

# What's New

high security remote access

# NCP

SECURE COMMUNICATIONS ■

## NCP Secure Entry Client (Windows 32/64 Bit für Windows 7, Vista und XP)

Neue Features von Version 9.2 bis 8.1

### **Haftungsausschluss**

Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

### **Warenzeichen**

Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

## Inhalt

|   |    |
|---|----|
| Neue Features der Version 9.23 Build 18 gegenüber Version 9.20.....         | 2  |
| Neue Features der Version 9.2 Build 33 gegenüber Version 9.10 Build 55..... | 2  |
| Neue Features der Version 9.1 gegenüber Version 9.0.....                    | 5  |
| Neue Features der Version 9.1 gegenüber 9.04 .....                          | 5  |
| Neue Features der Version 9.04 gegenüber 9.03.....                          | 6  |
| Neue Features der Version 9.03 gegenüber 9.01.....                          | 7  |
| Neue Features der Version 9.01 gegenüber 9.0 .....                          | 8  |
| Neue Features der Version 9.0 gegenüber Version 8.3.....                    | 8  |
| Neue Features der Version 8.3 gegenüber Version 8.2/8.1 .....               | 11 |

## Neue Features der Version 9.23 Build 18 gegenüber Version 9.20

### FIPS inside

Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1051).

*Vorteil:* Nachweis der Sicherheit durch offizielle Standards

### Verwenden des Benutzerzertifikats aus dem Windows Zertifikat-Store via CSP

Auf Benutzerzertifikate die im Windows Zertifikat-Store enthalten sind kann zur Authentisierung lesend via CSP zugegriffen werden. Die Nutzung dieser Funktionalität ist ausschließlich nach einer erfolgten Benutzeranmeldung am Windows System möglich.

Da diese Funktionalität erst nach einer Anmeldung des Benutzers am Windows-System zur Verfügung steht, kann sie nicht zur Domänenanmeldung über VPN eingesetzt werden!

*Vorteil:* Zertifikat lässt sich im vom Betriebssystem vorgesehenen Zertifikatsspeicher laden

### Icon für NCP VPN Path Finder

Wurde die Verbindung mit dem VPN Path Finder über den Port 443 aufgebaut, wird dies über ein Icon in der Statusanzeige des Monitors (rechts unter dem HQ/Gateway) angezeigt.

*Vorteil:* Die Anwender sehen direkt im Client-Monitor, wenn Sie über die NCP VPN Path Finder Technologie verbunden sind.

## Neue Features der Version 9.2 Build 33 gegenüber Version 9.10 Build 55

### Windows 7 Support (k)

Das neue Microsoft Betriebssystem Windows 7 wird ab der Version 9.2 ohne Einschränkungen unterstützt. Damit kann der NCP Secure Entry Client unter allen 32-/64-Bit Windows Betriebssystemen genutzt werden: Windows XP, Windows Vista, Windows 7.

Unterstützung aller aktuellen Windows Arbeitsplatz-Betriebssystem unter einer einheitlichen Benutzeroberfläche.

*(Hinweise: Ab der Version 9.2 entfällt der Support für Windows 2000. Die Installation auf Windows 7 erfordert einen Produktschlüssel der Version 9.2. Im Falle eines Updates von Windows Vista auf Windows 7 lässt sich bei einem Client der Version 9.2, der mit einem 9.1-er Schlüssel lizenziert wurde, nur der Monitor starten um die Eingabe eines 9.2-er Schlüssels zu ermöglichen.)*

### **VPN Path Finder inkl. Proxy-Support (k)**

Die NCP VPN Path Finder Technology bewirkt ein automatisches Umschalten auf ein alternatives Verbindungsprotokoll (TCP Encapsulation mit SSL Header über Port 443), wenn Standard IPsec über Port 500 bzw. UDP Encapsulation über einen frei konfigurierbaren Port nicht möglich ist. (In Verbindung mit NCP Secure Server 8.0.)

Der Anwender hat auch bei beschränktem Zugang ins Internet (auf den HTTPS-Zielport 443) die Möglichkeit sich via IPsec-Tunneling mit dem Firmennetz zu verbinden.

### **WLAN-Roaming**

Bewegt sich der Teleworker mit seinem Laptop innerhalb des Empfangsbereichs mehrerer Accesspoints mit derselben SSID, so wird im Falle einer schlechten WLAN-Empfangsleistung automatisch auf einen stärkeren Accesspoint gewechselt.

Anwendungen die über den VPN-Tunnel kommunizieren „merken“ davon nichts.

Der NCP Secure Entry Client kann innerhalb von Firmennetzen zwischen verschiedenen Accesspoints wechseln (z.B. bei Standortwechsel mit Laptop), ohne eine neue Datenverbindung aufbauen und sich neu am VPN Gateway anmelden zu müssen. D.h. kontinuierlichen Remote Access trotz wechselnder IP-Adresse.

