem anzufordern.

Erlaube NetBios over IP

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 Secure Client nutzen.

5.1.7 Authentisierung vor VPN



Dieses Parameterfeld erscheint nur, wenn für das Zielsystem die Verbindungsart "LAN" oder "WLAN" konfiguriert wurde, bzw. ein externer Dialer eingesetzt wird oder das Zielsystem für die automatische Medienerkennung konfiguriert wurde. Beachten Sie dazu die Beschreibungen zum Parameterfeld "Zielsystem / Verbindungsart".

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

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

Parameter:

☐ EAP-Authentisierung

☐ HTTP-Authentisierung

■ 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.

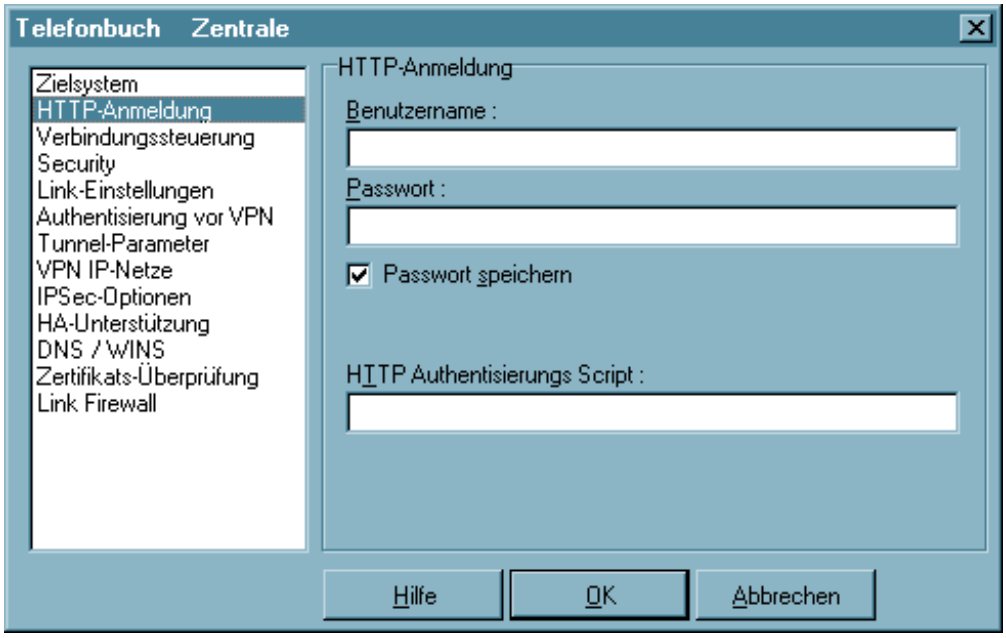
■ HTTP-Authentisierung

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 → nächstes Parameterfeld).

Bei einem Link mit der Verbindungsart WLAN wird die HTTP-Anmeldung im Telefonbuch nicht zugeschaltet! Statt dessen wird mit der Aktivierung dieser Funktion bewirkt, dass für dieses Zielsystem die Authentisierungsdaten aus den WLAN-Einstellungen im Monitor-Menü zum Einsatz kommen.

5.1.8 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:

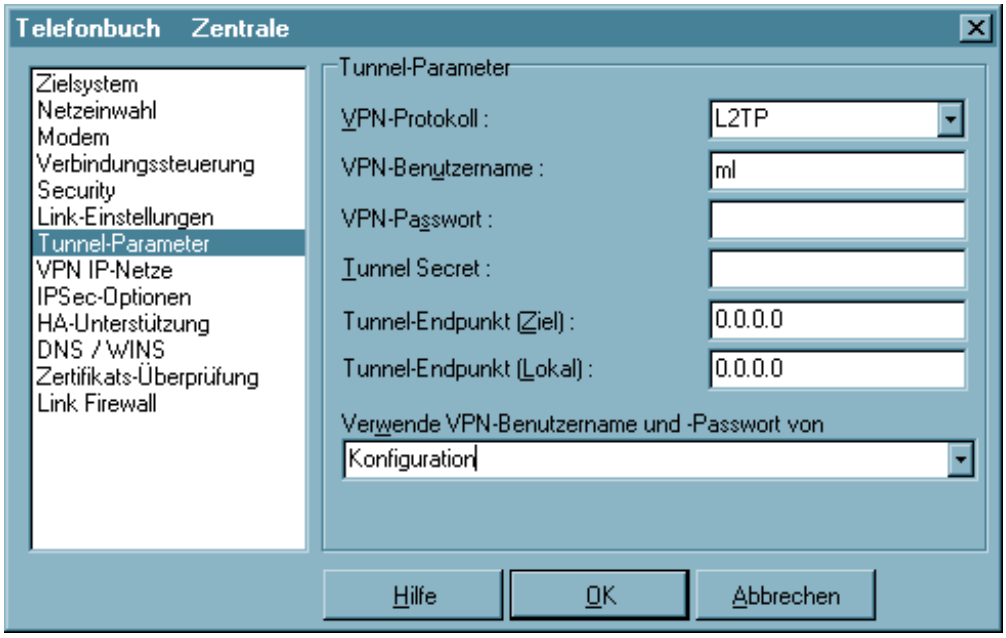
  `CACERTVERIFY_SUBJECT`
  überprüft den Inhalt des Subjects (z.B. cn=WEB Server 1)

  `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.

5.1.9 Tunnel-Parameter



Diese Parameter sind nur von Bedeutung, wenn zwischen dem Client und dem VPN-Gateway ein Tunnel (VPN) aufgebaut werden soll, d.h. das Zielsystem L2TP unterstützt. Die jeweiligen Einstellungen hängen vom Network Access Server des Zielsystems (VPN-Gateway) ab. Wenn Sie unsicher bei der jeweiligen Einstellung sind, wenden Sie sich bitte an Ihren Systemadministrator oder Ihren Internet Service Provider.

Parameter:

- ☐ VPN-Protokoll
- ☐ VPN-Benutzername
- ☐ VPN-Passwort
- ☐ Tunnel Secret
- ☐ Tunnel-Endpunkt (Ziel)
- ☐ Tunnel-Endpunkt (Lokal)
- ☐ Verwende VPN-Benutzername und -Passwort von

■ VPN-Protokoll

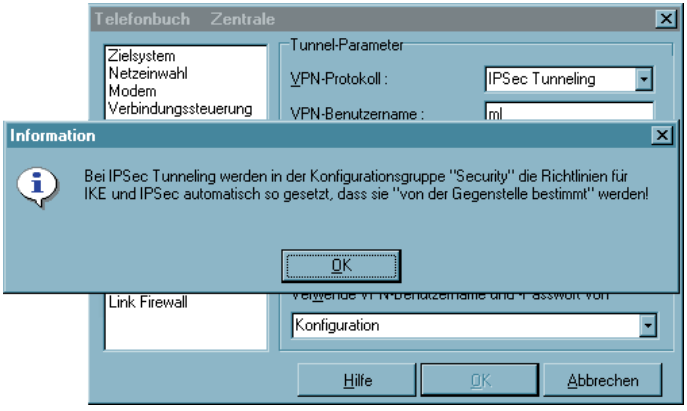
Nicht benutzen = Zwischen dem Client und dem Zielsystem wird kein Tunnel aufgebaut.

L2TP = Mit diesem Schalter bestimmen Sie, ob das L2TP-Protokoll (Layer 2 Tunneling Protokoll) gefahren werden soll. Dieses Protokoll wird für Tunneling über VPN benötigt.

IPSec-Tunneling = Wird das VPN-Protokoll “IPSec-Tunneling” (native IPSec) gewählt, so wird die IPSec-Verbindung ohne einen Layer 2-Tunnel (L2TP) hergestellt.

Verbindung zu IPSec Gateways anderer Hersteller

Bei Auswahl von “IPSec-Tunneling” wird darauf hingewiesen, dass im Konfigurationsfeld “Security” automatisch untenstehende Einstellungen vorgenommen werden:



Security-Modus = IPSec
IKE-Richtlinie = Von Gegenstelle bestimmt
IPSec-Richtlinie = Von Gegenstelle bestimmt
Austausch-Modus = Main Mode

Diese automatisch vorgenommenen Einstellungen können je nach den Anforderungen des fremden IPSec Gateways auch modifiziert werden. Weiterhin ist für den Einsatz von IPSec-Tunneling folgendes zu beachten:

Im Konfigurationsfeld “Security” werden die Parameter “IKE ID-Typ” und “IKE ID” zur Konfiguration eingeblendet (siehe → Security).

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

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

Wird “IPSec-Tunneling” genutzt, so erfolgt die Authentisierung über Extended Authentication (XAUTH Protokoll, Draft 6). Dazu müssen noch folgende Parameter im Konfigurationsfeld “Tunnel-Parameter” gesetzt werden:

VPN-Benutzername = Benutzername des IPSec-Benutzers
VPN-Passwort = Kennwort des IPSec-Benutzers
Verwende VPN-Benutzername und -Passwort von = 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. Der Einsatz von NAT Traversal erfolgt beim IPSec Client automatisch und ist immer nötig, wenn auf Seiten des Zielsystems ein Gerät mit Network Address Translation zum Einsatz kommt.

■ VPN-Benutzername

Ihre User ID, in diesem Fall für das VPN-Gateway, erhalten Sie von Ihrem Systemadministrator. Der Name kann bis zu 256 Zeichen lang sein.

■ VPN-Passwort

Das Passwort, in diesem Fall für das VPN-Gateway, erhalten Sie von Ihrem Systemadministrator. Das Passwort kann bis zu 256 Zeichen lang sein.

■ Tunnel Secret

“Tunnel Secret” ist ein Passwort, das für den Tunnelaufbau benötigt wird. Nur wenn dieses Passwort beim VPN-Gateway und dem VPN-Client übereinstimmt, wird der Tunnel aufgebaut. Das Passwort kann bis zu 16 Zeichen lang sein.

■ Tunnel-Endpunkt (Ziel)

Dies ist die IP-Adresse oder der Name des VPN-Gateways, auch Tunnel Endpoint. Die Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennte Zahlen. Für jede Zahl stehen 8 Bits zur Verfügung, wodurch sie 256 Werte annehmen kann. Sie erhalten die IP-Adresse von Ihrem Administrator.

■ Tunnel-Endpunkt (Lokal)

Dies ist die IP-Adresse des Clients. Die Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennt Zahlen. Für jede Zahl stehen 8 Bits zur Verfügung, wodurch sie 256 Werte annehmen kann. Sie erhalten die IP-Adresse von Ihrem Systemadministrator.

■ Verwende VPN-Benutzername und -Passwort von

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

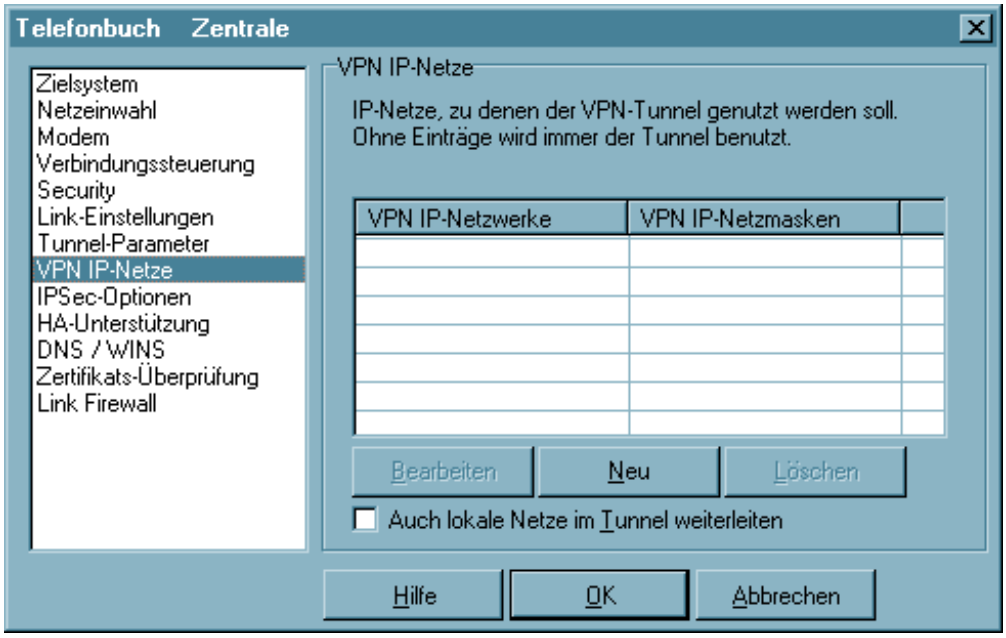
☑ Konfiguration: Dies bedeutet, dass die in diesem Parameterfeld unter “VPN-Benutzername” und ”VPN-Passwort” gemachten Angaben zur VPN-Authentisierung verwendet werden.

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

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

☑ Zertifikat (Seriennummer): Dies bedeutet, dass statt “VPN-Benutzername” und ”VPN-Passwort” die Seriennummer des Zertifikats verwendet wird.

5.1.10 VPN IP-Netze



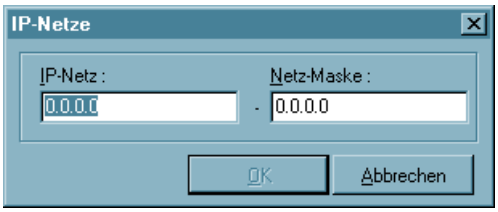
Hier können genau die IP-Netze definiert werden, über die der Client via VPN-Tunnel kommunizieren kann. Wenn Tunneling genutzt wird und hier keine Einträge erfolgen, so wird die Verbindung immer zum Tunnel-Endpunkt des Gateways aufgebaut. Soll alternierend einerseits ein Tunneling zur Zentrale erfolgen, 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:

☐ VPN IP-Netzwerke

☐ VPN IP-Netzmasken

☐ Auch lokale Netze im Tunnel weiterleiten



Klicken Sie auf den Button “Neu”, so können Sie in das daraufhin erscheinende Fenster (links) die IP-Adresse des Netzes und der Netzmaske eintragen.

■ VPN IP-Netzwerke

Hier tragen Sie die Adresse des IP-Netzes ein, das vom Client über das VPN-Gateway erreicht werden soll. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Machen Sie in dieser Liste keinen Eintrag, so werden alle IP-Pakete über den VPN-Tunnel gesendet.

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

■ VPN IP-Netzmasken

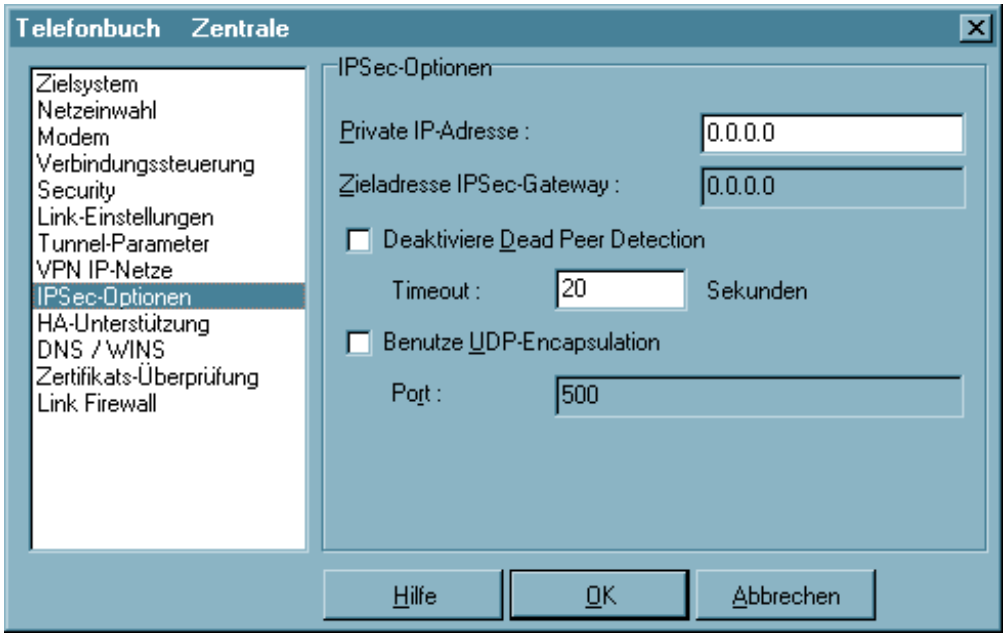
Hier tragen Sie die zugehörige Netzmaske des IP-Netzes ein. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Bitte achten Sie darauf, daß die IP-Adresse des VPN-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 IPSec-Optionen



Die IPSec-Optionen werden benötigt, wenn eine Verbindung von einem NCP Secure Client zu einer nicht NCP-Gegenstelle aufgebaut werden soll.

