

Universelle, zentral managebare IPsec Client-Software für Windows Mobile (CE)

- ▶ **Secure Mobile Computing**
- ▶ **Integrierte, dynamische Personal Firewall**
- ▶ **Weltweite Einwahl in das Firmennetz**
- ▶ **Kompatibilität zu VPN Gateways unterschiedlicher Hersteller**
- ▶ **Starke Authentisierung mit Zertifikaten**
- ▶ **Ende-zu-Ende-Sicherheit auch an Hotspots**
- ▶ **Zentrales Management**



Universalität

Der NCP Secure Enterprise Windows Mobile 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 Barcodeleser im Warenlager und Datentransfer via WLAN in das zentrale Warenwirtschaftssystem.

Sicherheit

Universelle Einsatzmöglichkeiten fordern umfangreiche Sicherheitsmechanismen zur Abwehr von Angriffen 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-Tokens (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure). Mittels der Personal Firewall können Regelwerke für Ports, IP-Adressen und Segmente sowie Applikatio-

nen 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 können zentral vom Administrator eingegeben und durch den Anwender nicht veränderbar eingestellt werden. Mechanismen des zentralen Managements (s.u.) ermöglichen eine automatische Übernahme aller Konfigurationsparameter in den Client. 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. 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.

Zentrales Management*

Die NCP Secure Enterprise Management Software bietet alle Funktionalitäten und Automatismen für die Inbetriebnahme und den Betrieb von Remote Access-VPNs von zentraler Stelle (Single-Point-of-Administration).

*) optional

Technische Daten

<p>System Anforderungen 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.x, Windows Mobile 7 (i.P.)) Ausstattung: StrongARM processor (min. 200 MHz); 3.3 MB Program Memory, 2.1 MB Speicher; Betriebssystem: Windows 7, Windows Vista, Windows XP (alle 32/64 Bit); 32 MB RAM, Ausstattung: min. 20 MB Speicher, MS Active Sync V.4.x oder höher</p>
<p>Security Features</p>	<p>Der Enterprise Client unterstützt alle gängigen IPsec Standards nach RFC</p>
<p>Personal Firewall Firewall Configuration*</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, Schutz des LAN-Adapters, zentrale Administration mit Client Firewall Configuration Plug In*</p>
<p>Virtual Private Networking</p>	<p>IPsec (Layer 3 Tunneling), RFC-konform; IPsec-Proposals können determiniert werden durch das IPsec-Gateway (IKE, IPsec Phase 2); Event log; Kommunikation nur im Tunnel; MTU Size Fragmentation und Reassembly, DPD, NAT-Traversal (NAT-T); IPsec Tunnel 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>Authentisierungs- verfahren</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; PAP, CHAP, 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 und USB Tokens; Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready.</p>
<p>Starke Authentisierung – Standards PKI Enrollment*</p>	<p>X.509 v.3 Standard; Entrust Ready PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); Smart Card Betriebssysteme: TCOS 1.2 and 2.0; Smart Card ReaderInterfaces: PC/SC, CT-API; PKCS#12 Interface für Private Schlüssel in Soft Zertifikaten; PIN-Richtlinie; administrative Vorgabe für die Eingabe beliebig komplexer PINs; Revocation: EPRL (End-entity Public-key Certificate Revocation List, <i>vorm. CRL</i>), CARL (Certification Authority Revocation List, <i>vorm. ARL</i>), OCSP. CMP* (Certificate Management Protocol),</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 (inkl. HSCSD), GPRS, UMTS, Internet, analoge Modems (Mobiltelefone)</p>
<p>Line Management</p>	<p>DPD mit konfigurierbarem Intervall; WLAN-Roaming (Handover);</p>
<p>Datenkompression</p>	<p>Stac (lzs), Deflate</p>
<p>Point-to-Point Protokolle</p>	<p>PPP over ISDN, 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); intuitive Bedienung; Konfiguration, Verbindungsstatistik, Log-Files, Trace-Werkzeug für Fehlerdiagnose; Ampelsymbol für Anzeige des Verbindungsstatus; Konfigurations- und Profil-Management mit Passwortschutz</p>

*) Voraussetzung: NCP Secure Enterprise Management