### **Verbesserter Datendurchsatz auf 64 Bit Windows Plattformen.**

Der Datendurchsatz konnte durch die Optimierung (RWSNT-Dienst) um ca. 20% erhöht werden.

### **Unterstützung der neuesten Intel WLAN Treiber Version 12.4.0.21 und höher.**

Die neuen Treiber stellen sich nicht mehr als Ethernet- sondern als WLAN-Treiber dar. Das erfordert ggf. eine Deinstallation des bisherigen NCP Secure Entry Clients. Die Neuinstallation kann nach dem Reboot durchgeführt werden, wobei alle bisherigen Einstellungen erhalten bleiben.

### **Unterstützung der neuen Windows 7 Mobile Broadband Treiber (3G/UMTS).**

#### **Überarbeitete 3G/UMTS-Konfiguration, Providerliste ist über INI-Datei (APN.ini) konfigurierbar**

Das Konfigurationsmenü wurde umbenannt in GPRS / UMTS (Darin wird auch die UMTS-Konfiguration überarbeitet. Es existieren nun drei Varianten:

- a) Providerliste (Standardeinstellung)  
bei der Auswahl des Providers werden der Access Point Name (APN) und die Einwahlnummer vorgeschlagen.

- b) APN von SIM Karte  
es wird kein APN an die SIM-Karte weitergegeben und setzt voraus, dass ein APN in der SIM-Karte konfiguriert ist.
- c) Benutzerdefiniert;  
der Anwender kann alle Einwahlparameter manuell konfigurieren.

Die GPRS/UMTS-Konfiguration wurde für den Anwender weiter vereinfacht.

### **Überarbeitung WLAN GUI und Feldstärkemessung, Tray Icon**

Ist „WLAN“ im Client aktiviert, erscheint in der Taskbar das zugehörige Tray Icon. Dieses Icon zeigt für den aktuellen Verbindungsstatus die Feldstärke und Verschlüsselungsart an. Nach einem Mausklick auf das Tray Icon werden alle verfügbaren WLANs angezeigt. Durch die Auswahl eines bestimmten WLANs wird der Verbindungsaufbau gestartet oder, sofern noch kein WLAN-Profil für dieses Netz besteht, der WLAN-Verbindungsassistent gestartet. Der WLAN-Assistent erleichtert die Profil-Erstellung und automatisiert den Verbindungsaufbau zu einem neuen WLAN. Die Verschlüsselungsart (WEP, WPA, WPA2) wird dabei automatisch erkannt.

Das WLAN-Handling wurde für den Anwender weiter vereinfacht.

### **Statusanzeige beim Scannen von WLANs und beim Verbindungsaufbau (animierte Grafik)**

Ist WLAN aktiviert so wird periodisch nach allen verfügbaren WLANs gescannt. Während des Scanvorganges ist das entsprechende Icon animiert. Ein Verbindungsaufbau zu einem Accesspoint wird durch einen blinkenden, gelben Punkt, links neben der gewählten SSID des WLANs, angezeigt. Ein grüner Punkt zeigt die bestehende WLAN-Verbindung an. Verwenden mehrere WLAN-Accesspoints dieselbe SSID, so erscheint neben der SSID zusätzlich ein kleines rotes Dreieck. Das WLAN-Handling wurde für den Anwender weiter vereinfacht.

### **Tipp des Tages**

Mit jedem Monitorstart erscheint ein neuer „Tipp des Tages“ in der Reihenfolge in der die Tipps in der zugehörigen INI-Datei abgelegt sind (im Verzeichnis Tipps). Darin ist die zugehörige HTML-Antwortseite verlinkt, die beim Klicken auf den Tipp durch den Standardbrowser dargestellt wird. Der Anwender wird kontinuierlich über das Leistungspotential seines Telearbeitsplatzes informiert.

### **Profil-Export**

Das aktuell ausgewählte Profil kann mittels dieser Funktionalität exportiert und bei einem anderen NCP Secure Entry Client importiert werden. Zertifikate müssen allerdings separat kopiert werden.

Der Anwender kann sein VPN Profil auf einfachste Weise von einem Rechner auf einen weiteren übernehmen.

### **Budgetmanager mit Historie für die letzten zwölf Monate**

Dem Anwender stehen bei Bedarf alle relevanten Informationen seiner Datenkommunikation innerhalb der letzten zwölf Monate zur Verfügung.

### **Vodafone Websessions Unterstützung**

Easy-to-Use auch für Vodafone-User. Der Anwender kann sich mit nur einem Klick auf „Verbinden“ an Vodafone Websessions anmelden und den VPN-Tunnel aufbauen.