Parameter:

☐ Private IP-Adresse

☐ Zieladresse IPSec Gateway

☐ Deaktiviere Dead Peer Detection

☐ Benutze UDP-Encapsulaion

Private IP-Adresse

Dies ist die IP-Adresse des Clients, welche im inneren IP-Header des IPSec-Tunnelpaketes als Source Adresse vom Client verwendet wird.

Zieladresse IPSec Gateway

Dies ist die IP-Adresse des IPSec-Gateways der Gegenstelle.

Deaktiviere Dead Peer Detection

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 zu prüfen, ob die Gegenstelle noch aktive ist. Ist dies nicht der Fall erfolgt ein automatischer Verbindungsabbau.

Mit dieser Funktion kann DPD ausgeschaltet oder das DPD-Intervall eingestellt werden. Mit einem größeren Intervall werden weniger häufig Pakete geschickt, die prüfen ob die Gegenstelle noch erreichbar ist.

Benutze UDP-Encapsulation

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.

5.1.12 HA-Unterstützung

Dieses Parameterfeld ist nur von Bedeutung, wenn das Zielsystem ein HA-Server (High Availability) ist, der das Tunnelaufkommen je nach Konfiguration an VPN-Gateways weiterleitet. Außerdem erscheint das Parameterfeld nur im Telefonbuch, wenn ein VPN-Protokoll für die Verbindung zum Zielsystem selektiert wurde.

Ein DVE (Dynamic VPN Endpoint) kann zum Lastausgleich (Loadbalancing) oder zur Ausfallsicherung (Backup) eines Virtual Private Networks mit zwei VPN-Gateways genutzt werden. Mit DVE wird, je nach Konfiguration im HA-Manager des Zielsystems, sichergestellt, dass kein Engpass beim Tunnelaufbau auftritt. Je nach Lastaufkommen wird vom HA-Server zum Tunnelaufbau zwischen den Tunnel-Endpunkten der VPN-Gateways gewechselt. (siehe → Beispiele und Erklärungen).

Parameter:

☐ Aktivierung

☐ Erster / Zweiter HA-Server

☐ DVE Secret

☐ Zuletzt zugewiesenes Gateway benutzen

Aktivierung

Mit diesem Parameter wird die DVE-Funktionalität eingechaltet (Dynamic Virtual Endpoint). Im Parameterfeld “Tunnel-Parameter” wird daraufhin die ”Tunnel IP-Adresse (Ziel)” ausgeblendet. Stattdessen muss die IP-Adresse des HA-Servers (siehe →Erster / Zweiter HA-Server) angegeben werden. Dieser HA-Server führt den Tunnel dann je nach Konfiguration weiter an eines der VPN-Gateways.

Erster / Zweiter HA-Server

Hier tragen Sie die IP-Adresse der HA-Server ein. Die Adresse erhalten Sie von Ihrem System-Administrator.

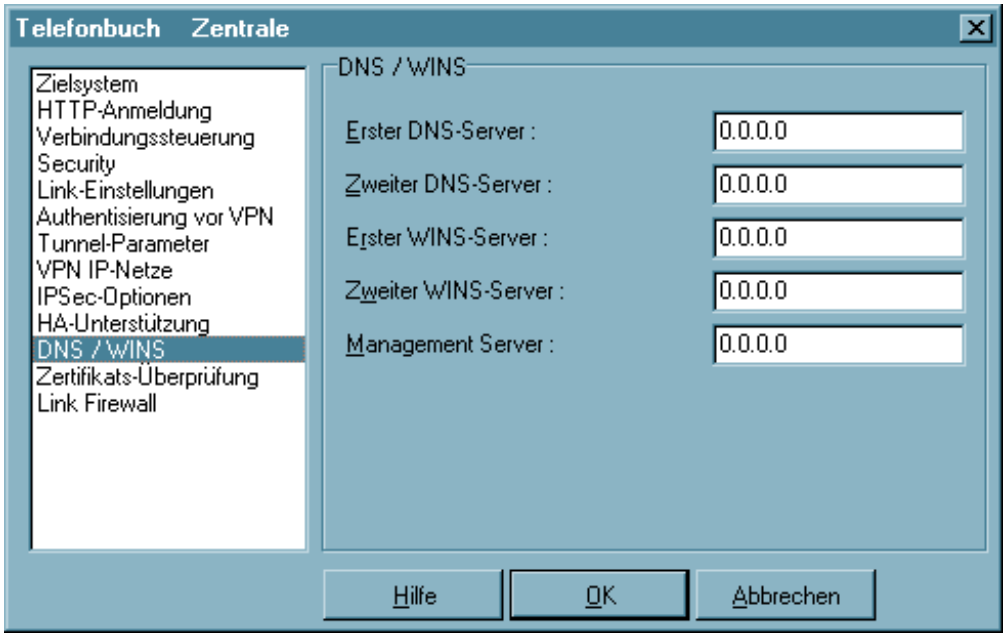
DVE Secret

Hier tragen Sie das Passwort für die Verbindung des DVE-Clients zum Zielsystem (DVE-Server) ein. Sie erhalten es von Ihrem System-Administrator.

Zuletzt zugewiesenes Gateway benutzen

Ist im Gateway die Option “IP-Adressen aus Pool” gewählt und wird ein HA-Server mit Load Balancing verwendet, sollte der Client immer zu dem Gateway verbunden werden, aus dessen IP-Pool er seine IP-Adresse erhalten hat. Um dies zu gewährleisten, aktivieren Sie diese Funktion.

5.1.13 DNS / WINS



In diesem Parameterfenster 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:

☐ DNS-Server

☐ WINS-Sever

☐ Management Server

DNS-Server

erster/zweiter DNS-Server: Der zuerst eingetragene DNS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt. Der zweite DNS-Server dient als Backup-DNS-Server.

WINS-Server

erster/zweiter WINS-Server: Der zuerst eingetragene WINS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt. Der zweite WINS-Server dient als Backup-WINS-Server.

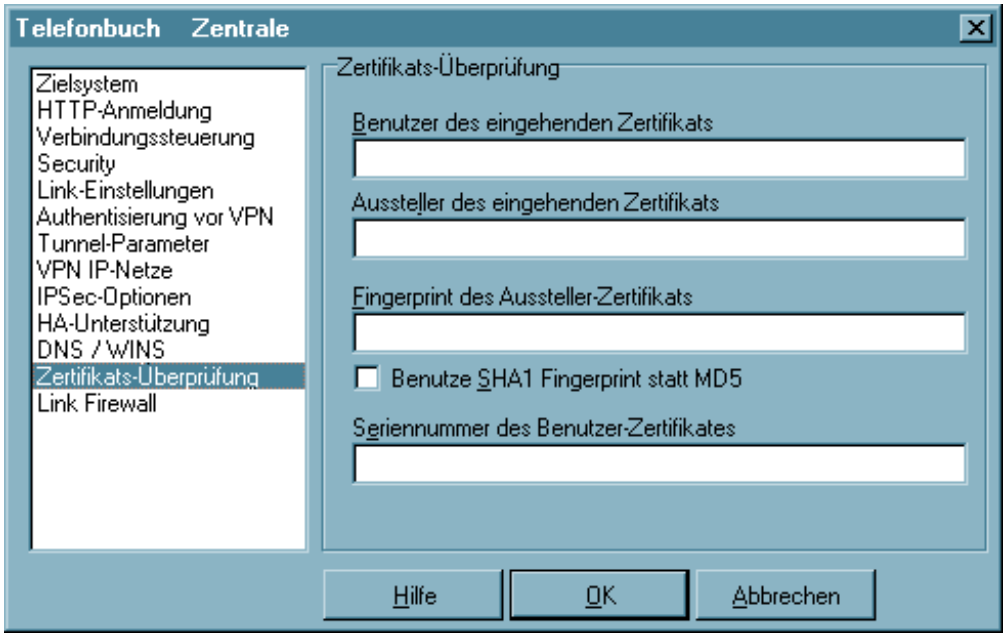
Hinweis: Je nach Anwendung können Sie ein oder zwei DNS- oder WINS-Server eintragen. Genutzt wird immer der jeweils erste. Wird kein alternativer Server eingetragen, wird der Server genutzt, der über PPP zugewiesen wird.

Management Server

Die IP-Adresse des NCP Management Servers muss hier eingetragen werden, wenn das Gateway der Gegenstelle kein NCP-Gateway ist und somit kein NCP Management-Server automatisch über die PPP-Verhandlung bekannt gegeben werden kann.

Wird die IP-Adresse eines Management Servers eingetragen, obwohl die Gegenstelle ein NCP-Gateway ist, so wird unabhängig von der eingetragenen IP-Adresse der Management-Server des NCP Secure Enterprise Managements genutzt, welcher bei der PPP-Verhandlung zwischen NCP-Gateway und NCP Secure Client bekannt gegeben wird. Die eingetragene IP-Adresse wird in diesem Fall ignoriert.

5.1.14 Zertifikats-Überprüfung



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

(Siehe auch → Beispiele und Erklärungen, Zertifikats-Überprüfungen)

Parameter:

☐ Benutzer des eingehenden Zertifikats

☐ Aussteller des eingehenden Zertifikats

☐ Fingerprint des Aussteller-Zertifikats

☐ Benutze SHA1 Fingerprint statt MD5

☐ Seriennummer des Benutzer-Zertifikats

■ 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. Sie 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=NCP, 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 NCP 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. Sie 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=NCP engineering 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.

■ Benutze SHA1 Fingerprint statt MD5

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

■ Seriennummer des Benutzer-Zertifikates

In dieses Feld kann die Seriennummer der Benutzer-Zertifikats in Hexadezimalwerten (mit Doppelpunkt getrennt) eingetragen werden.

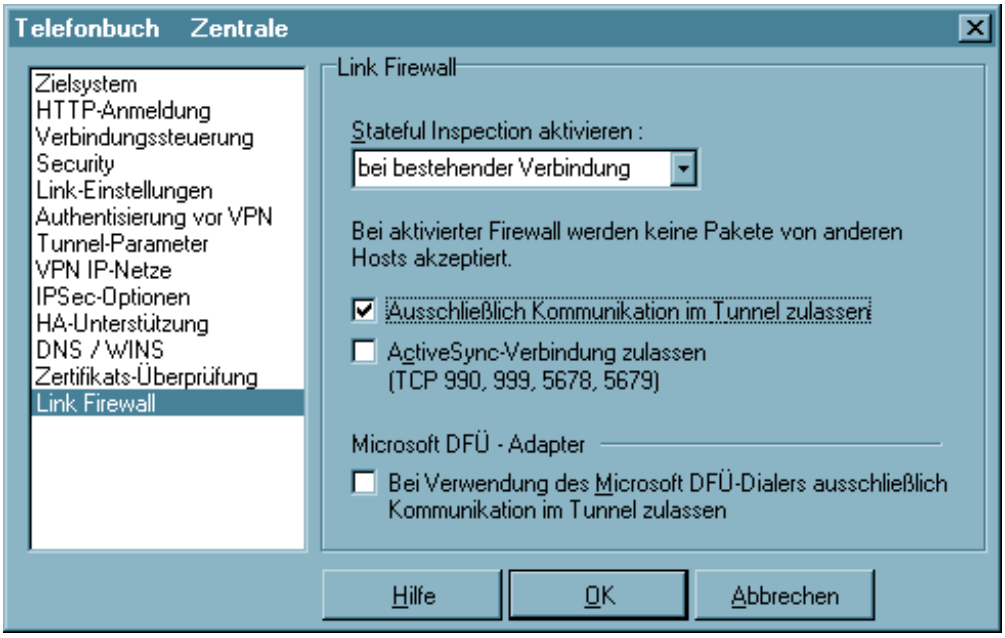
☐ Stimmt dieser Wert mit der Seriennummer des verwendeten Zertifikats überein, wird die Verbindung zur Gegenstelle aufgebaut.

☐ Stimmt dieser Wert nicht mit der Seriennummer des verwendeten Zertifikats überein, wird die Verbindung abgebrochen und eine entsprechende Meldung in die Log-Datei geschrieben.

☐ Benötigt die Gegenstelle kein Zertifikat, wird der Eintrag ignoriert.

☐ Werden Telefonbücher automatisch vom Administrator verteilt, und verwenden die Benutzer Zertifikate mit fortlaufender Seriennummer, so können die unterschiedlichen Zähler in den Seriennummern der Benutzer-Zertifikate mit einem Stern (*) als Wildcard ersetzt werden, sodass nicht einzelne Telefonbücher für die Benutzer ausgegeben werden müssen, z.B.: 00:02:07:04:*

5.1.15 Link Firewall



Die Einstellungen der Link Firewall gelten nur für dieses Zielsystem und können für alle Netzwerkadapter wie auch für RAS-Verbindungen genutzt werden.

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 → Beispiele und Erklärungen).

■ 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

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.

- **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.

  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.

Diese Seite ist frei

5.2 IPSec

Die Parameter zu IPSec, einschließlich der zur Konfiguration einer "statischen" Secure Policy Database benötigten, sind in drei Zweige des Konfigurationsbaums unterteilt:

IKE-Richtlinie

IPSec-Richtlinie

SPD Secure Policy Database

Richtlinien | IPSec

Parameterfelder:

1 ***IKE-Richtlinie (Phase-1-Parameter) (5.2.1)***

2 ***IPSec-Richtlinie (Phase-2-Parameter) (5.2.2)***

Die Richtlinien (IKE- / IPSec-Richtlinie) werden in jeder IPSec-Konfiguration benötigt. Das heißt, sie müssen sowohl bei Verwendung einer statischen Secure Policy Database (SPD) als auch bei Verwendung einer dynamischen SPD konfiguriert werden.

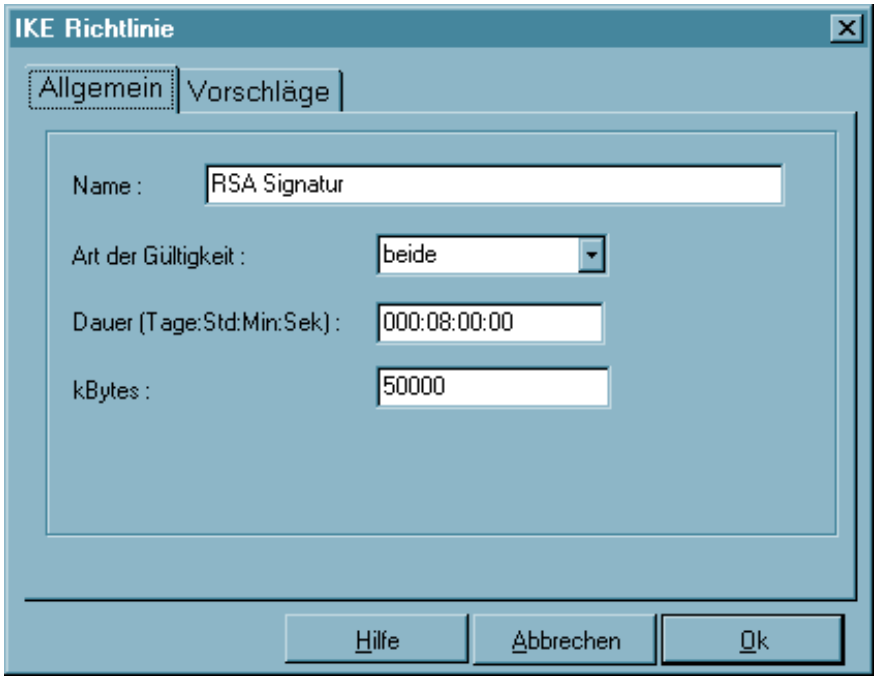
Nach der Maßgabe der IKE-Richtlinie wird die Authentisierungsverhandlung zwischen IPSec-Initiator und Gegenstelle durchgeführt und ein verschlüsselter Kontrollkanal zwischen ihnen hergestellt.

