

Universelle IPSec Client-Software für Windows CE Betriebssysteme – inklusive Windows Mobile

- ▶ **Secure Mobile Computing**
- ▶ **Integrierte, dynamische Personal Firewall**
- ▶ **Weltweite Einwahl über alle öffentlichen Funknetze**
- ▶ **Kompatibilität zu VPN Gateways unterschiedlicher Hersteller**
- ▶ **Ende-zu-Ende Sicherheitsprinzip auch an Hotspots**
- ▶ **Starke Authentisierung mit Zertifikaten – Software und Hardware**
- ▶ **Intelligentes Verbindungs-Management für transparentes Arbeiten auch bei Unterbrechungen der Funkstrecke**



Universalität

Der NCP Secure Entry CE Client ist eine Kommunikationssoftware für den universellen Einsatz in beliebigen Remote Access VPN-Umgebungen. Auf Basis des IPSec-Standards können hochsichere Datenverbindungen zu VPN-Gateways aller namhaften Anbieter hergestellt werden. Der Datentransfer erfolgt über beliebige öffentliche Funknetze und das Internet sowie Nahbereichs-Funknetze wie Wireless LANs am Firmengelände und an Hotspots. Mobile Teleworker können beispielsweise mittels PDA, MDA oder TabletPC von jedem Standort auf zentrale Datenbestände und Anwendungen zugreifen. Ein weiteres interessantes Einsatzgebiet ist die mobile Datenerfassung z.B. Bestandsaufnahme im Warenlager mit PDAs über einen integrierten Barcodeleser und Datenübertragung via WLAN.

Sicherheit

Universelle Einsatzmöglichkeiten fordern umfangreiche Sicherheitsmechanismen zur Abwehr von Attacken in jeder Remote Access-Umgebung. Auch an Hotspots während des An- und Abmeldevorganges des Teleworkers. Die wichtigsten, integrierten Security-Bausteine sind neben dem VPN-Tunneling: Datenverschlüsselung, eine dynamische Personal Firewall, die Unterstützung von OTP-Token (One Time Password) 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 Sicherheitskriterium 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 erfolgen – für den Anwender nicht veränderbar - grundsätzlich durch den Administrator. Der NCP-Dialer bietet zudem Schutz vor kostenintensiven Fremddialern.

Komfort

„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. Der mobile Anwender arbeitet in der gewohnten Weise wie an einem Büroarbeitsplatz. 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. Im Falle von E-Mail-Pushdiensten sorgt ein spezieller Verbindungsmodus für den automatischen Wiederaufbau des VPN-Tunnels zum zentralen VPN-Gateway. Der Teleworker bleibt somit immer erreichbar.

IPSec- und CE-Kompatibilität

Siehe www.ncp.de/deutsch/services/index.html

Technische Daten

<p>System Anforderungen</p> <p>Mobiles Endgerät</p> <p>Konfigurations-PC</p>	<p>Betriebssystem: Windows CE 3.0 (Handheld PC 2000, Pocket PC 2000), Windows CE.net 4.2 (Windows Mobile 2003 for PocketPC, Windows Mobile 5.0 for Pocket PC bzw. for Smartphone, Windows Mobile 6.0 Ausstattung: StrongARM processor (min. 200 MHz); 3.3 MB Program Memory, 2.1 MB Speicher; WAN oder WLAN Adapter</p> <p>Betriebssystem: Windows 98SE, NT (v.4.0 SP5), 2000, XP; 32 MB RAM, Ausstattung: min. 10 MB Arbeitsspeicher, MS Active Sync v.4.x oder höher</p>
<p>Security Features</p>	<p>Der Entry CE Client unterstützt alle IPSec Standards nach RFC und erfüllt auch die höchsten Sicherheitsanforderungen.</p>
<p>Personal Firewall</p>	<p>Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (Auswertung von: aktueller Netzwerkadresse, IP-Adresse und MAC-Adresse des DHCP-Servers); Secure Hotspot Logon; differenzierte Filterregeln bezüglich: Protokolle, Ports und Adressen</p>
<p>Virtual Private Networking (VPN)</p>	<p>IPSec (Layer 3 Tunneling), RFC-konform; IPSec-Proposals können determiniert werden durch das IPSec -Gateway (IKE, IPSec Phase 2); Event log; Block und Central Tunneling; MTU Size Fragmentation und Reassembly, DPD; NAT-Traversal (NAT-T); IPSec Modes: Tunnel Mode, Transport Mode</p>
<p>Verschlüsselung (Encryption)</p>	<p>Symmetrische Verfahren: AES 128,192,256 Bits; Blowfish 128,448 Bits; Triple-DES 112,168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 2048 Bits; Diffie-Hellman Groups 1,2,5 Seamless Rekeying (PFS); Hash Algorithmen: SHA1, MD5</p>
<p>Authentisierungsverfahren</p>	<p>IKE (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP); PFS; MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): erweiterte Authentifikation gegenüber Switches und Access Points auf Basis von Zertifikaten (Layer 2); Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards; Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready.</p>
<p>Starke Authentisierung - Standards</p>	<p>X.509 v.3 Standard; PKCS#11 Interface für Verschlüsselungs-Tokens (Smart Cards and MMC Flash Memory Cards); Smart Card Betriebssysteme: TCOS 1.2 und 2.0; Smart Card Reader Interfaces: PC/SC, CT-API; PKCS#12 Interface für Private Schlüssel in Soft-Zertifikaten</p>
<p>Networking Features</p>	<p>LAN Emulation: Virtual Ethernet-Adapter mit NDIS-Interface oder Transparent Mode</p>
<p>Netzwerkprotokolle</p>	<p>IP</p>
<p>Dialer</p>	<p>PPC Connection Manager, NCP Secure Dialer, Microsoft RAS Dialer (für ISP Einwahl mittels Einwahl-Script)</p>
<p>IP Address Allocation</p>	<p>DHCP (Dynamic Host Control Protocol); DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server</p>
<p>Übertragungsmedien</p>	<p>WLAN (WiFi), GSM (incl. HSCSD), GPRS, UMTS; Internet; analoge Modems (Mobiltelefone über Infrarot oder Bluetooth).</p>
<p>Line Management</p>	<p>DPD mit konfigurierbarem Zeitintervall; WLAN-Roaming (Handover)</p>
<p>Datenkompression</p>	<p>IPCOMP (Izs), Deflate</p>
<p>Point-to-Point Protocolle</p>	<p>PPP over GSM, PPP over PSTN, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP</p>
<p>Internet Society RFCs und Drafts</p>	<p>RFC 2401 –2409 (IPSec), RFC 3498, RFC 3947: IP Security Architecture, ESP, HMAC-MD5-96, HMAC-SHA-1-96, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP</p>
<p>Client Monitor Grafische Benutzeroberfläche</p>	<p>Mehrsprachig (Deutsch, Englisch); Verbindungsstatistik, Log-Files, Trace-Werkzeug für Fehlerdiagnose; Ampelsymbol für Anzeige des Verbindungsstatus. Konfigurations- und Profil-Management mit Passwortschutz</p>

Eine 30-Tage Vollversion des Secure Entry CE Clients können Sie hier kostenlos testen:
http://www.ncp.de/deutsch/services/testsoftware/index_entry.html