**Modernisierung der Benutzer-Oberfläche**

Die grafische Benutzeroberfläche wurde weiter optimiert und den Markterfordernissen angepasst. Wesentliche Anpassungen sind:

- Einheitlicher Verbinden/Trennen-Schalter
- Weltkarte in Abhängigkeit der Zeitzone  
In Abhängigkeit der am Rechner konfigurierten Zeitzone wird ein entsprechender Ausschnitt der Weltkarte angezeigt: Europa, Amerika, Asien/Australien.
- Weltkarte mit Tag/Nacht-Grenze in Abhängigkeit von der Uhrzeit  
In Abhängigkeit von der Uhrzeit wird über der Weltkarte die Tag/Nachtgrenze dargestellt. Die Position wird alle 10 Minuten aktualisiert.

**Verbessertes Log-Handling.**

Bei Markierung einer Zeile im Monitor „Log“ stoppt das Log. Das erleichtert die Durchsicht und Überprüfung von Log-Ausgaben direkt im Monitor erheblich.

**Beschleunigung des Verbindungsaufbaus**

Das wird durch ein optimiertes Verhalten des Clients im getrennten Zustand im DHCP-Modus und manuellem Verbindungsaufbau erreicht.

**Erweiterung der Encryption- und Hash Optionen.**

Diffie-Hellmann-Gruppe 14, SHA-256, SHA-384 und SHA-512.

**Weitere Änderungen:**

- Die Konfigurationsgruppe "VPN IP Networks" heißt nun "Split Tunneling".
- Optimierte Darstellung der verfügbaren WLAN Netze.
- Setup Routine ist auch in Französisch und Polnisch verfügbar.
- Die maximale Anzahl der remote VPN Netze wurde auf 250 erweitert.
- IPsec Optimierungen: Weitere Verbesserung der Kompatibilität.
- Entlastung des Systems durch Optimierung der Personal Firewall bei Verwendung anwendungsbezogener Regeln.
- Verbessertes Menü-Handling bei der Sprachauswahl.

**Neue Features der Version 9.1 gegenüber Version 9.0**Neue Features der Version 9.1 gegenüber 9.04**Budget Manager (k)**

Der Budget Manager dient zur Überwachung der Verbindungskosten über die verfügbaren Verbindungsarten, im Fokus stehen hierbei UMTS- oder GPRS- sowie WLAN-Verbindungen. Hierzu werden per Konfiguration Volumen- bzw. Zeitlimits vorgegeben. Der Anwender kann bereits vor einer Überschreitung der vorgegebenen Limits durch Hinweise gewarnt werden. Abhängig von den Einstellungen können weitere Verbindungsaufbauten bei überschrittenen Schwellwerten verboten werden.

Ein weiterer Vorteil des Budget Managers, neben der Kostenkontrolle, ist das Einschränken bzw. Unterbinden von Roaming.

**Erweiterte Zertifikatskonfiguration (k)**

In der Konfiguration des Clients kann nun eine Vielzahl individueller Zertifikatseinstellungen hinterlegt werden. Diese können dann innerhalb der Zielsysteme unabhängig voneinander ausgewählt werden, sodass die Möglichkeit besteht gegen verschiedene VPN-Gegenstellen mit unterschiedlichen Zertifikaten zu authentifizieren, z.B. zu VPN Gateway 1 mit Softzertifikat und zu Gateway 2 mit einem auf Smartcard gespeicherten Zertifikat.

**Zielsystem-Filter**

Die konfigurierten Zielsysteme können zu Gruppen zusammengefasst werden, die dann über ein Kontextmenü des Client Monitors bequem ausgewählt werden können. Dadurch kann die Übersichtlichkeit der vorhandenen Verbindungsprofile für den Anwender erhöht werden, da er nur die aktuell gewünschten Einträge einblenden lassen kann.

**Client Status Info Center**

Mit dem Client Status Info Center lässt sich der User Helpdesk optimieren. Die Log- und Fehlermeldungen sind überarbeitet und deren Aussagekräftigkeit verbessert.

Neben einer Testoption, um zu bestimmen, ob eine vorhandene Internetverbindung besteht (im LAN- und WLAN-Umfeld), steht zusätzlich eine Übersicht mit folgenden Informationen zur Verfügung:

- Client Version (inkl. Build-Nummer)
- Aktueller Verbindungsstatus (verbunden, getrennt, getrennt mit Fehler)
- Status der Client Dienste
- Aktuelle Zertifikatskonfiguration (inkl. Gültigkeit)
- VPN Benutzer-ID
- Benutzer für Management Server-Verbindung

**Neue Features der Version 9.04 gegenüber 9.03****Import von PCF-Dateien**

Über das Monitormenü des Entry Clients "Konfiguration / Profile importieren" können mit Hilfe eines Assistenten Konfigurationsdaten für die Profile eingelesen werden. Diese Profileinstellungen können vom jeweiligen Zielsystem als unterschiedliche Dateitypen erstellt werden. Sind in diesen Profileinstellungen einzelne Parameter nicht vorhanden (z. B. Passwort), werden diese vom Assistenten beim Import automatisch abgefragt. Der NCP Entry Client unterstützt folgende Dateitypen:

\*.ini, \*.pcf, \*.wgx und \*.spd.