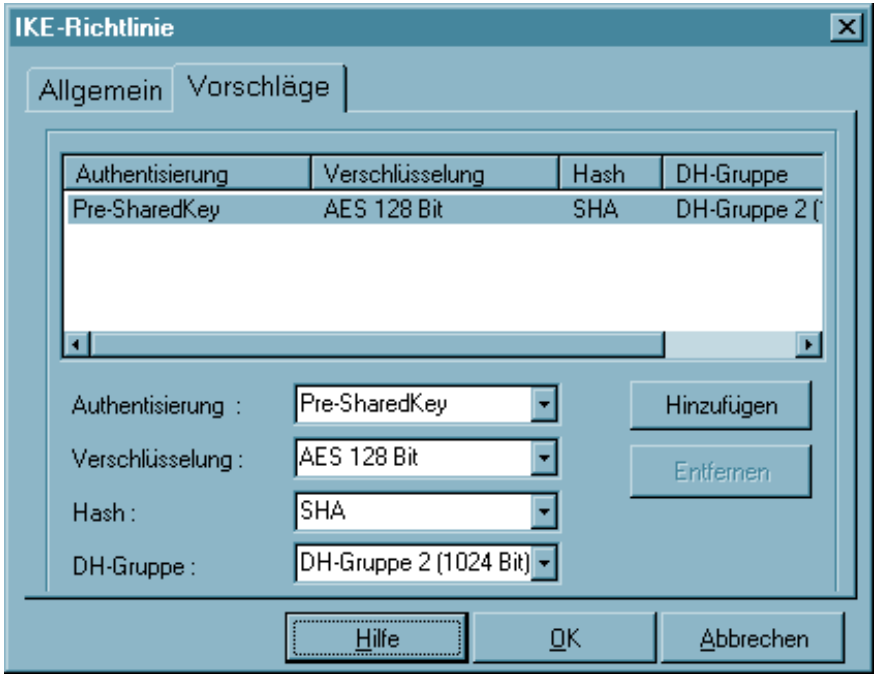
Nach der Maßgabe der IPSec-Richtlinie wird festgelegt, wie die Nutz-Daten gemäß IPSec bearbeitet werden sollen.

Einzelne Parameterfelder oder Parameter, die Sie für Ihre Arbeit mit dem Client nicht benötigen, können von Ihrem Systemadministrator ausgeblendet worden sein.

Bitte beachten Sie zur IPSec-Konfiguration unbedingt die Hinweise im Abschnitt "Beispiele und Erklärungen" unter "Security" in diesem Handbuch.

5.2.1 IKE-Richtlinie (Allgemein / Vorschläge)





Die Parameter in diesen Feldern beziehen sich auf die Phase 1 des Internet Key Exchange (IKE) mit dem der Kontrollkanal für die SA-Verhandlung aufgebaut wird (siehe → Beispiele und Erklärungen, IKE-Modi). Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in den Parameterfeldern "Security" im Telefonbuch (für eine dynamische SPD) und unter "Secure Policy Database" (für eine statische SPD.)

Die IKE-Richtlinien, die Sie hier konfigurieren, werden zur Auswahl für die SPD gelistet.

Sofern IPSec für Remote Access eingesetzt wird, ordnen sie eine der IKE-Richtlinien im Parameterfeld "Security" im Telefonbuch für eine dynamisch aufgebaute SPD dem jeweiligen Zielsystem zu.

Die IKE-Richtlinie gilt für eine statische SPD, wenn sie in der Verzweigung der IPSec-Parameter unter "Secure Policy Database" für eine statische SPD im Parameterfeld "Security" selektiert wurde.

Funktional unterscheiden sich zwei IKE-Richtlinien, die standardmäßig vorkonfiguriert mit der Software ausgeliefert werden (siehe → Beispiele und Erklärungen, IPSec, IKE-Modi) als "Preshared 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 → IPSec, IKE-Richtlinie, Authentisierung, Verschlüsselung), 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.

Parameter (Allgemein):

☐ Name | IKE-Richtlinie

☐ Art der Gültigkeit | IKE-Richtlinie

☐ Dauer | IKE-Richtlinie

☐ kBytes | IKE-Richtlinie

Parameter (Vorschläge):

☐ Authentisierung | IKE-Richtlinie

☐ Verschlüsselung | IKE-Richtlinie

☐ Hash | IKE-Richtlinie

☐ DH-Gruppe | IKE-Richtlinie

Name | IKE-Richtlinie

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

Art der Gültigkeit | IKE-Richtlinie

Bestimmt nach welchen Kriterien die Art der Schlüsselgültigkeit festgelegt wird, nach Dauer, nach übertragenen kBytes oder nach beiden. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt.

Dauer | IKE-Richtlinie

Die Menge der kBytes oder die Größe der Zeitspanne kann eigens eingestellt werden.

kBytes | IKE-Richtlinie

Die Menge der kBytes oder die Größe der Zeitspanne kann eigens eingestellt werden.

Authentisierung | IKE-Richtlinie

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

Werden mehrere Vorschläge mit unterschiedlichen Verschlüsselungen eingetragen, so werden alle Vorschläge der Reihe nach ausgewertet.

Preshared Key = Zur gegenseitigen Authentisierung wird ein (allen) gemeinsamer statischer Schlüssel verwendet. Diesen Schlüssel definieren Sie in den Security-Parameterfeldern (siehe → Telefonbuch, Security bzw. IPSec, Secure Policy Database, Security).

RSA Signature = Zur gegenseitigen Authentisierung wird das Zertifikat verwendet, das Sie für die “Erweiterte Authentisierung” konfiguriert haben (siehe → Verbindung, Benutzer-Zertifikat). Im Main Mode wird das Zertifikat zusätzlich verschlüsselt (siehe → Beispiele und Erklärungen, IKE-Modi). Dies ist nur mit PKI-Unterstützung des Systems möglich (Secure Server).

Verschlüsselung | IKE-Richtlinie

Nach einem der optionalen Verschlüsselungsalgorithmen erfolgt die symmetrische Verschlüsselung der Messages 5 und 6 im Kontrollkanal (siehe → Beispiele und Erklärungen, IKE-Modi), 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

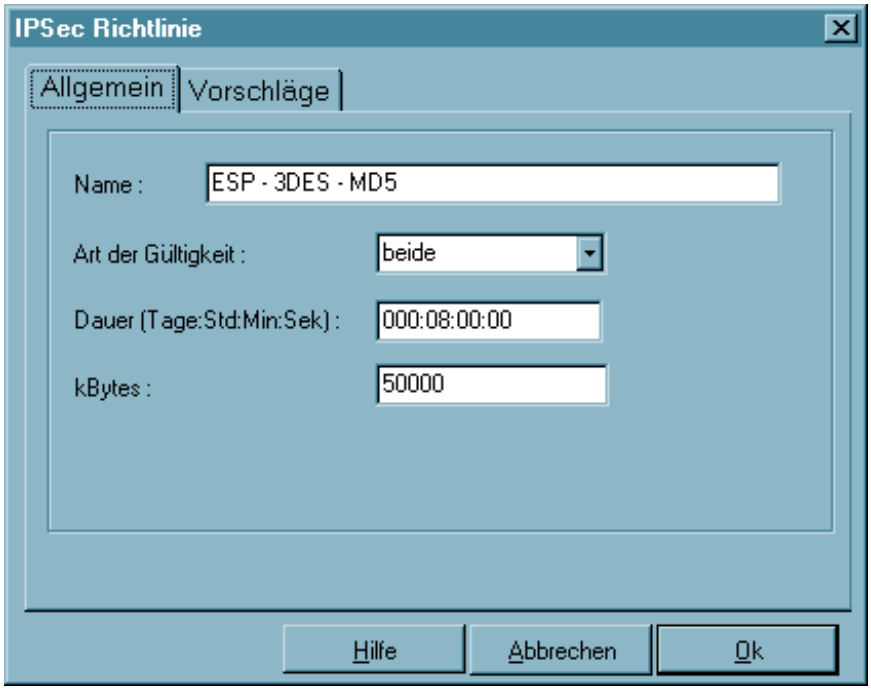
Modus, wie der Hash-Wert über die ID bzw. das Zertifikat der Messages im Kontrollkanal gebildet wird (siehe → Beispiele und Erklärungen, IKE-Modi).

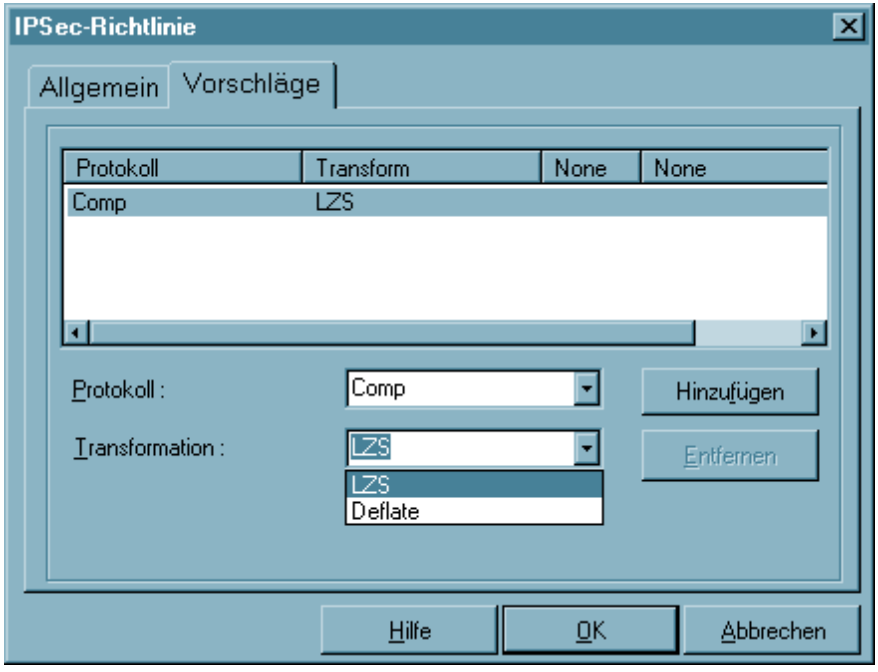
Zur Wahl stehen: MD5 (Message Digest, Version 5) und SHA (Secure Hash Alogrithm).

DH-Gruppe | IKE-Richtlinie

Mit der Wahl einer der angebotenen Diffie-Hellmann-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.

5.2.2 IPSec-Richtlinie (Allgemein / Vorschläge)





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

Sofern IPSec für Remote Access eingesetzt wird, ordnen sie eine der IPSec-Richtlinien im Parameterfeld "Security" im Telefonbuch für eine dynamisch aufgebaute SPD dem jeweiligen Zielsystem zu.

Die IPSec-Richtlinie gilt für eine statische SPD, wenn sie unter den IPSec-Parametern in der Verzweigung "Secure Policy Database" im Parameterfeld "Security" selektiert wurde.

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 eine IPSec-Richtlinie mit ESP-Protokoll standardmäßig vorkonfiguriert mit der Software ausgeliefert (siehe → Beispiele und Erklärungen, IPSec, AH und ESP).

Inhalt und Name dieser Richtlinie können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu IPSec-Protokoll und Authentisierung 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.

Parameter (Allgemein):

☐ Name | IPSec-Richtlinie

☐ Art der Gültigkeit | IPSec-Richtlinie

☐ Dauer | IPSec-Richtlinie

☐ kBytes | IPSec-Richtlinie

Parameter (Vorschläge):

☐ Protokoll | IPSec-Richtlinie

☐ Transformation (ESP) | IPSec-Richtlinie

☐ Transformation (Comp) | IPSec-Richtlinie

☐ Authentisierung (nur ESP) | IPSec-Richtlinie

Name | IPSec-Richtlinie

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

Art der Gültigkeit | IPSec-Richtlinie

Bestimmt nach welchen Kriterien die Art der Schlüsselgültigkeit festgelegt wird, nach Dauer, nach übertragenen kBytes oder nach beiden. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt.

Dauer | IPSec-Richtlinie

Dauer und kBytes können eigens festgelegt werden.

kBytes | IPSec-Richtlinie

Dauer und kBytes können eigens festgelegt werden.

Protokoll | IPSec-Richtlinie

Die IPSec-Richtlinien sind im Wesentlichen nach den beiden Sicherheitsprotokollen unterschieden, AH oder ESP, die sich im Tunnelmodus gegenseitig ausschließen. Standard ist ESP.

Transformation (ESP) | 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 (nur ESP) | IPSec-Richtlinie

Für das Sicherheitsprotokoll ESP kann der Modus der Authentisierung eigens eingestellt werden.

Zur Wahl stehen: MD5 und SHA.

DH-Gruppe | IPSec-Richtlinie

Mit der Wahl einer der angebotenen Diffie-Hellmann-Gruppen wird festgelegt, dass zusätzlich in Phase 2 mit der SA-Verhandlung ein kompletter Schlüsselaustausch (PFS) stattfinden soll. Standard ist inaktiv.

Secure Policy Database | IPSec

In dieser Verzweigung des Konfigurationsbaums können die statischen SPDs konfiguriert werden. Die Verzweigung ist wie folgt unterteilt.

Parameterfelder:

3 ***Allgemein | SPD (5.2.3)***

4 ***Selektoren | SPD (5.2.4)***

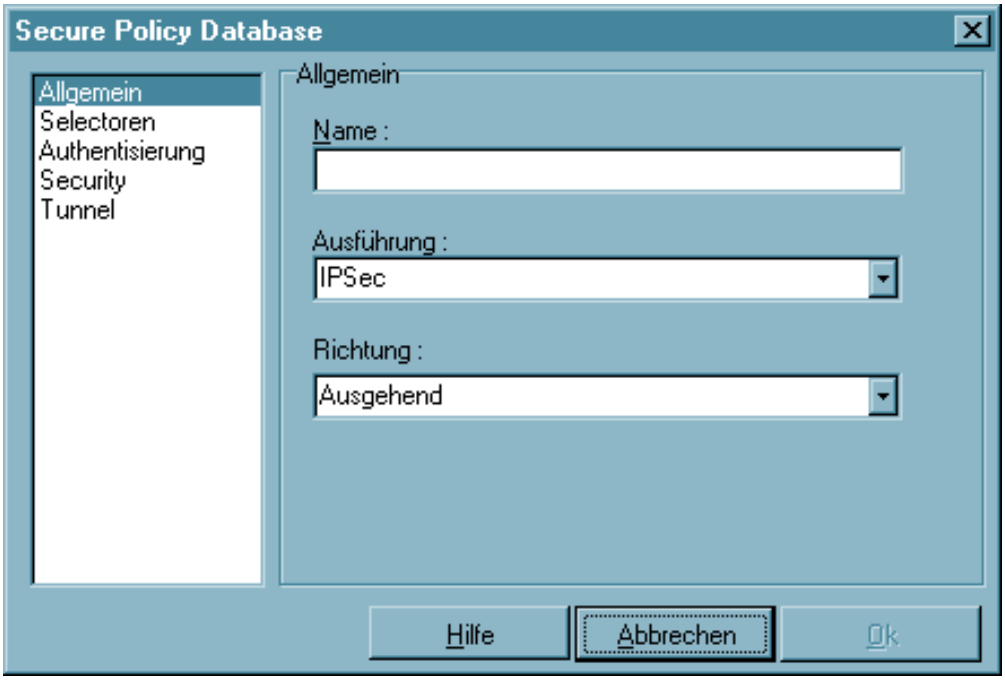
5 ***Authentisierung | SPD (5.2.5)***

6 ***Security | SPD (5.2.6)***

7 ***Tunnel | SPD (5.2.7)***

Bitte beachten Sie zur IPSec-Konfiguration unbedingt die Hinweise im Abschnitt “Beispiele und Erklärungen” unter “Security” in diesem Handbuch.

