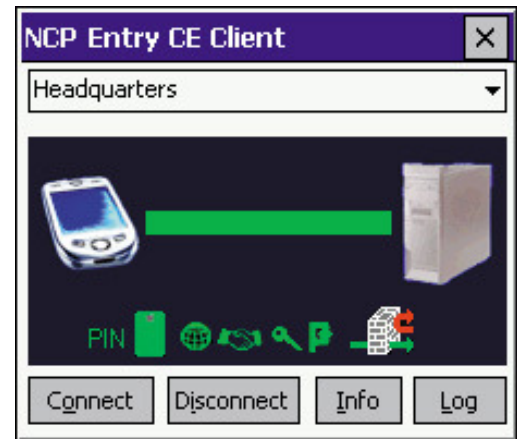


## Versatile IPSec client software for Windows CE operating systems – including Windows Mobile 5.0

- ▶ **Secure Mobile Computing**
- ▶ **Worldwide dial-in via all public networks**
- ▶ **Compatible with VPN gateways from different manufacturers**
- ▶ **End-to-end security principle even at hotspots**
- ▶ **Integrated, dynamic personal firewall**
- ▶ **Strong authentication with certificates – software and hardware**
- ▶ **Intelligent connection management for transparent work even if the wireless path is interrupted**



### Versatility

The NCP Secure Entry CE Client is a communication software product for universal implementation in any remote access environment. It can be implemented in any Virtual Private Network and terminate against any IPSec gateway (e.g., concentrator, router, firewall). The connection can be established over any wireless network, be it public or private. Mobile teleworkers can access central data repositories and applications via PDA, smartphone, or TabletPC from any location.

Another application is mobile data acquisition. PDAs with integrated barcode readers are used for taking stock in the warehouse. The data is transferred via WLAN.

### Security

Universal implementation possibilities require security mechanisms to repel attacks in any remote access environment. Even at hotspots during the login and logoff process. The Entry Client supports all IPSec standards as set in the RFCs. The product meets the highest security requirements. Support of certificates provides strong user authentication in a Public Key Infrastructure. An integrated personal firewall shields against attacks from the Internet. The latest encryption algorithms protect sensitive data in transit.

### Convenience

"Easy-to-use" – simple installation and operation of the client software. Convenience is ensured by the integrated configuration wizard for the configuration PC and an intuitive graphic user interface on the mobile end device. The mobile user works in precisely the same manner as he does on his office workstation. Interruptions of a wireless connection while transferring data e.g. wireless failures, or when changing access points in the WLAN, have no effect on these transparent work methods. For E-mail push services a special connection mode ensures automatic re-establishment of the VPN tunnel to the central VPN gateway. The teleworker can always be reached.

### \*IPSec Compatibility

Compatible IPSec gateways: Astaro, Bintec, Check Point, Cisco, Concept04, Cosine, D-Link, F-Secure, Fortinet, FreeSwan, Genua, Intermate, Lancom, Linksys, NCP, Netgear, Netscreen, OpenBSD, OpenSwan, Pyramid, Smoothwall, SonicWall, Symantec, TelcoTech, WatchGuard.

For further information see:

[www.ncp.de/english/services/ipseckompat](http://www.ncp.de/english/services/ipseckompat)

## Technical Data

<p><b>System Requirements</b></p> <p>Mobile end device</p> <p>Configuration PC</p>	<p>Platform: Windows CE 3.0 (Handheld PC 2000, Pocket PC 2000), Windows CE.net 4.2 (Windows Mobile 2003 for PocketPC, Windows CE 5.0 (Windows Mobile 5.0 for PocketPC); StrongARM processor (min. 200 MHz); 3.3 MB Program Memory, 2.1 MB Storage; WAN or WLAN adapter</p> <p>Platform: Windows 98se, NT (v.4.0 SP5), 2000, XP; 32 MB RAM, min. 10 MB free on HD, MS Active Sync v.4.x or higher</p>
<p><b>Security Features</b></p>	<p>The Entry Client supports all IPSec standards as set in the RFCs. The product meets the highest security requirements.</p>
<p><b>Personal Firewall</b></p>	<p>Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (check of current network address against IP address and MAC address of DHCP server); Secure Hotspot Logon; differentiated filter rules for protocols, ports and addresses</p>
<p><b>Virtual Private Networking</b></p>	<p>Native IPSec (Layer 3 tunneling), RFC conform; IPSec proposals can be determined by IPSec gateway (IKE, IPSec Phase 2); event log; block and central tunneling; MTU size fragmentation and reassembly; DPD; NAT traversal (NAT-T); IPSec Modes: Tunnel Mode, Transport Mode</p>
<p><b>Encryption</b></p>	<p>Supported Symmetric Ciphers: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits; Dynamic key exchange protocols: RSA up to 2048 bits; Diffie-Hellman groups 1,2,5 Seamless rekeying (PFS); Hash process: SHA1, MD5</p>
<p><b>Authentication Methods</b></p>	<p>IKE (aggressive and main mode), Quick Mode; XAUTH for extended user authentication; IKE config mode for dynamic allocation of a virtual address from the internal address range (private); MS CHAP V.2; PFS; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): extended authentication against switches and access points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): extended, certificate based authentication against switches and access points (Layer 2); Support of certificates in a PKI: Soft Certificates, Smart Cards; Pre-shared secrets; One-Time Passwords &amp; Challenge Response systems; RSA SecurID Ready.</p>
<p><b>Strong Authentication Standards</b></p>	<p>X.509 v.3 certificate format; PKCS#11 interface for cryptographic tokens (Smart Cards and MMC flash memory cards); Smart Card OS: TCOS 1.2 and 2.0; Smart Card reader interfaces: PC/SC, CT-API; PKCS#12 interface for private keys stored in Soft Certificates</p>
<p><b>Networking Features</b></p>	<p>LAN Emulation: virtual Ethernet adapter with NDIS interface, or transparent mode</p>
<p><b>Network Protocol</b></p>	<p>IP</p>
<p><b>Dialer</b></p>	<p>PPC Connection Manager, NCP Secure Dialer, Microsoft RAS Dialer (for ISP dial-in via dial-in script)</p>
<p><b>IP Address Allocation</b></p>	<p>DHCP (Dynamic Host Control Protocol); DNS: dial into the central gateway with changing public IP addresses through IP address query via a DNS server</p>
<p><b>Communications Media</b></p>	<p>WLAN (WiFi), GSM (incl. HSCSD), GPRS, UMTS; Internet; analog modems (cell phones via Infra Red or Bluetooth).</p>
<p><b>Line Management</b></p>	<p>DPD for connection monitoring; WLAN Roaming (handover)</p>
<p><b>Compression</b></p>	<p>IPCOMP (lzs), Deflate</p>
<p><b>Point-to-Point Protocols</b></p>	<p>PPP over GSM, PPP over PSTN, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP</p>
<p><b>Internet Society RFCs and Drafts</b></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, UDP encapsulation (NAT-T), IPCOMP</p>
<p><b>Client Monitor Graphical User Interface</b></p>	<p>Multilingual (German, English); connection statistics, log files, trace tool for error diagnosis; traffic light icon displays the connection states. Configuration and profile management with password protection</p>

More information on NCP Secure Communication products is available on the Internet at: [www.ncp.de](http://www.ncp.de)