**WISPr für komfortable Anmeldung an T-Mobile Hotspots**

Der NCP Secure Entry Client 9.04 Build 60 unterstützt die neue Hotspot-Anmeldetechnik über das WISPr-Protokoll (Wireless Internet Service Provider roaming). Damit ist die Kompatibilität zu T-Mobile Hotspots in Deutschland, Österreich, Niederlande, Tschechien und Großbritannien, sowie in Lufthansa Lounges einiger internationaler Flughäfen gewährleistet. Die Konfiguration erfolgt über die Eingabe der Zugangsdaten in das Script eines WLAN-Profiles.

### **Roaming mit IPSsec-Verbindungen**

Wird dem Client während einer Session mit wireless LAN- oder LAN-Verbindung über DHCP eine neue IP-Adresse zugewiesen wird die IPSec-Verbindung währenddessen nicht unterbrochen und muss nicht neu aufgebaut werden.

Voraussetzung: NCP Secure Server >= 7.02 Build 25.

### **SIM PIN in Konfiguration speichern**

Im Dialog zur Eingabe der SIM PIN für GPRS/UMTS-Karten wurde die Option "SIM PIN in Konfiguration speichern" hinzugefügt. Wird diese Funktion genutzt, so wird die einmal eingetragene SIM PIN für jedes Zielsystem mit dem Verbindungsmedium GPRS/UMTS verwendet und muss nicht mehr eigens eingegeben werden.

### **Verbessertes UMTS-Karten-Handling**

Das Verhalten des Secure Clients in Verbindung mit UMTS-Karten wurde verbessert, insbesondere nach Rückkehr des Systems aus dem Standby, bei Fehlverhalten oder

Nichtverfügbarkeit einer Karte. Darüber hinaus erkennt der Client bei mehreren aktiven UMTS-Geräten automatisch das Device mit gesteckter SIM-Karte.

### Neue Features der Version 9.03 gegenüber 9.01

#### **64-Bit Betriebssystem (k)**

Die neue Client Software unterstützt das 64-Bit Betriebssystem von Microsoft Windows XP.

#### **Lizenzschlüssel für Windows Betriebssysteme**

Für den Einsatz der Client Software unter den Windows Betriebssystemen XP 64 Bits und Vista 64 Bits sowie Vista 32 Bit wird ein Lizenzschlüssel ab der Version 9.0 benötigt.

#### **Treibersignierung für Windows XP**

Der NCP Intermediate-Treiber wurde für die Windows-Betriebssysteme XP 32 Bit und XP 64 Bit signiert.

#### **Integriert ist die 2-Faktor-Authentisierungslösung OTP Mobile**

OTP Mobile von T-Systems und T-Mobile nutzt das meist vorhandene Mobiltelefon für eine 2-Faktor-Authentisierung. Auf Knopfdruck berechnet es - ganz ohne Mobilfunkverbindung - ein einmalig gültiges Passwort, das der Nutzer in die Logon-Maske der Anwendung einträgt.

#### **Unterstützung von Zertifikaten mit 4096 Bit Schlüssellänge**

Für die Benutzer-Authentisierung können Server- und Client-seitig Zertifikate mit einer Schlüssellänge von 4096 Bits eingesetzt werden.

## Neue Features der Version 9.01 gegenüber 9.0

### **64-Bit Betriebssystem**

Die neue Client Software unterstützt das 64-Bit Betriebssystem von Microsoft Windows Vista.

## **Neue Features der Version 9.0 gegenüber Version 8.3**

### **Betriebssystem Windows Vista (k)**

Mit der Version 9.0 des NCP Secure Entry Clients wird neben den Betriebssystemen Windows 2000 und Windows XP auch das Betriebssystem Windows Vista unterstützt.

Die Oberfläche des Clients wurde dem Betriebssystem Windows Vista optisch angepasst, ohne den Zusammenhang zwischen den Symbolen und dem funktionalen Ablauf von Verbindungsaufbau und Authentisierung zu ändern.

Die Installation der Client Software 9.0 unter Microsoft Vista erfordert einen Lizenzschlüssel für diese Version. Unter einem älteren Lizenzschlüssel kann diese Software nicht betrieben werden. Die Eingabe eines älteren Lizenzschlüssels verursacht eine Fehlermeldung.

### **Neue Benutzeroberfläche (Monitor)**

Die Oberfläche des Clients wurde dem Betriebssystem Windows Vista optisch angepasst. Der mit Symbolen unterlegte funktionale Ablauf von Verbindungsaufbau, Verbindungsabbau und Authentisierung wurde in seiner Gestaltung noch übersichtlicher. Hinweistexte (Tooltips) erklären die einzelnen Symbole und erleichtern die Fehlersuche im Störfall. Der Status der integrierten Personal Firewall wird im Icon innerhalb der Taskleiste dargestellt.