5.2.3 Allgemein | SPD



In diesem Parameterfeld werden allgemeine Parameter zur Secure Policy Database konfiguriert.

Parameter:

☐ Name | SPD

☐ Ausführung | SPD

☐ Richtung | SPD

Name | SPD

Geben Sie dieser Secure Policy Database einen eindeutigen Namen.

Ausführung | SPD

IPSec (IPSec) → für die IP-Pakete mit Adressen aus dem definierten Bereich werden die IPSec-Sicherheitsdienste angewendet, die SPD-Filtertabelle kommt zum Einsatz

gestatten (permit) → die IP-Pakete mit Adressen aus dem definierten Bereich werden durchgelassen, ohne dass die SPD zum Einsatz kommt

sperren (deny) → alle IP-Pakete mit Adressen aus dem definierten Bereich werden weggeworfen

inaktiv (disabled) → diese SPD wird ausgeschaltet und kommt für IPSec nicht zum Einsatz, ohne dass sie gelöscht werden muss

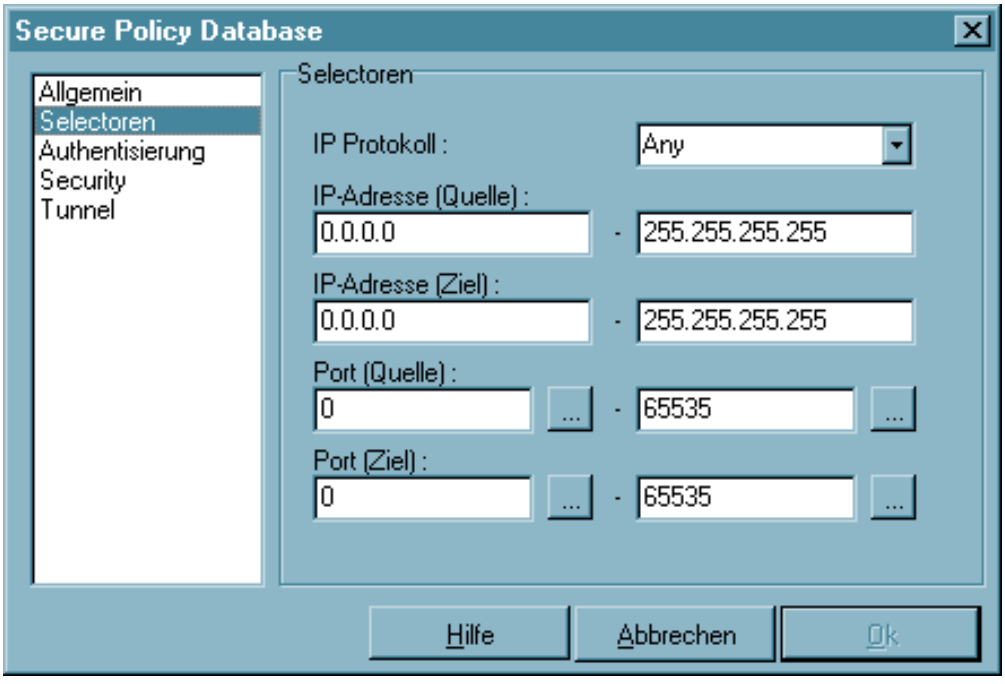
Richtung | SPD

eingehend = Sie stellen auf “eingehend” wenn der Aufbau des Kontrollkanals und die IKE-Verhandlung (siehe → Beispiele und Erklärungen, IKE-Modi) von der Gegenstelle aus eingeleitet wird.

ausgehend = Der Aufbau des Kontrollkanals und die IKE-Verhandlung (siehe → Beispiele und Erklärungen, IKE-Modi) wird von dieser Stelle aus eingeleitet. Auf der Gegenseite muss der Aufbau des Kontrollkanals zugelassen werden, bzw. “eingehend” konfiguriert sein.

Beim Client ist standardmäßig “ausgehend” eingestellt, so dass bei Kommunikation (mit statischer SPD) am Server auf “eingehend” eingestellt werden muss.

5.2.4 Selektoren | SPD



Der Selektor oder Filterteil des SPD-Eintrags besteht aus IP- und Port-Adressen. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des SPD-Eintrags übereinstimmen, wird im Status festgelegt, wie mit diesem IP-Paket weiter zu verfahren ist.

Parameter:

☐ IP-Protokoll | SPD

☐ IP-Adresse (Quelle) | SPD

☐ IP-Adresse (Ziel) | SPD

☐ Port (Quelle) | SPD

☐ Port (Ziel) | SPD

IP-Protokoll | SPD

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) | SPD

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) | SPD

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).

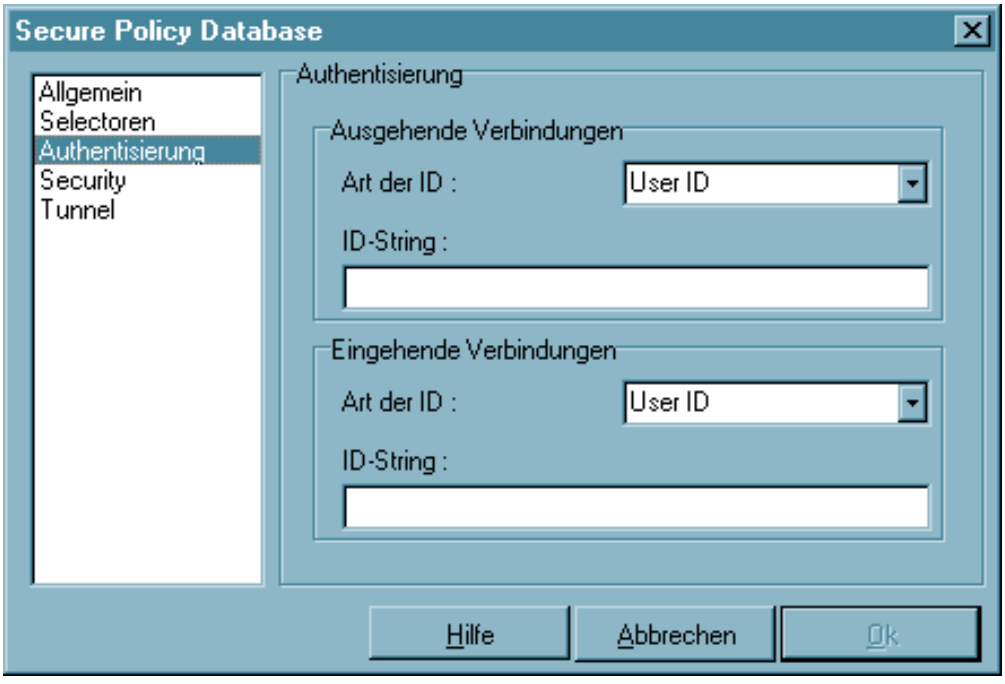
Port (Quelle) | SPD

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) | SPD

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

5.2.5 Authentisierung | SPD



ID, die zum Aufbau des Kontrollkanals (Main Mode Message 5,6 und Aggressive Mode Message 2) benötigt wird (bei statischer SPD).

(Bei dynamischer SPD wird automatisch die gleiche ID verwendet, die auch beim Layer 2-Tunnelaufbau verwendet wird.)

Parameter:

☐ Art der ID (Ausgehende Verbindung / Eingehende Verbindung) | SPD

☐ ID String (Ausgehende Verbindung / Eingehende Verbindung) | SPD

■ Art der ID (Ausgehende Verbindung / Eingehende Verbindung) | SPD

Bei IPSec wird für eingehende und ausgehende Verbindungen unterschieden.

Was der Sender als ID für ausgehende Verbindung gewählt hat, muss der Empfänger als ID für eingehende Verbindung wählen.

Folgende Arten der ID stehen zur Verfügung:

☐ IP Address

☐ Domain Name

☐ User ID

☐ Subnet ID

☐ IP Address Range

☐ X.500 Distinguished Name

☐ X.500 General Name

☐ Key ID

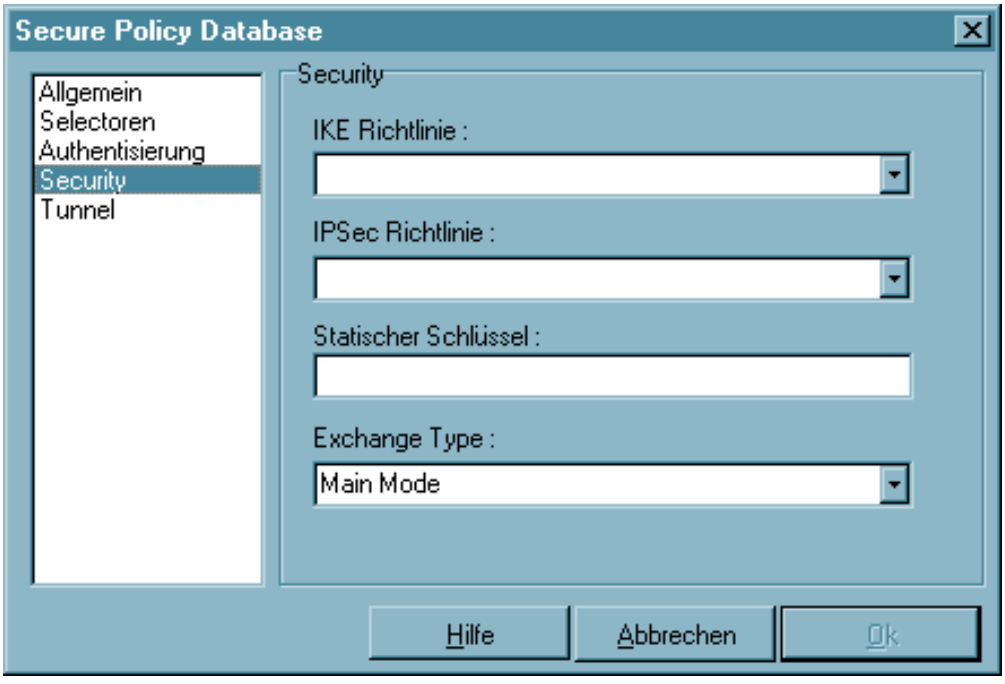
■ ID String (Ausgehende Verbindung / Eingehende Verbindung) | SPD

Bei IPSec wird für eingehende und ausgehende Verbindungen unterschieden.

Was der Sender als ID für ausgehende Verbindung gewählt hat, muss der Empfänger als ID für eingehende Verbindung wählen.

Je nach gewählter Art der ID, muss in dieses Feld die zugehörige Zeichenfolge bzw. der Adressbereich (mit Minus “-”) eingegeben werden.

5.2.6 Security | SPD



In diesem Feld wählen Sie die vorkonfigurierten Richtlinien aus und setzen die zugehörigen Parameter.

Parameter:

☐ IKE-Richtlinie | SPD

☐ IPSec-Richtlinie | SPD

☐ Statischer Schlüssel | SPD

☐ Austausch-Modus | SPD

IKE-Richtlinie | SPD

Sie wählen aus der Listbox der vorkonfigurierten IKE-Richtlinien diejenige aus, nach der der Kontrollkanal (siehe → IKE-Modi) aufgebaut werden soll.

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

Funktional unterscheiden sich zwei IKE-Richtlinien, die standardmäßig vorkonfiguriert mit der Software ausgeliefert werden (siehe → Beispiele und Erklärungen, IPSec, IKE-Modi). Sie finden sie im Konfigurationsbaum unter der Verzweigung “IPSec - IKE-Richtlinie” als “Preshared Key” und “RSA-Signatur”.

Die IKE-Richtlinien werden im Konfigurationsbaum unter dem Zweig “IPSec - IKE-Richtlinie” vorkonfiguriert.

IPSec-Richtlinie | SPD

Sie wählen aus der Listbox der vorkonfigurierten IPSec-Richtlinien (siehe → IPSec, IPSec-Richtlinie) diejenige aus, nach der in der Phase 2 die Datenverschlüsselung erfolgen soll.

In der Listbox werden die IPSec-Richtlinien aufgeführt. Sie 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 eine IPSec-Richtlinie mit ESP-Protokoll standardmäßig vorkonfiguriert mit der Software ausgeliefert (siehe → Beispiele und Erklärungen, IPSec, AH und ESP).

Die IPSec-Richtlinien werden im Konfigurationsbaum unter dem Zweig “IPSec - IPSec-Richtlinie” vorkonfiguriert.

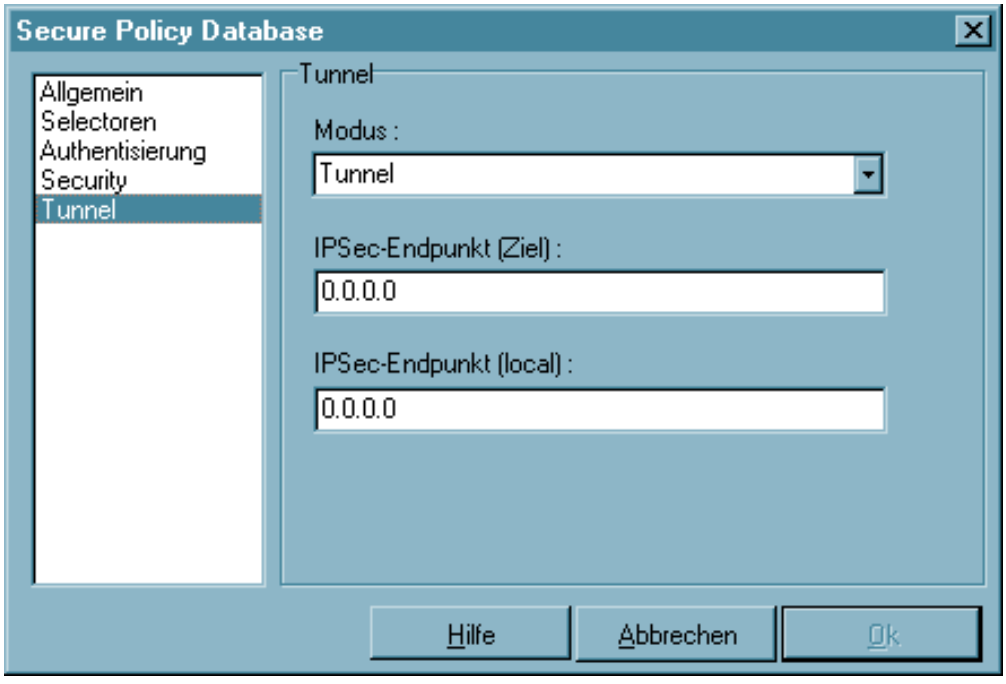
Statischer Schlüssel | SPD

Ein statischer Schlüssel kann zur Authentisierung in der IKE-Verhandlung verwendet werden (siehe → IKE-Richtlinie, Authentisierung, Preshared Key). An beiden Endpunkten der Kommunikation muss der gleiche statische Schlüssel verwendet werden. (Der statische Schlüssel für eine dynamische SPD wird unter “Telefonbuch, Security, Statischer Schlüssel” eingegeben.)

■ Austausch-Modus | SPD

Der Internet Key Exchange kann 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 (siehe → Beispiele und Erklärungen, IKE-Modi).