### **Integrierte Unterstützung von weiteren Multifunktionskarten (Mobile Connect Cards)**

Ist eine Multifunktionskarte gesteckt, die vom Client erkannt wurde, wird im Monitormenü "Verbindung" der Menüpunkt "Multifunktionskarte" sichtbar.

Zu den bereits unterstützten Multifunktionskarten\* sind neu hinzugekommen:

- integrierte Karte des Lenovo Notebooks (Sierra Chipset)
- Vodafone EasyBox USB-Adapter für UMTS/GPRS.

Über den Menüpunkt "Multifunktionskarte" stehen folgende Funktionen zur Verfügung:

- Netzsuche
- UMTS bzw. GPRS aktivieren
- SIM PIN eingeben bzw. ändern

Die Funktionen "Netzsuche" und "UMTS bzw. GPRS aktivieren" können auch über das Feld zur grafischen Anzeige der Signalstärke ausgelöst werden. Dieses Feld wird immer dann geöffnet, wenn ein Profil mit der Verbindungsart "UMTS/GPRS" aus den Profil-Einstellungen selektiert wurde. Der PIN-Dialog zur Eingabe der SIM PIN erscheint immer dann, wenn in einem Profil der Mediatyp "UMTS/GPRS" konfiguriert und eine Multifunktionskarte gesteckt wurde, die der Client erkennt.

\*) siehe Kompatibilitätsliste unter: <http://www.ncp-e.com/de/support/kompatibilitaeten/umts-3g-hardware.html>

### **WLAN-Panel**

Die Anzeige des WLAN-Panels kann so konfiguriert werden, dass sie permanent den aktuellen WLAN-Status anzeigt, unabhängig vom genutzten Übertragungsmedium. Der Teleworker hat damit die Möglichkeit, laufend die Feldstärke zu überprüfen und den Mediatype nach Bedarf zu wechseln.

### **Verfeinerte Zertifikatsüberprüfung bei „automatischer Hotspot-Anmeldung“ (mittels Script)**

Ab sofort können auch die eingehenden Server-Zertifikate bei der HTTP-Authentisierung am Hotspot überprüft werden. Dies erhöht das Sicherheitsniveau mobiler Telearbeitsplätze und verringert die Gefahr von Man-in-the-Middle Attacken.

### **EAP-Authentisierung**

#### Erweiterung der Konfiguration:

Um die EAP-Anmeldung zu beschleunigen, kann der Administrator vorgeben, auf welchen Medien die EAP-Authentisierung durchgeführt werden soll.

Hierzu kann in den "EAP-Optionen" des Monitor-Menüs angegeben werden, ob die EAP-Authentisierung nur über WLAN-, LAN- oder alle Netzwerkkarten erfolgen soll. Die gewählte Einstellung gilt jeweils global für alle Einträge des Telefonbuchs. Die EAP-Authentisierung kann in einer Aktivierungsbox wie folgt eingestellt werden:

- Deaktiviert
- Für alle Netzwerkkarten
- Nur für WLAN-Karten
- Nur für LAN-Karten

### **EAP-Authentisierung vor einer Domänenanmeldung**

Dieser Parameter ermöglicht, dass bereits vor dem Zielauswahl-Dialog in der Gina die EAP-Authentisierung durchgeführt und die PIN abgefragt werden, unabhängig davon, ob zur späteren Einwahl EAP benötigt wird oder nicht. Dieser Parameter kann dann verwendet werden, wenn die NCP Gina nur für die EAP-Authentisierung eingesetzt werden soll, ohne dass eine Verbindung zu einem Zielsystem aufgebaut wird (d.h. Verwendung als reinen EAP-Client).

Die "Logon-Optionen" des Monitor-Menüs wurden hierzu um den Parameter "EAP-Authentisierung vor Zielauswahl durchführen" ergänzt

### **EAP für WPA-Verschlüsselung (k)**

Im Monitormenü kann unter "Konfiguration / WLAN-Profil" für die WPA-Verschlüsselung unter "Schlüsselverwaltung" die Option "EAP" hinzugefügt werden. Dies bewirkt, dass der Schlüssel, der während der EAP-Verhandlung erzeugt wurde, weiter für die WPA-Verschlüsselung verwendet wird. D.h. es wird WPA mit Zertifikaten unterstützt.

Voraussetzung: Konfiguration eines Zertifikates. Unabhängig von der EAP-Konfiguration wird hier immer EAP mit Zertifikat genutzt.

### **Erweiterung der IPSec Hash-Algorithmen**

Sowohl für die IKE-Richtlinien als auch für die IPSec-Richtlinien können zur Authentisierung die Algorithmen SHA 256, SHA 384 und SHA 512 Bit eingesetzt werden

### Anwendungsausführung für ein spezifisches Verbindungsprofil

Diese Feature ermöglicht, eine Applikation in Abhängigkeit vom Verbindungsprofil nach dem Verbindungsaufbau automatisch zu starten.

### HotSpot-Anmeldung

Die HotSpot-Anmeldung der 2. Generation erfolgt über das Monitor-Menü "Verbindung / HotSpot-Anmeldung" und erlaubt in der erweiterte Konfiguration die Einstellung eines alternativen Browsers und einer Default Startseite welche bei bestehender Internet Verbindung aufgerufen wird. Der alternative Browser lässt sich speziell für die Anforderungen an HotSpots konfigurieren, 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!) 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.

### Projekt-Logo im Client Monitor

Der Client Monitor wurde um ein frei gestaltbares Grafikfeld z.B. für Kundenlogo erweitert. Das sog. Projekt-Logo erscheint in einem Panel des Clients ganz unten über die gesamte Breite des Monitors. Für das Logo muss lediglich eine Ini-Datei (ProjectLogo.ini) angelegt werden, in der folgende Parameter angegeben werden können:

- Projekt-Logo für kleine Schriftarten
- Projekt-Logo für große Schriftarten
- Info-Text (ToolTip) wenn sich der Mauszeiger über dem Logo befindet
- HTML-Datei (frei gestaltbar) wenn ein Maus-Click auf das Logo erfolgt.



### Informationsfenster „Verfügbare Verbindungsarten“

Im Monitor-Menü unter "Verbindung" kann ein Informationsfenster zu den verfügbaren Verbindungsarten geöffnet werden. Dieses Fenster dient ausschließlich der Benutzerinformation über die zur Verfügung stehenden Netze und das aktuell genutzte Übertragungsmedium. Darüber hinaus werden im Fehlerfall in diesem Fenster Fehlermeldungen im Klartext angezeigt. Ob sich das Fenster bei fehlgeschlagenem Verbindungsaufbau automatisch öffnen soll oder nicht, kann per Konfiguration variabel festgelegt werden.

## **Neue Features der Version 8.3 gegenüber Version 8.2/8.1**

---

### **Integrierte WLAN-Konfiguration**

Die Konfiguration eines Zielsystems mit Verbindungsart WLAN ermöglicht das direkte Ansteuern und Konfigurieren der WLAN-Karte. Die Installation der Managementsoftware entfällt (nur unter Windows 2000/XP).

### **Automatische Medienerkennung (k)**

Diese Verbindungsart erlaubt ein einfaches Handling in wechselweise genutzten Übertragungsmedien. Der Client erkennt automatisch die aktuell verfügbaren Verbindungsarten und wählt die jeweils schnellste aus. In einer Suchroutine ist die Priorisierung der Verbindungsarten in folgender Reihenfolge festgelegt: 1. LAN, 2. WLAN, 3. DSL, 4. UMTS/GPRS, 5. ISDN, 6. MODEM. Die verfügbaren und genutzten Verbindungsarten werden dem Benutzer grafisch angezeigt.

### **Friendly Net Detection (FND)**

Mit FND erkennt der NCP Secure Entry Client automatisch, ob er sich in einem Friendly Net (FN) befindet oder nicht. Was ein FN ist, wird vom Administrator in den Firewall-Einstellungen des Monitors festgelegt. Die Signalisierung eines FN erfolgt im Monitor, indem das Firewall-Icon grün erscheint.

Integrierte intelligente Automatismen in der Personal Firewall ersetzen manuelle Eingriffe. Der Anwender muss sich nicht um die Einstellung der Personal Firewall kümmern. Je nach Kommunikationsumgebung greift der NCP Secure Entry Client dynamisch auf ein

passendes Firewall-Regelwerk zu. Versehentliches Benutzen falscher Firewall-Konfigurationen und damit Attacken auf das Firmennetz werden verhindert.

### **Priorisierung von Voice over IP (VoIP)**

Der Secure Entry Client ermöglicht eine sichere Sprachkommunikation in einem IPSec-VPN (VoIPSec). Ein integriertes Bandbreitenmanagement und Traffic Shaping garantiert die erforderlichen Quality of Service (QoS). Somit werden Sprachdaten verzögerungs- und verzerrungsfrei gesendet und empfangen.

### **Chipkartenunterstützung**

Folgende Chipkarten werden zusätzlich direkt über die PC/SC- oder CT-API-Schnittstelle unterstützt:

- Signtrust
- NetKey 2000
- TC Trust (CardOS M4)
- Telesec PKS SigG

### **EAP-Authentisierung**

Standardmäßig erfolgt die EAP-Authentisierung vor dem Verbindungsaufbau zum VPN Gateway. Soll EAP genutzt werden, ohne dass anschließend eine Verbindung über den Client (reiner EAP Client) aufgebaut werden soll, muss diese Funktion aktiviert werden. Wird EAP mit Zertifikat eingesetzt, erscheint der PIN-Dialog zur Authentisierung an den Netzwerkkomponenten. Danach kann die Zielauswahl erfolgen. Wird die Funktion nicht aktiviert, findet die EAP-Authentisierung erst nach der Zielauswahl statt.