5.2.7 Tunnel | SPD



In diesem Parameterfeld werden die Betriebsart und die IP-Adressen der Endpunkte der IP-Sec-Kommunikation festgelegt.

Parameter:

☐ Modus | SPD

☐ IPSec-Endpunkt (Ziel) | SPD

☐ IPSec-Endpunkt (lokal) | SPD

■ Modus | SPD

Hier bestimmen Sie den IPSec-Betriebsmodus (siehe auch → Erklärungen und Beispiele, AH und ESP im Transport- und Tunnelmodus).

Transport	=	Der Transportmodus eignet sich nur für eine direkte Kommunikation zwischen zwei Hosts mit festen IP-Adressen oder zwischen Arbeitsplatzrechnern im LAN. (Dieser Modus ist für Remote Access ungeeignet.)
Tunnel	=	Im Tunnelmodus wird das gesamte IP-Paket mit einem neuen IP Header versehen. Das IP-Paket wird auf diese Weise durch einen Layer 3-Tunnel geschickt. Der innere IP Header mit Original-Adressen ist dabei versteckt und kann nicht eingesehen werden - nur die (Layer 3-) Tunnelendpunkte sind erkennbar. Rechner in Netzen hinter Firewalls oder Routern mit IPSec können in diesem Modus sicher miteinander kommunizieren.

■ IPSec-Endpunkt (Ziel) | SPD

Hier geben Sie die IP-Adresse des Endpunkts der IPSec-Kommunikation ein. Der “IPSec-Endpunkt (Ziel)” muss der lokalen IP-Adresse der Gegenstelle entsprechen und umgekehrt.

■ IPSec-Endpunkt (lokal) | SPD

Hier geben Sie die IP-Adresse des Endpunkts der IPSec-Kommunikation ein. Der “IPSec-Endpunkt (Ziel)” muss der lokalen IP-Adresse der Gegenstelle entsprechen und umgekehrt.

Frei für Notizen →

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:

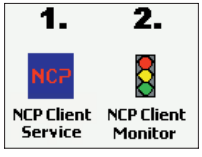
Aus dem Startmenü wählen Sie →
Einstellungen, danach →
Verbindungen, danach nochmals →
Verbindungen, dann →
Wahlparameter und schließlich →
Wählmuster (siehe Bild rechts)

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).

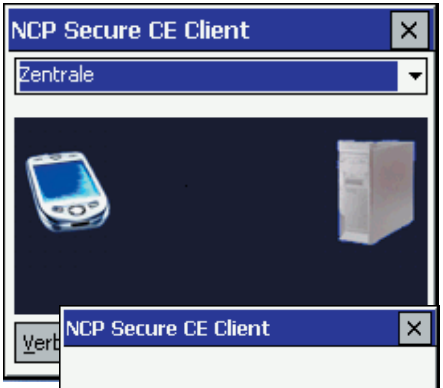


Vergessen Sie außerdem nicht die Smart Card einzustecken bzw. den Reader zu initialisieren, wenn Sie PKI mit Smart Cardsnutzen! In diesem Fall muss nach dem Start des Monitors ein Smart Card-Symbol dargestellt werden (siehe Bild rechts)

6.4 Verbinden

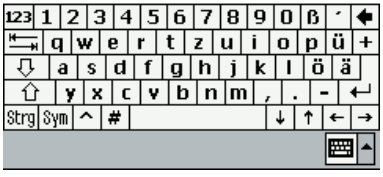
Gleich in welcher Art die Verbindung aufgebaut wird, der Monitor, sofern er im Vordergrund sichtbar ist, zeigt immer den Status des Verbindungsaufbaus wie in folgendem Beispiel an:

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 wesentliche Grundbegriffe des Routings erklärt. Anhand von Beispielen wird die Konfiguration des Secure 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

Dieser Abschnitt beschreibt die Besonderheiten der Security-Verfahren L2Sec und IPSec und dient der grundlegenden Erläuterung der Konfigurationsparameter zu diesen beiden Verfahren.

Im Parameterfeld “Security” des Telefonbuchs sind die Konfigurationsparameter zu L2Sec und IPSec für den Einsatz in Remote Access-Umgebungen gesammelt. Sofern IPSec für Remote Access eingesetzt wird, wird die Secure Policy Database (SPD) dynamisch nach Vorgabe der Parameter im Feld “Security” aufgebaut (siehe unten →IPSec für Remote Access, IPSec over L2TP). In diesem Fall wird eine statische SPD-Konfiguration nicht benötigt!

Bei ausgehendem IP-Verkehr mit IPSec werden vom Secure Client zuerst die statischen SPDs abgearbeitet, die im Konfigurationsbaum im Zweig “IPSec” unter der Rubrik “Secure Policy Database” angelegt wurden. Nur wenn keine dieser statischen SPDs zum Einsatz kommt, wird eine dynamische SPD aufgebaut.

Statische SPDs werden nur für IP-Verbindungen zu anderen Access Servern benötigt, die nicht L2Sec unterstützen. Ansonsten kann ihr Status auf “inaktiv” gesetzt werden (siehe unten →Sicherheits-Richtlinien von IPSec).

7.2.1 Verschlüsselungsart L2Sec nach RFC 2716

Die Praxis zeigt, dass es in VPN-Projekten gilt, einerseits eine sehr große Anzahl von verteilten PC-Arbeitsplätzen an die Firmenzentrale anzubinden und andererseits neben IP- auch IPX-, SNA- und NetBios-Datenpakete (native) zu übertragen sind.

Wichtig für die Sicherheit einzurichtender Kommunikationsnetze ist in besonderem Maße eine angemessene Authentisierung der Kommunikationsteilnehmer – bereits während des Verbindungsaufbaus. Dies ist umso vorrangiger, je mehr sich Mitarbeiter vom Telearbeitsplatz oder vom mobilen Büro über das Internet oder andere öffentliche Netze in das Datennetz des Unternehmens einwählen.

Ohne Zweifel hat IPSec seine Berechtigung, aber der aktuelle Entwicklungsstand hat sogar einige seiner Initiatoren gezwungen, proprietäre Derivate zu implementieren, um einige seiner immanenten Schwächen zu überwinden (siehe unten →IPSec für Remote Access). So wird bei IPSec etwa vorausgesetzt, dass die Verbindung bereits steht, bevor die Sicherheits-Verhandlung beginnt.

NCP hat L2Sec (siehe →Konfiguration,Telefonbuch, Security, Verschlüsselungsart (L2Sec)) implementiert, um die Schwächen von IPSec auszuschalten und gleichzeitig den Anforderungen der Unternehmen hinsichtlich offener Standards nachzukommen. L2Sec gilt sowohl vom Standpunkt der Sicherheit als auch der Kommunikation als einzige echte Alternative zu IPSec. L2Sec vereint die Vorteile von L2TP mit Authentisierung und Verschlüsselung nach SSL (TLS). Dieses Verfahren ist im RFC 2716 (Microsoft) niedergelegt. NCP war nicht nur der erste Hersteller, der L2Sec implementiert hatte, lange bevor der RFC veröffentlicht wurde, sondern hat heute bereits auf die Bedürfnisse zahlreicher Großunternehmen, Organisationen und Behörden, die über die Unzulänglichkeiten von IPSec desillusioniert waren, erfolgreich reagiert.

L2Sec – Funktionsbeschreibung

Die PPP-Sicherheits-Verhandlungen erfolgen bei L2Sec, einer Layer 2-Verbindungen mit Security, sobald ein Kanal zum Zentralsystem aufgebaut ist. Layer 2-Kanäle können sein: ISDN B-Kanal, Modem-Verbindung, Tunnel (L2TP). Bei der NCP VPN-Tunneling-Lösung erfolgen alle Verhandlungsschritte verschlüsselt und sicher in einem End to End-Tunnel zwischen Client und VPN Gateway.

Dabei gewährleistet die Datenkommunikation über den End to End-Tunnel im virtuellen privaten Netz völlige Unabhängigkeit von der Kommunikationsumgebung. Der hierbei aufgebaute Tunnel, Geheimgang der Teilnehmer durch ein öffentliches Wählleitungsnetz, verläuft zwischen entferntem VPN Client und zentralem VPN Gateway.

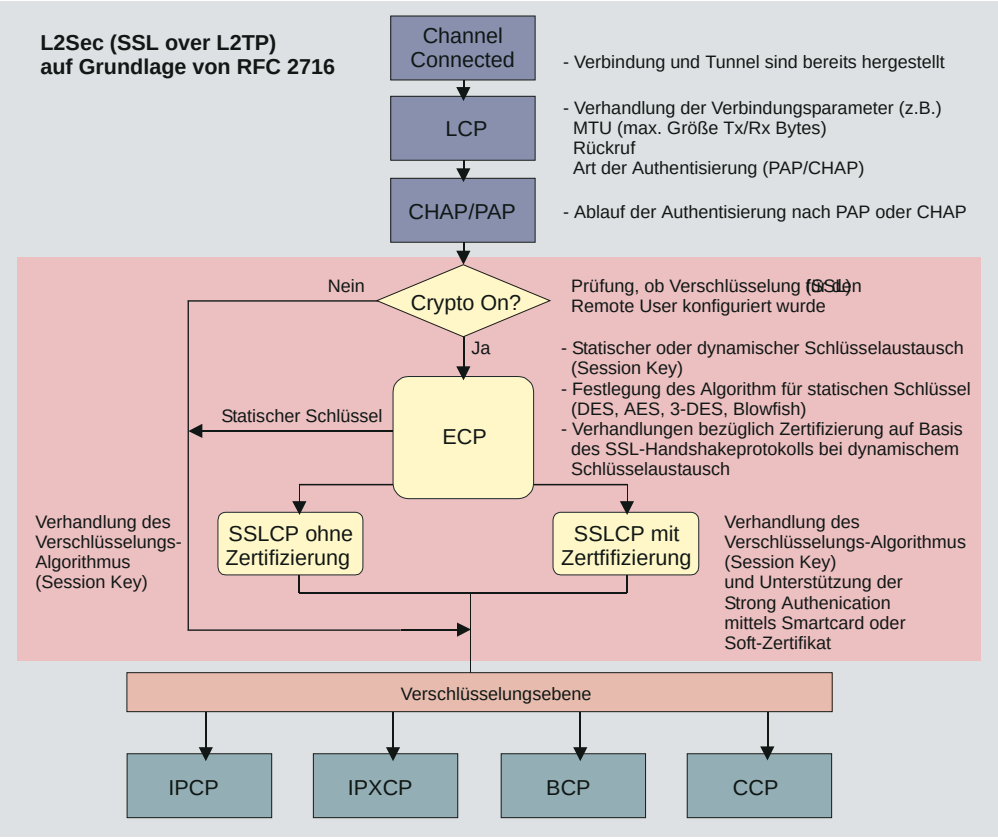
Das komplette IP-Datenpaket, bestehend aus Nutzdaten und IP-Header, wird für die Übertragung verschlüsselt und mit einem neuen Header versehen. Mit anderem Worten: Auch die ursprünglichen IP-Quell- und Zieladressen unterliegen der Kryptierung – ein enormes Sicherheitsplus.

Zwischen dem VPN-Client und dem VPN-Gateway können auf der Wegstrecke des NCP End-to-End-Tunnels beliebig viele IP-Router unterschiedlicher Hersteller installiert sein. Diese müssen weder über Funktionalitäten zur Datenkompression und -Verschlüsselung noch über Tunneling-Protokolle verfügen.

Dies bedeutet Investitionsschutz und Offenheit pur, denn: In das Virtuelle Private Netz können somit sowohl Network Access Server von Internet Service Providern als auch bereits vorhandene eigene bzw. bei Geschäftspartnern installierte IP-Router integriert werden.

Auf diese Weise bildet die NCP Secure Software eine universelle Sicherheits-Infrastruktur, in die sich beliebige Business-Applikationen auf einfache Weise integrieren lassen. Ein zuverlässiges Schlüsselmanagement ist ebenso sichergestellt wie die Einbindung von Certificate Authorities (CAs).

L2Sec – Funktionsskizze



LCP	*Link Control Protocol*
IPCP	*Internet Protocol Control Protocol*
CHAP	*Challenge Authentication Protocol*
IPXCP	*Internetwork Packet Exchange Control Protocol*
PAP	*Password Authentication Protocol*
ECP	*Encryption Control Protocol*
BCP	*Bridge Control Protocol*
SSLCP	*Secure Socket Layer Control Protocol*
CCP	*Compression Control Protocol*
L2Sec	*Layer 2 Security ist funktionell im RFC 2716 beschrieben*

7.2.2 IPSec – Übersicht

IPSec ist ein Standard mit ausgezeichneten Sicherheitsmechanismen, der in bestimmten VPN-Szenarien funktioniert, in denen mit festen IP-Adressen gearbeitet wird (z.B. B2B, Extranet). In diesen Fällen lassen sich auch VPN Gateways verschiedener Hersteller einsetzen. Hier sind feine, bis auf Port-Ebene reichende Sicherheitseinstellungen möglich. Allerdings kann IPSec 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 – 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. (Zunächst die statischen SPDs, die im Konfigurationsbaum unter dem Zweig “IPSec, Secure Policy Database” gelistet sind, erst danach, sofern keine Übereinstimmung gefunden wurde, die dynamische SPD.)

Die SPD besteht aus mehreren Einträgen (SPD Entries), die wiederum einen Filterteil beinhalten. Der Filterteil 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.

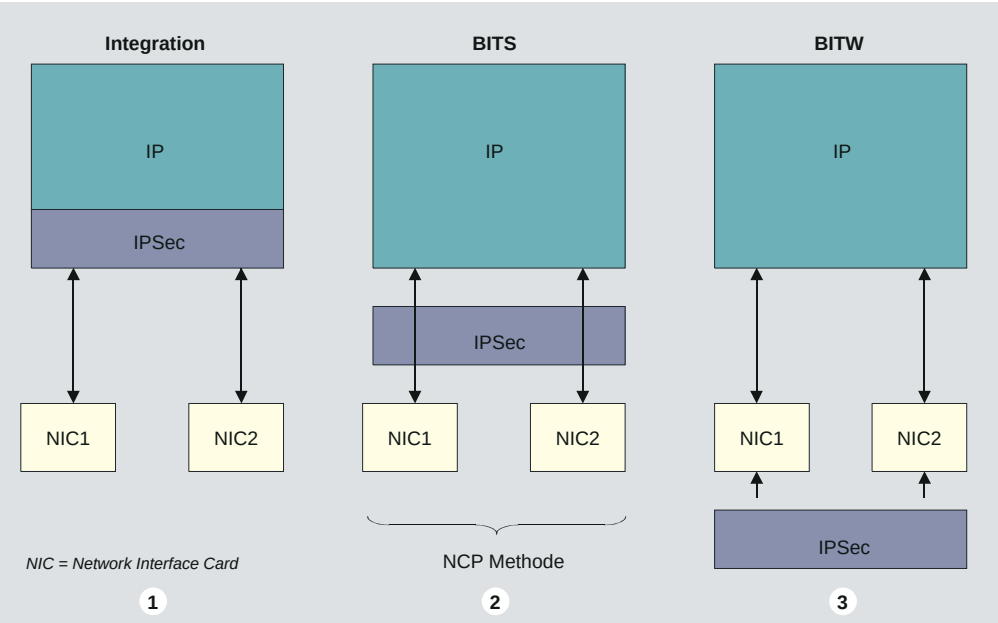
Wird auf diese Weise festgestellt, dass ein IP-Paket mit einem SPD-Eintrag verknüpft ist, der einen IPSec-Prozess einleitet, so wird überprüft, ob bereits eine Sicherheits-Verknüpfung (Security Association, SA) für diesen SPD-Eintrag existiert. Existiert noch keine SA, wird vor dem Aushandeln einer SA 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 und ob im Tunnel- oder Transportmodus übertragen werden soll (siehe unten →Transport- und Tunnelmodus).