### **Initialisierungszeit nach Netzwerk-Logon**

Zwischen Netzanmeldung und Domänenanmeldung kann Windows eine gewisse Initialisierungszeit benötigen. Diese Vorbereitungszeit für die Domänenanmeldung kann hier aktiviert und eingestellt werden. Die Windows-Anmeldung findet erst nach der hier eingestellten Initialisierungs-Zeit nach dem Verbindungsaufbau statt. Der Standardwert beträgt 45 Sekunden und kann nach Bedarf verändert werden.

### **HTTP-Authentisierung (k)**

Die "HTTP-Authentisierung" gestattet eine automatische scriptgesteuerte Anmeldung mobiler Nutzer an Hotspots (auch DSL).

Wenn der Access Point einen HTTP-Redirect ausführt, kann die Eingabe von Benutzername und Passwort in einem Browser-Fenster entfallen. Der Benutzer baut die Verbindung zum Hotspot automatisch auf, wenn die HTTP- Anwendung aktiviert ist. Eine Message-Box weist den Benutzer darauf hin, dass diese Verbindung gebührenpflichtig ist und er die Vertragsbedingungen des Hotspot-Betreibers akzeptiert.

### **Unterstützung von UDP-Encapsulation**

Dieses Feature erlaubt den UDP-Port für die IPSec-Gegenstelle frei zu wählen. Der Vorteil ist, dass IPSec-Kommunikation auch hinter Firewalls möglich ist, die nicht die Standard-IPSec-Ports freigeschaltet haben z.B. Port 80.

### **Unterstützung von Multifunktionskarten für UMTS/GPRS**

Ist eine Multifunktionskarte für UMTS/GPRS installiert, erscheint bei der Verbindungsart "GPRS/UMTS" ein zusätzliches Feld über das die Feldstärke, die Verbindungsart (UMTS oder GPRS) und das Netz angezeigt werden. Zusätzlich kann die aktuelle Verbindungsart umgeschaltet und das Netz gewechselt werden.

### **Menüpunkt zur Eingabe der SIM PIN für Multifunktionskarten**

Das Menü für die Multifunktionskarte wurde um den Punkt "SIM PIN Eingabe" erweitert. Der Menüpunkt ist nur aktiv, wenn die SIM PIN nicht konfiguriert oder nicht eingegeben wurde.

### **PIN-Handling für SIM überarbeitet**

Für die Unterstützung der Multifunktionskarte (UMTS/GPRS) wurde das PIN-Handling für die SIM komplett überarbeitet. Es erfolgt automatisch die notwendige Aufforderung zur Eingabe der PIN bzw. PUK. Wird die Eingabe der PIN/PUK abgebrochen, kann diese später über das Menü aufgerufen werden. Zusätzlich kann über das Menü die aktuelle PIN der SIM geändert werden.

**Log-Eintrag bei Verbindungsabbau (Grund des Abbaus)**

Wird eine bestehende Verbindung abgebaut, wird ins Logbuch des Clients ein Log-Eintrag mit dem Grund des Verbindungsabbaus geschrieben.

**Log-Eintrag bei Verbindungsabbau (Status der Feldstärke)**

Wird eine bestehende Verbindung abgebaut, wird ins Logbuch des Clients ein Log-Eintrag mit den letzten Statuswerten der Feldstärke für UMTS/GPRS geschrieben.

**Personal Firewall**

Die bisher verfügbare „erweiterte Firewall“ wurde grundlegend überarbeitet und verbirgt sich nun hinter der schlichten Bezeichnung „Firewall“ im Konfigurationsmenü des Monitors. Dem Secure Client steht mit der neuen Version eine vollständige und umfassende Personal Firewall zur Verfügung, die neben maximaler Sicherheit auch in punkto Bedienungsfreundlichkeit keine Wünsche offen lässt. Natürlich ist sie als fester Bestandteil perfekt auf die VPN Client Software abgestimmt.

Die 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. Auch im Fall einer Deaktivierung der Client-Software ist der vollständige Schutz des Endgerätes gewährleistet.

Die Firewall erlaubt die Erstellung von Regeln nach dem Prinzip der Stateful Packet Inspection. Darüber hinaus können neben Paketfiltern auch anwendungsabhängige Filter-Regeln definiert werden. Zusätzlich ist die Firewall in der Lage bekannte von unbekanntem und damit nicht vertrauenswürdigen Netzwerken zu unterscheiden und je nach Anbindung mit dem passenden Regelsatz zu arbeiten.