Die SA beschreibt, welches Sicherheitsprotokoll verwendet werden soll (ESP oder AH). 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.

Die Implementierung von IPSec



Die Implementierung von IPSec kann auf drei verschiedene Arten erfolgen:

1. Intergration: Dabei wird IPSec vollständig in den IP Stack integriert. Dies ist jedoch nur möglich, wenn der IP Stack vom gleichen Hersteller entwickelt wird wie IPSec.

2. BITS (Bump in the Stack): In diesem Fall wird IPSec durch zusätzliche Treiber zwischen Layer 2 und dem Netzwerkadapter implementiert. Dies ist die am weitesten verbreitete und auch von NCP angewendete Methode. Dabei stellt sich das IPSec-Modul von NCP als ein LAN-Adapter und Intermediate-Treiber für IPSec und Tunneling (siehe →unten) dar. Die IP-Sec-Implementierung von NCP ist RFC-konform und vollständig kompatibel zu Drittherstellern.

3. BITW (Bump in the Wire): Hierbei wird IPSec in die Hardware integriert.

IPSec-Dienste

IPSec bietet durch die Wahlmöglichkeit alternativer Sicherheitsprotokolle und Verschlüsselungsalgorithmen verschiedene Sicherheitsdienste. Bei den Sicherheitsprotokollen handelt es sich um ein Authentisierungsprotokoll, festgelegt durch den Header (Authentisierungs-Header / AH), und ein kombiniertes Verschlüsselungs- und Authentisierungsprotokoll, festgelegt durch das Format (Encapsulating Security Payload / ESP). Folgende Sicherheitsdienste werden durch IPSec bereitgestellt:

- ☐ Zugriffskontrolle (Access Control)
- ☐ Integrität (Integrity, AH/ESP)
- ☐ Authentisierung der Datenherkunft (Data origin Authentication, AH/ESP)
- ☐ Vertraulichkeit (Confidentiality, ESP)

IPSec-Richtlinien / IPSec Policy

Die IPSec-Richtlinien sind im Wesentlichen nach den beiden Sicherheitsprotokollen unterschieden, AH oder ESP, die sich im Tunnelmodus gegenseitig ausschließen. Desweiteren legen Sie fest:

- ☐ wie mit ESP verschlüsselt oder mit AH der Hash-Wert zur Authentisierung gebildet werden soll (Transform / Authentisierung)
- ☐ ob zusätzlich in Phase 2 mit der SA-Verhandlung ein kompletter Schlüsselaustausch (PFS) nach Diffie-Hellmann (DH-Gruppe) stattfinden soll
- ☐ und nach welchen Kriterien die Dauer der Schlüsselgültigkeit bemessen wird (Dauer / Gültigkeit)

Im Konfigurationsbaum unter “IPSec” ist eine IPSec-Richtlinie vorkonfiguriert. Sie ist für das Sicherheitsprotokoll ESP eingerichtet.

AH und ESP im Transport- und Tunnelmodus

Beachten Sie zur folgenden Beschreibung bitte die Abbildung auf der gegenüberliegenden Seite.

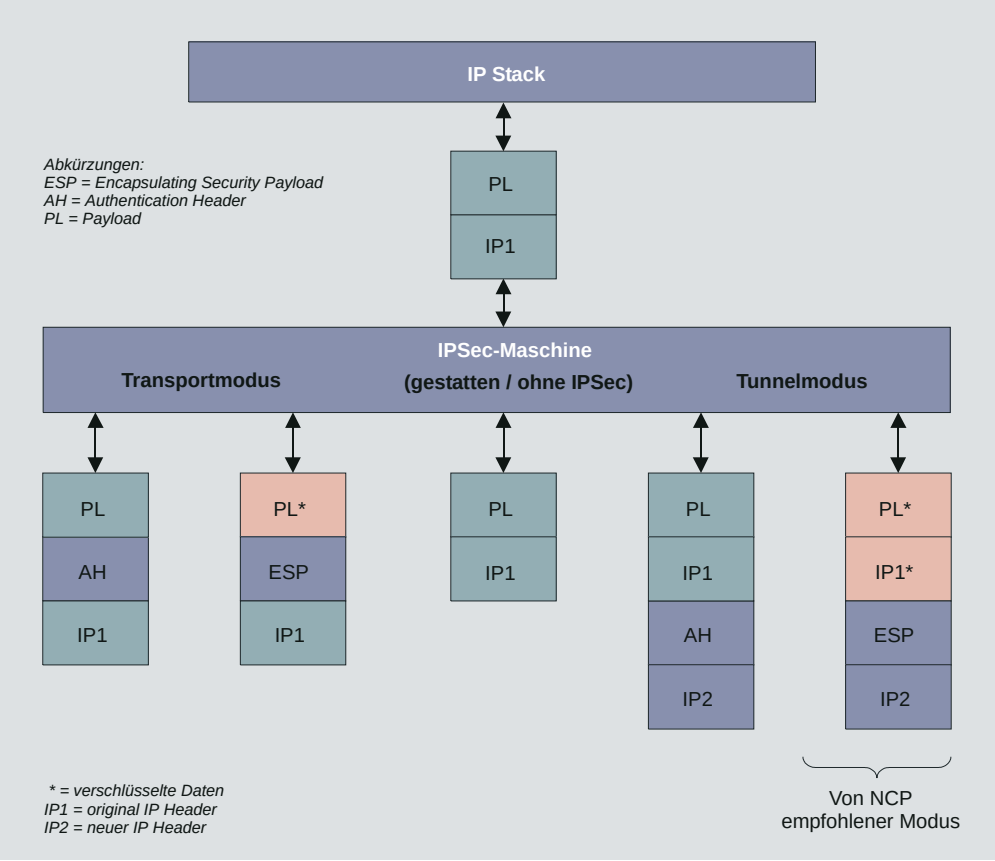
Beide IPSec-Sicherheitsprotokolle (AH und ESP) unterstützen zwei verschiedene Betriebsarten, den Transport- und den Tunnelmodus.

AH im Transportmodus authentifiziert die Nutzdaten des IP-Pakets (Payload) und ausgewählte Teile des IP Headers (IP1). ESP im Transportmodus verschlüsselt (und authentifiziert) die Nutzdaten (Payload) des IP-Pakets, nicht aber den IP Header (IP1). Im Transportmodus werden Ziel- und Quelladressen mit dem IP Header unverschlüsselt übertragen – Quell- und Zieladresse bleiben ungeschützt. Der Transportmodus eignet sich daher nur für eine direkte Kommunikation zwischen zwei Hosts mit festen IP-Adressen oder zwischen Arbeitsplatzrechnern im LAN. (Dieser Modus ist für flexiblen Remote Access völlig ungeeignet.)

Im Tunnelmodus wird das gesamte IP-Paket, einschließlich des hinzugefügten AH- oder ESP-Feldes, eingekapselt und mit einem neuen IP Header (IP2) versehen. Das IP-Paket wird auf diese Weise durch einen Layer 3-Tunnel geschickt. Der innere IP Header mit Original-Adressen ist dabei versteckt und kann nicht eingesehen werden – nur die (Layer 3-) Tunnelendpunkte sind erkennbar. Rechner in Netzen hinter Firewalls oder Routern mit IPSec können in diesem Modus sicher miteinander kommunizieren. Der neue IP Header (IP2) kann völlig andere Quell- und Zieladressen beinhalten als der Original-Header aber er muss Informationen für die Gegenstelle bereithalten, die nötig sind, um das eingekapselte IP-Paket nach den Richtlinien der Sicherheitsverknüpfung (SA) anzunehmen und weiterzuleiten. (Dieser Modus ist für den Secure Server Standard-Einstellung.)

Welches IPSec-Sicherheitsprotokoll mit welchem Verschlüsselungsalgorithmus und welcher Art der Authentisierung kombiniert wird, wird in den IPSec-Richtilinien (IPSec Policy) festgelegt. In der SPD wird auf diese IPSec-Richtlinie, d.h. das Sicherheitsprotokoll, wie auch auf den Betriebsmodus, d.h. Tunnel- oder Transportmodus, verwiesen (siehe →Secure Policy Database, Tunnel).

Funktion der IPSec-Maschine



Die Abbildung (oben) zeigt wie ein IP-Datenpaket vom IP Stack zum IPSec-Modul gesendet wird. Der originale IP Header (IP1) mit seinem Payload (PL-Nutzdaten) wird bearbeitet. Der untere Teil des Bildes zeigt das Ergebnis des IPSec Prozesses.

Der Transportmodus ist nur für Host-zu-Host Kommunikation geeignet, der Tunnelmodus dagegen ermöglicht auch den Betrieb über ein VPN Gateway. Mit dem IP2 Header ist der Transfer von einem Client über das Internet zu einem Gateway möglich. Das VPN Gateway entfernt den IP2 Header, entschlüsselt und sendet das Paket weiter ins lokale LAN. Für Remote Access und End to Site VPN kommt generell nur der ESP-Tunnelmodus in Frage!

7.2.3 Anwendungen

In beiden Betriebsmodi von IPSec erfolgen Authentisierung und Verschlüsselung IP-Adressen-orientiert (auf Layer 3). Daher kommt IPSec insbesondere dann zum Einsatz, wenn beide Kommunikationsendpunkte durch offizielle IP-Adressen gekennzeichnet sind, bzw. die Verbindung vordefiniert ist:

- So lässt sich mit IPSec eine sichere Kommunikation zwischen Zweigstellen eines Unternehmens herstellen. Die Sicherheit dieser LAN-LAN-Kommunikation über ein öffentliches Netz kann auch ohne gemietete Standleitung gewährleistet werden. Ein Unternehmen kann zu diesem Zweck das Internet nutzen. Voraussetzung ist, dass eine Firewall oder ein Router mit IPSec-Funktionalität am Einwahlpunkt des jeweiligen LANs über eine feste offizielle IP-Adresse verfügt.

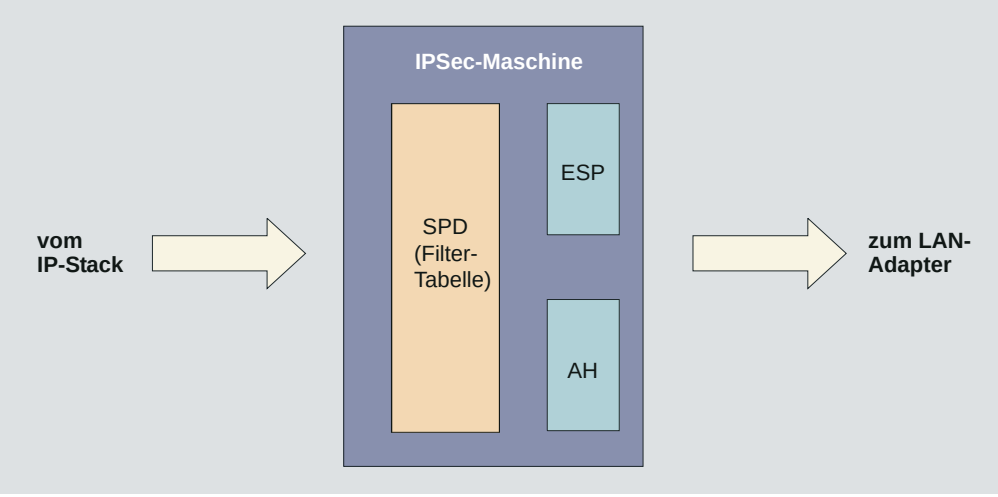
- Ebenso lassen sich mit IPSec Extranet- und Internet-Verbindungen zu Partnern schützen, indem Authentisierung und Vertraulichkeit sichergestellt werden und ein Mechanismus für den Austausch von Schlüsseln festgelegt wird.

- Weitaus schwieriger und nur mit Einschränkungen lassen sich Remote-Anbindungen mehrerer Telearbeiter an das zentrale Firmennetz ausschließlich mit IPSec sichern. Dies liegt daran, dass sich der Client am VPN/GW durch seine IP-Adresse eindeutig identifizieren muss. 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. Die IP-Adresse, die IPSec zur Authentisierung benötigt (siehe →Bild oben IP1), steht nicht mehr zur Verfügung.

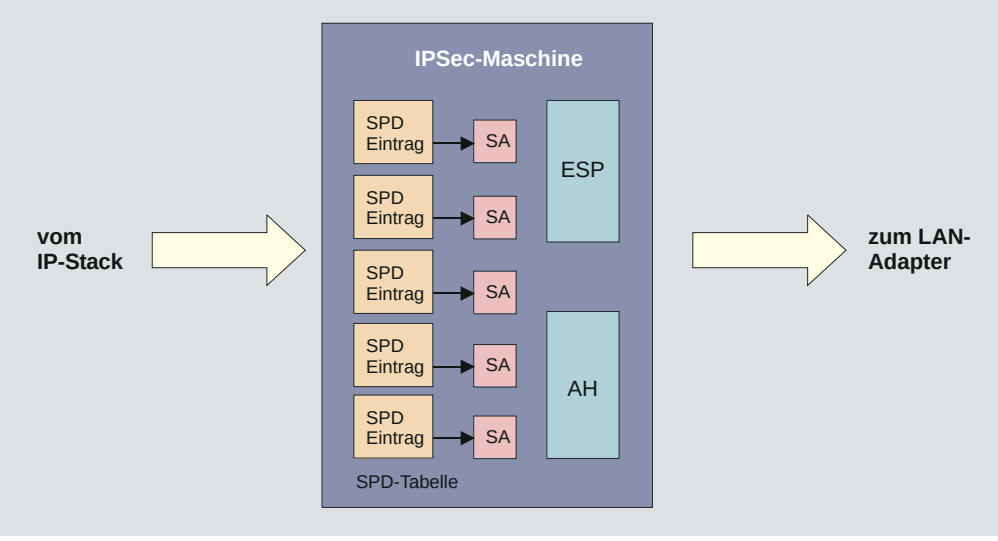
- IPSec kann in diesem Fall nur im Tunnelmodus zum Einsatz kommen. Zudem muss jeder Remote Client über eine eigene private IP-Adresse (eingetragen im Microsoft IP Stack) verfügen, die dem Ziel-Gateway bekannt ist – und für alle Remote Clients muss ein einziger Preshared Key gelten, was die Sicherheit für Remote Access-Anbindungen einschränkt.

7.2.4 Secure Policy Database – Datenbank der Sicherheits-Richtlinien

Ein wesentlicher Bestandteil von IPSec, bzw. der IPSec-Maschine, ist eine Datenbank, in der die Sicherheits-Richtlinien festgehalten sind, die Secure Policy Database (SPD). Siehe Abbildung unten.



Jeder der Einträge der SPD, die wie eine Filtertabelle aufgebaut ist, definiert einen Teil des IP-Verkehrs, sowie die Punkte einer Security Association (SA) dieses Verkehrs. Siehe Abbildung unten.



Zunächst entscheiden drei verschiedene Stati der SPD über den weiteren Umgang mit den IP-Paketen (siehe →Selektoren, Status). Da in der IPSec-Maschine immer die Pakete definierter IP-Adressen bearbeitet werden, beziehen sich die Stati der SPD immer auch nur auf die in den Selektoren angegebenen Adressen oder Adressbereiche:

- ☐ IPSec (IPSec) →für die IP-Pakete mit Adressen aus dem definierten Bereich werden die IPSec-Sicherheitsdienste angewendet, die SPD-Filtertabelle kommt zum Einsatz
- ☐ gestatten (permit) →die IP-Pakete mit Adressen aus dem definierten Bereich werden durchgelassen, ohne dass die SPD zum Einsatz kommt
- ☐ sperren (deny) →alle IP-Pakete mit Adressen aus dem definierten Bereich werden weggeworfen
- ☐ inaktiv (disabled) →diese SPD wird ausgeschaltet und kommt für IPSec nicht zum Einsatz, ohne dass sie gelöscht werden muss

■ Sicherheits-Verknüpfung (Security Association / SA)

Die Security Association bezeichnet eine Einwegbeziehung zwischen Sender und Empfänger von Daten, die die Sicherheitsdienste für den Datenaustausch definiert (und bereitstellt). Für sicheren Datenaustausch in einer bidirektionalen Peer-to-Peer-Verbindung sind zwei SAs erforderlich. Mit Hilfe der SPD wird dem IP-Verkehr eine bestimmte Sicherheitsverknüpfung (SA) zugeordnet. (Vergleiche Abbildung und Bildbeschreibung auf der folgenden Seite.)