**Automatische HotSpot-Erkennung**

Damit der remote Client in jeder Phase des Verbindungsaufbaus auch in WLANs und an Hotspots ohne Zutun des Benutzers gegenüber jeglichen Attacken geschützt ist, wurde die Firewall fest in die Secure Client-Software integriert. Sie verfügt über intelligente Automatismen für eine sichere Hotspot-Anmeldung.

**Funktionsbeschreibung:**

Befindet sich ein Benutzer mit seinem Endgerät im Empfangsbereich eines öffentlichen WLAN, wählt er im Hauptmenü "Verbindung" den Menüpunkt "HotSpot-Anmeldung". Der Client sucht daraufhin automatisch den Hotspot und öffnet die Website zur Anmeldung im Standard-Browser. Nach erfolgreicher Eingabe der Zugangsdaten und Freischaltung durch den Betreiber, kann die VPN-Verbindung z.B. zur Firmenzentrale aufgebaut und sicher wie an einem Büroarbeitsplatz kommuniziert werden.

Damit der PC bei der Anmeldung im WLAN zu keiner Zeit angreifbar ist, gibt die Firewall 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. Nicht angeforderte Datenpakete werden abgewiesen. Auf diese Weise ist garantiert, dass ein öffentliches WLAN ausschließlich für die VPN-Verbindung zum zentralen Datennetz genutzt wird und kein direkter Internet-Zugriff erfolgt. Die direkte Kommunikation zum Internet unter Umgehung des VPN-Tunnels ist ausgeschlossen, aufgrund der oben beschriebenen dynamischen Firewall-Regeln, die von der integrierten Personal Firewall des Clients selbständig gesetzt werden. Für die Anmeldung über den Standard-Browser am Hotspot ist zu beachten, dass eventuell eingetragene Proxy-Einstellungen angepasst bzw. deaktiviert werden müssen. Sollte keine Hotspot-Anmeldung durchgeführt werden, wird dies durch die Meldung "Hotspot konnte nicht gefunden werden" mitgeteilt.

### **Chipkartenunterstützung**

Unterstützung der Datev-, IICS- und Telesec PKS SigG- Chipkarte. Der Client unterstützt diese Chipkarten direkt über die PC/SC-Schnittstelle.

### **Domain Name**

Neuer Parameter "Domain Name" im Telefonbuch unter "DNS/WINS". Im Telefonbuch des Secure Clients kann unter "DNS/WINS" neben einem DNS/WINS-Server auch ein "Domain Name" angegeben werden.

### **Deflate-Kompression**

Bei IPSec wird als Kompression jetzt auch "Deflate" unterstützt. In der IPSec-Richtlinien-Konfiguration kann unter den Vorschlägen nach Selektion des Protokolls "Comp" (Kompression) zwischen "LZS" und "Deflate" gewählt werden.

### **Installationsverzeichnis**

In der benutzerdefinierten Installation kann ein beliebiges Installationsverzeichnis für die Software gewählt werden. Dies ist insbesondere dann wichtig, wenn der Benutzer keine Rechte auf das System-Root-Verzeichnis hat.

### **Firewall bei der Installation aktivieren**

In der benutzerdefinierten Installation kann die Firewall-Funktion dauerhaft aktiviert werden. Dies entspricht im Telefonbuch der Link Firewall-Einstellung "Aktivierung = immer". Wird diese Einstellung während der Installation vorgenommen, so gilt sie global für alle Zielsysteme und zudem auch wenn der Client gestoppt ist. In den Einstellungen der Firewall im Monitor, die immer global gelten, ist daher die Option "Firewall bei gestopptem Client weiterhin aktivieren" eingeschaltet und nicht änderbar. Eine Deaktivierung der Firewall ist nur möglich wenn die Client Software deinstalliert und danach neu installiert wird.

### **Einsatz von EAP 802.1x**

Zur Port-Authentisierung im WLAN und an Switches unterstützt der Client EAP-MD5/TLS. Dadurch ist ein separater EAP-Client überflüssig. EAP-MD5: Benutzername und Passwort werden zur Authentisierung genutzt. Beide Größen können auch vom Zertifikat bezogen werden, das für die VPN-Verbindung genutzt wird. EAP-TLS: Zertifikate werden genutzt und aus der NCP-Zertifikats-Konfiguration gelesen. EAPOL KEY (Dynamic WEP key) wird unterstützt.

### **Statefull Packet Inspection**

Statefull Packet Inspection (SPI) ist immer aktiv. Dies bedeutet, dass SPI automatisch auch bei Verbindungen ohne VPN, z.B. Provider-Verbindungen, eingesetzt wird.

### **XAUTH-Protokoll**

Das XAUTH-Protokoll kann auch für OTP mit Netscreen eingesetzt werden.

### **(k) = kostenpflichtig**