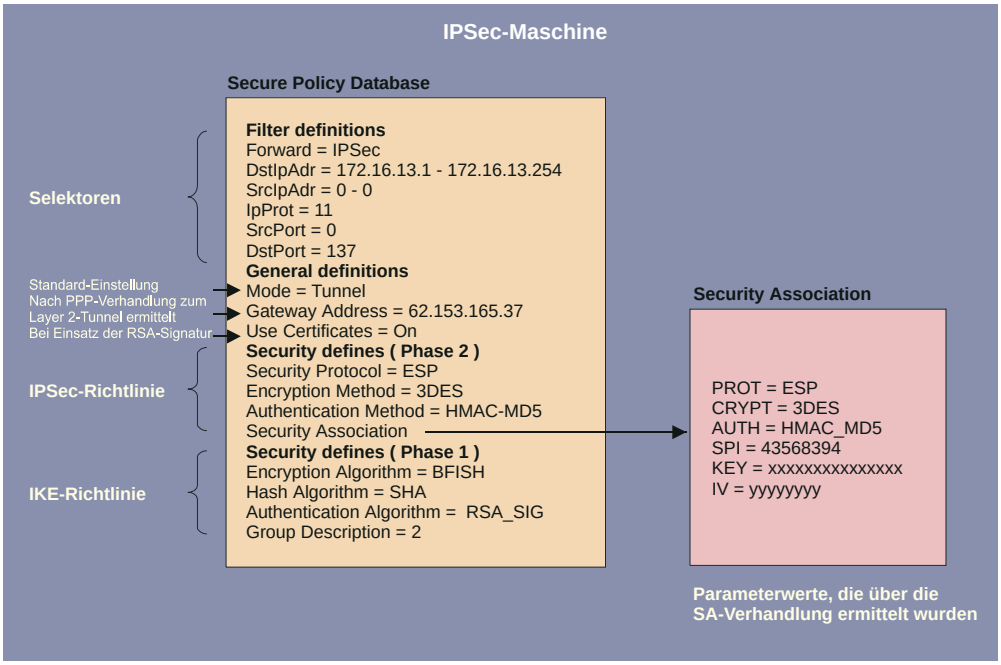
Jeder SPD-Eintrag wird durch eine Gruppe von IP- und Oberschichtprotokoll-Parametern definiert, den Selektoren. Mit ihnen wird der ausgehende Verkehr so gefiltert, dass er zu einer bestimmten SA passt.

Dabei wird jedes einzelne IP-Paket nach folgenden Kriterien untersucht:

1. Vergleiche die Selektorenfelder des IP-Pakets mit der SPD, um einen Eintrag zu finden, der auf eine SA verweist
2. Selektiere eine passende SA nach dem Security Parameter Index (SPI)* im IP-Paket
3. Führe die entsprechenden IPSec-Anweisungen aus (z.B. AH oder ESP)

** Der SPI (Security Parameters Index) ist ein Bitstring und wird in den AH- oder ESP-Header des IP-Pakets eingetragen, damit die Gegenstelle die zugehörige SA erkennen kann.*

Beispiel einer Secure Policy Database von NCP



Bildbeschreibung zu obiger Abbildung:

Die Prüfung der vom IP Stack ausgehenden IP-Pakete erfolgt bezüglich einer Secure Policy Database (SPD). Die SPD besteht aus mehreren Einträgen (SPD Entries), die wiederum einen Filterteil beinhalten. Der Filterteil oder Selektor eines SPD-Eintrags besteht hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderen IP Header-spezifischen Einträgen. 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 (IPSec). 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-Verhandlung (Security Association, SA) für diesen SPD-Eintrag existiert. Die SA beschreibt, welches Sicherheitsprotokoll verwendet werden soll (ESP oder AH). 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.

■ Selektoren (der statischen SPD)

Der Selektor oder Filterteil 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.

Im folgenden die Selektoreneinträge zur Konfiguration im Secure Client von NCP:

☐ Status / State (siehe oben)

IPSec (IPSec), 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 [...].

7.2.5 SA-Verhandlung und Richtlinien / Policies

Damit der IPSec-(Filter-)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 (siehe →Selektoren) – einmal statt. Für diese SA-Verhandlung wird ein Kontrollkanal benötigt.

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

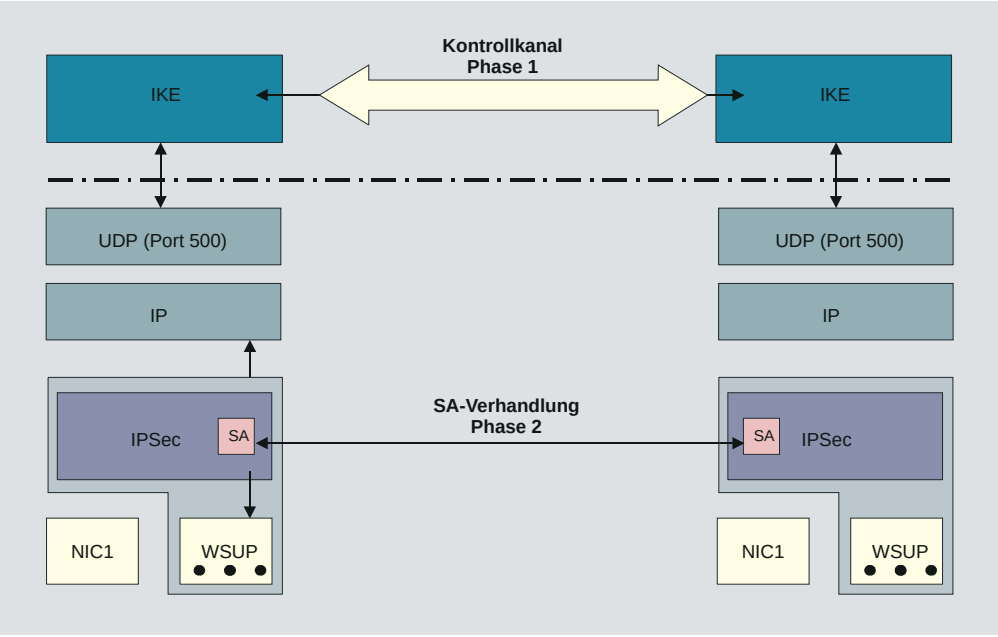
Der Kontrollkanal wird im Tunnelmodus von IPSec über das IKE-Protokoll zur IP-Adresse des Secure Gateways aufgebaut, im Transportmodus direkt zur IP-Adresse der Gegenstelle. (Tunnel- oder Transportmodus wird gesetzt unter “Secure Policy Database, Tunnel”).

Parameter zur Festlegung von Verschlüsselungs- und Authentisierungsart über das IKE-Protokoll definieren Sie in den IKE-Richtlinien. Dabei kann die Authentisierung über einen Preshared Key oder eine RSA Signatur erfolgen. (In der Secure Policy Database wird unter Security auf diese IKE-Richtlinie verwiesen.)

- **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 (Secure Server) ausgehandelt werden kann, muss eine Art Kontrollkanal vom Client zum Secure Server 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 Secure Server (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.

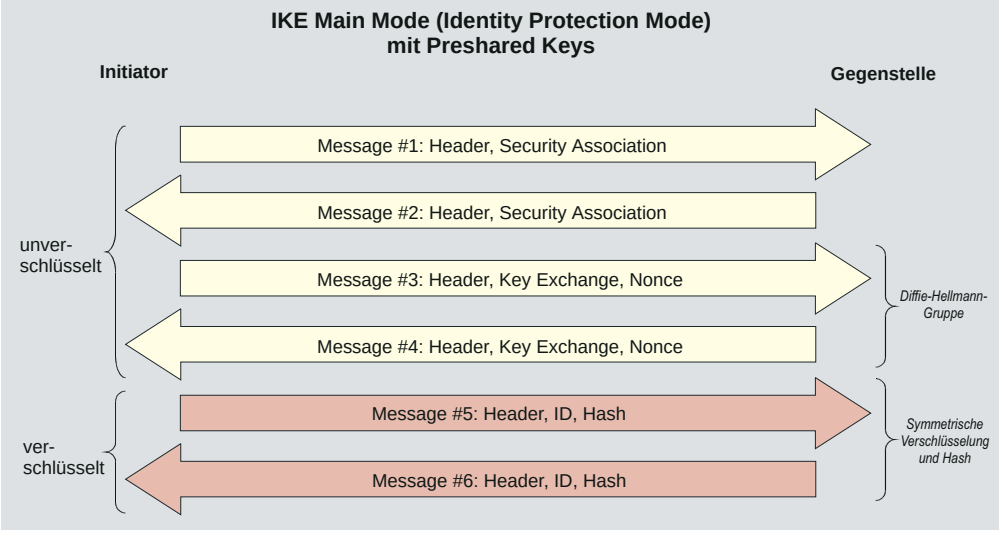
IKE-Modi

Im wesentlichen können zwei Arten der IKE-Richtlinien konfiguriert werden. Sie unterscheiden sich durch die Art der Authentisierung, entweder über Preshared 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.

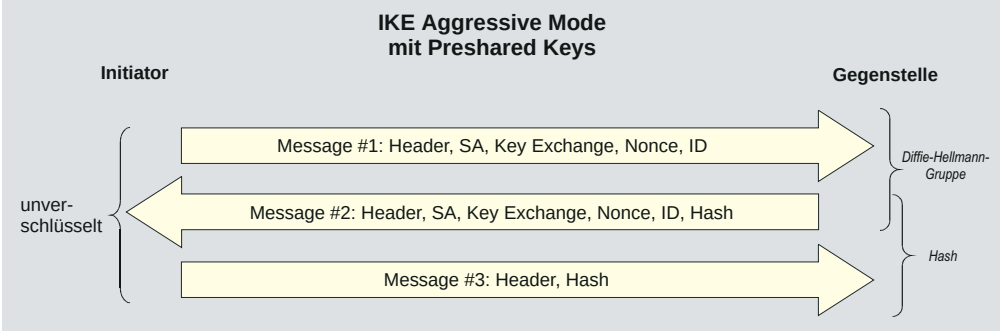
Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch Identity Protection Mode.

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

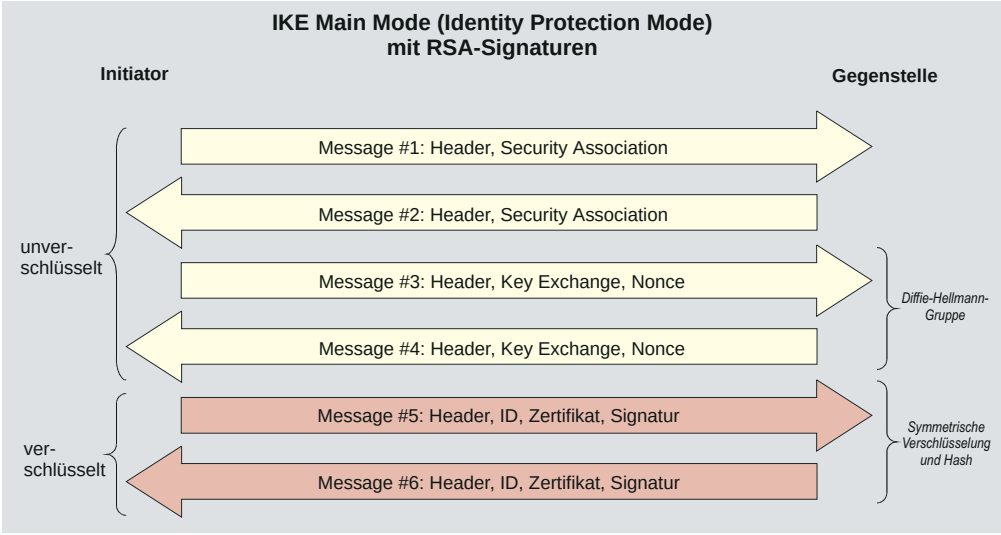
Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in den Parameterfeldern “Security” des Telefonbuchs (für eine dynamische SPD) und unter “IPSec, Secure Policy Database” (für eine statische SPD). (Siehe auch →Austausch-Modus / Exchange Mode)



Wird die Preshared Key-Methode im Main Mode genutzt (Bild oben), so muss der Client am VPN/GW durch seine IP-Adresse eindeutig identifizierbar sein, da der Preshared 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 Preshared Key vergeben werden, was allerdings die Authentisierung abschwächt.



Eine Möglichkeit, einen allgmeinen Preshared 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.

7.3 IPSec für Remote Access – IPSec over L2TP

Wie lässt sich IPSec in uneingeschränktem Funktionsumfang für Remote Access nutzen, ohne dass Sicherheitslücken entstehen, d.h. wie kann trotz sich ändernder IP-Adressen das Prinzip der IP-Adressen-Orientierung von IPSec beibehalten werden, ohne dass die oben beschriebenen Einschränkungen vorgenommen werden müssen?

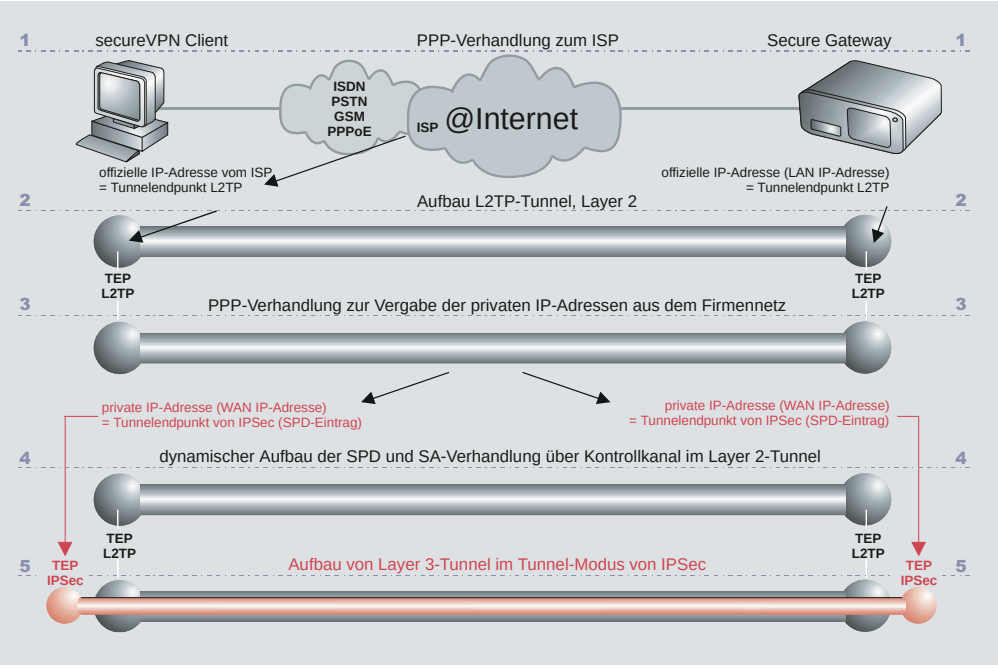
Wie in RFC 2888 beschrieben und von verschiedenen IPSec-Experten empfohlen, kann dies bewerkstelligt werden, indem zunächst ein Layer 2-Tunnel über das Internet zwischen Remote Access Client und Zentralsystem aufgebaut wird, so dass die anschließende IPSec-Verhandlung bereits in einem VPN (Virtual Private Network) getunnelt stattfindet.

Der Tunnelaufbau wird durch eine Benutzer-orientierte Authentisierung (Layer 2) gesichert. Danach kann eine IP-Adresse aus dem Firmennetz vergeben werden, die für den daraufhin einsetzenden IPSec-Prozess verwendet werden kann.

Mit IPSec over L2TP werden alle Nachteile von IPSec im Remote Access-Bereich wett gemacht. Jeder handelsübliche Router, der IP Network Address Translation unterstützt, kann eingebunden werden. Zudem besteht die Möglichkeit, über standardisierte Schnittstellen zusätzliche Sicherheitsmechanismen einer Public Key Infrastucture zu nutzen. Um die Sicherheit von IPSec over L2TP auf ganzer Strecke gewährleisten zu können, empfiehlt NCP das Secure Gateway hinter dem Access Server und der Firewall in der Demilitarisierten Zone (DMZ) zu installieren. Damit befinden sich alle Parameter der sicheren Datenübertragung im Einflussbereich des Unternehmens:

- ☑ Endpunkte des Layer 2-Tunnels (Secure Server, VPN Gateway, Remote Client)
- ☑ Tunnelingverfahren
- ☑ Schlüsselalgorithmus
- ☑ Netzwerkprotokoll
- ☑ Datenkompression
- ☑ Übertragungsmedium
- ☑ IP-Adresse aus dem Firmennetz
- ☑ IPSec-Parameter

IPSec over L2TP mit dynamischer SPD



1. Standard-PPP-Verhandlung über Benutzer / Passwort (User ID / Password) und Authentisierung vom Client gegenüber Internet Service Provider (ISP), wonach der Client eine offizielle IP-Adresse vom ISP erhält. Anschließend baut der Client eine Verbindung zum Secure Server via Internet auf. Die dazu nötigen Parameter befinden sich im Telefonbuch des Clients unter "Zielsystem" und "Netzeinwahl". Die "Tunnel IP-Adresse (Ziel)", eingetragen im Telefonbuch unter "Tunnelparameter", entspricht der offiziellen IP-Adresse des Secure Servers.
2. Nach Prüfung des "Tunnelsecret" werden die Tunnel-Parameter verhandelt und der L2TP-Tunnel im Layer 2 aufgebaut. Tunnelendpunkte sind die offizielle IP-Adresse, die der Client vom ISP erhalten hat und die offizielle IP-Adresse des Secure Servers, die im Telefonbuch des Clients als "Tunnel IP-Adresse (Ziel)" eingetragen ist.(1 (*2*
3. Nach einer weiteren PPP-Verhandlung und Prüfung von "Benutzer" und "Passwort", erfolgt die Vergabe der privaten IP-Adressen aus dem Firmennetz. Diese Adressen können aus einem Pool des Secure Servers stammen (siehe →Routing Interfaces, Pools). Der Remote Client ist damit – unabhängig von seinem Standort – immer eindeutig anhand seiner IP-Adresse identifizierbar.
4. Über den Kontrollkanal im Layer 2-Tunnel findet die SA-Verhandlung statt. Die Strong Authentication erfolgt gemäß der IKE-Richtlinien (IKE Policy), die für dieses Link-Profil festgelegt wurden (siehe →Telefonbuch, Security).
5. Der Layer 3-Tunnel wird nach Vorgabe des IPSec-Betriebsmodus (siehe →Telefonbuch, Security, IPSec-Richtlinie) aufgebaut. Tunnelendpunkte sind die IP-Adressen aus dem Firmennetz.

*(*1 Nach IETF muss das Tunnelende immer im geschützten privaten Bereich des VPN-Betreibers, hinter der Firewall in der DMZ liegen.*
*(*2 Bei L2Sec erfolgt hier die SSL-Verhandlung.*

7.4 Verbindungen über das Tunnelprotokoll “IPSec Tunneling”

Im Telefonbuch des Clients unter “Tunnel-Parameter” kann zwischen den VPN-Protokollen “L2TP” (Layer 2) und “IPSec Tunneling” (Layer 3) gewählt werden. Wird das VPN-Protokoll “IPSec Tunneling” gewählt, so wird die IPSec-Verbindung ohne einen Layer 2-Tunnel (L2TP) hergestellt. Diese Art des IPSec Tunnelings entspricht dem standardmäßigen Einsatz von IPSec (IPSec native), das auf diese Weise auch gegenüber IPSec-Gateways zum Einsatz kommen kann, die von anderen Herstellern als NCP stammen.

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 (Preshared 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

– SHA1

Zusätzliche Unterstützung für Phase 2

– PFS (Perfect Forward Secrecy)

– IPCOMP (LZS)

– Seamless re-keying

Wird ein Zielsystem im Telefonbuch des Clients mit “IPSec-Tunneling” konfiguriert, so werden zunächst einige Standards gesetzt (siehe unten “Zur Konfiguration ...”):

– IKE Phase 1 Richtlinie - Von Gegenstelle bestimmt

– IKE Phase 2 Richtlinie - Von Gegenstelle bestimmt

– IKE Phase 1 Modus RSA - Main Mode

– IKE Phase 1 Modus PSK - Aggressive Mode

Diese automatisch gesetzten Richtlinien und Verhandlungsmodi sind jedoch im Telefonbuch konfigurierbar gehalten, sodass sie anderslautenden Verbindungsanforderungen entsprechend modifiziert werden können.

Standard IKE-Vorschläge:

1. Bleibt das Feld für “Preshared Key” leer, wenn die Einstellung “von Gegenstelle bestimmt” vorgenommen wurde, so werden an die Gegenstelle standardmäßig folgende Vorschläge für die IKE-Richtlinie versendet, wobei die Authentisierung immer mit Zertifikat erfolgt (vgl. →IKE-Richtlinie, Phase-1-Parameter):

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 des Client-Telefonbuchs eingestellt, so wird immer auch automatisch der gleiche Vorschlag zusätzlich mit Extended Authentication generiert und versendet.

2. Wird in das Feld für “Preshared 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 folgendes geschickt:

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

Zur Konfiguration des VPN-Protokolls “IPSec Tunneling”

Im Telefonbuch des Clients unter “Tunnel-Parameter” kann zwischen den VPN-Protokollen “L2TP” (Layer 2) und “IPSec Tunneling” (Layer 3) gewählt werden. Wird das VPN-Protokoll “IPSec Tunneling” gewählt, so wird die IPSec-Verbindung ohne einen Layer 2-Tunnel (L2TP) hergestellt. Bei Auswahl von “IPSec Tunneling” wird darauf hingewiesen, dass im Konfigurationsfeld “Security” automatisch folgende Einstellungen vorgenommen werden:

Security-Modus	=	IPSec
IKE-Richtlinie	=	Von Gegenstelle bestimmt
IPSec-Richtlinie	=	Von Gegenstelle bestimmt
Austausch-Modus	=	Main Mode

Im Telefonbuch unter der Rubrik “Security” werden die Parameter “IKE ID-Typ” und “IKE ID” zur Konfiguration eingeblendet:

IKE ID-Typ	=	Alternativen: IP-Adresse, Fully Qualified Domain Name, Fully Qualified Username, IP Subnet-Adresse, ASN1 Distinguished Name, ASN1 Group Name, Free String used to identify Groups
IKE ID	=	je nach ausgewähltem ID-Typ muss der zugehörige String eingetragen werden.

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

IP-Adressen und DNS Server werden über das Protokoll IKE-Config Mode (Draft 2) zugewiesen (kompatibel derzeit nur gegen Cisco, siehe auch unten DHCP-Modus). Für die NAS-Einwahl können alle bisherigen WAN-Schnittstellen verwendet werden.

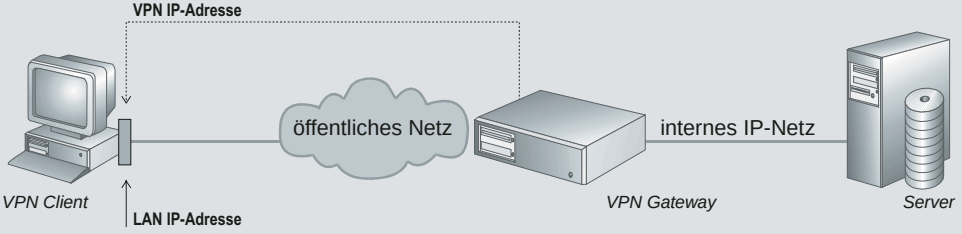
Die Authentisierung bei “IPSec Tunneling” erfolgt über das XAUTH Protokoll (Draft 6). Dazu müssen außerdem noch folgende Parameter im Konfigurationsfeld “Tunnel-Parameter” gesetzt werden:

VPN-Benutzername	=	Kennwort des IPSec-Benutzers
VPN-Passwort	=	Passwort des IPSec-Benutzers
Benutze Zugangsdaten von Zertifikat	=	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. 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.

DHCP-Modus und private IP-Adresse am Client

Die VPN IP-Adresse darf nicht mit der des physikalischen LAN-Adapters übereinstimmen. Desweiteren muss eine private IP-Adresse im Telefonbuch des Clients unter IPSec-Optionen eingetragen werden, wenn der Client keine IP-Adresse vom IPSec Gateway über IKE-Config erhält.



	IKE Config-Mode Verhandlung	DHCP-Modus auf NCP Adapter aktiviert	Private IP-Adresse in IPSec-Optionen eingetragen
LAN IP-Adresse entspricht nicht VPN IP-Adresse	ja	ja	nein
	nein	ja	ja
LAN IP-Adresse entspricht VPN IP-Adresse	ja	nein	nein
	nein	nein	ja

7.5 Parallele Verbindungen ins Internet und zu einem VPN IP-Netz

Der Secure Client unterscheidet die Art der Verbindung anhand der verwendeten „offiziellen" IP-Adressen.

1 Konfigurieren Sie ein Ziel zu Ihrem ISP im Telefonbuch des Secure Client (z.B. „Internet1"). Achten Sie darauf, dass IP Network Address Translation aktiv ist.

Führen Sie anschließend folgenden Test durch, um zu sehen ob zusätzlich ein VPN-Tunnel aufgebaut werden kann: Öffnen Sie eine DOS-Box und pingen Sie das VPN-Gateway an. Bitte beachten Sie dabei, dass das VPN-Gateway nicht antworten kann, wenn der Zugang durch eine Firewall geschützt ist, dass VPN-Datenströme aber dennoch das VPN-Gateway erreichen können.

2 Um zusätzlich zum ISP einen VPN-Tunnel zu einem IP-Netz (VPN IP-Netz) aufbauen zu können, werden zu den oben konfigurierten Parametern des Ziels „Internet1" in den folgenden Parameterfeldern weitere Einstellungen vorgenommen:

■ Parameterfeld Tunnel-Parameter

VPN-Protokoll	=	L2TP
Benutzer (VPN)	=	(abgestimmt mit Administrator)
Passwort (VPN)	=	(abgestimmt mit Administrator)
Tunnel Secret	=	(abgestimmt mit Administrator)
Tunnel IP-Adr. (Ziel)	=	"offizielle" IP-Adresse des VPN Gateways
Tunnel IP-Adr. (lokal)	=	leer

■ Parameterfeld VPN IP-Netze

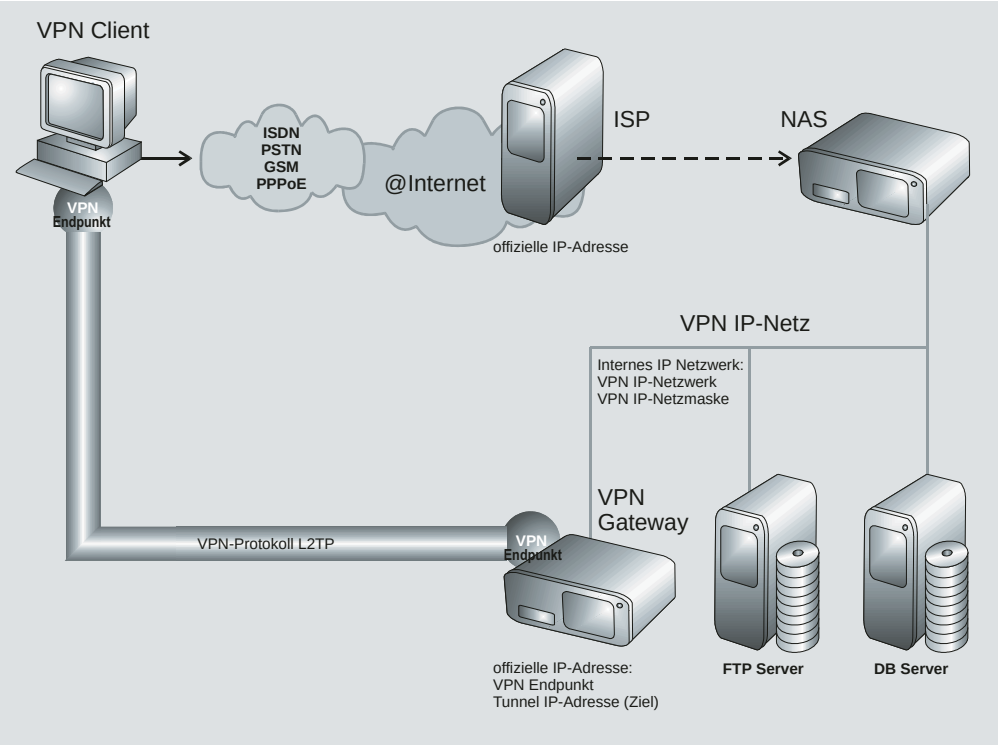
VPN IP-Netzwerk	=	firmeninterne IP-Adresse des IP-Netzes (nur zu dem hier eingetragenen Netz oder Netzen wird ein Tunnel aufgebaut. Ist keine Netzadresse eingetragen, so wird immer zum VPN-Gateway über Tunnel übertragen, sobald für dieses Ziel Tunneling aktiviert ist. D.h. in diesem Fall würde die Verbindung zum ISP über Tunnel und NAS aufgebaut werden, gestrichelte Linie)
VPN IP-Netzmaske	=	IP-Adresse der Netzmaske

Bitte achten Sie darauf, dass die offizielle Internet IP-Adresse nicht im Bereich der internen Firmenadressen liegt.

3 Die Verbindung zum Ziel „Internet1" wird über den Secure Client hergestellt.

4 Anwendung für das VPN IP-Netz (z.B. E-Mail oder Datenbank-Recherche) wird gestartet.

Parallele Verbindungen ins Internet und zu einem VPN IP-Netz



7.6 Zertifikats-Überprüfungen

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

7.6.1. 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 Secure 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\CA-CERTS\. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande. Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

7.6.2. 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 Secure Client und den Secure Server sind folgende Erweiterungen von Bedeutung:

– KeyUsage
– extendedKeyUsage
– subjectKeyIdentifier
– authorityKeyIdentifier
– CDP (Certificate Distribution Point)

KeyUsage

Ist in einen eingehenden Zertifikat die Erweiterung KeyUsage enthalten, so wird diese überprüft. Folgende KeyUsage-Bits werden akzeptiert:
– Digital Signatur
– Key Encipherment (Schlüsseltransport, Schlüsselverwaltung)
– Key Aggrenment (Schlüsselaustaschverfahren)
Ist eines des Bits nicht gesetzt, wird die Verbindung abgebaut.

extendedKeyUsage

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der Secure 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.)

CDP (Certificate Distribution Point)

Im Certificate Distribution Point ist die URL für den Download einer CRL hinterlegt. Ist im Zertifikat die Erweiterung CDP enthalten, wird nach dem Verbindungsaufbau die CRL über die angegebene URL heruntergeladen und überprüft. Wird dabei festgestellt,

dass das Zertifikat ungültig ist, wird die Verbindung abgebaut. Die CRL wird dabei unter dem Common-Name der CA im Verzeichniss ncple\crls gespeichert.

7.6.3. Überprüfung von Sperrlisten

Zu jedem Aussteller-Zertifikat kann dem Secure 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 Secure 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.

7.7 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

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z