

## Versatile IPsec client software for Windows 32 operating systems (also Vista)

- ▶ **Highly secure, encrypted access to the central data network**
- ▶ **Worldwide dial-in via all public cable networks and wireless networks**
- ▶ **Compatible with VPN gateways from different manufacturers**
- ▶ **Support of all IPsec protocol extensions**
- ▶ **Integrated personal firewall**
- ▶ **Strong authentication with certificates**
- ▶ **Integrated support of Mobile Connect Cards**
- ▶ **Customer banner field**



### Versatility

The NCP Secure Entry Client is an intelligent client software that 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 wired or wireless networks, be it public or private. Data are transferred independent of the media type via stationary networks, public wireless networks, LANs (e.g. in the branch office network), the Internet, as well as wireless LANs (WiFi) on corporate campuses and at hotspots. Teleworkers can use any end device to access central data repositories and applications from any location. Voice Data (VoIP) are transmitted with priority. Integrated QoS (Quality of Service) ensures communication without delay, and without distortion.

### 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 PKI. An integrated personal firewall shields against attacks from the Internet. The latest encryption algorithms protect sensitive data in transit. The NCP dialer also offers protection against cost-intensive outside dialers.

### Convenience

"Easy-to-use" - the NCP Secure Entry Client offers simple installation and simple operation. The integrated installation wizard and an intuitive graphic user-interface ensure convenient operation. Integrated support of Mobile Connect Cards for UMTS, GPRS, WLAN means that additional installation of the user interface supplied by the card manufacturers is not necessary. The user works from any location, just like he does on his/her office workstation. Domain logon is also every bit as convenient and familiar as it is in the local network. Prior to logging onto the domain controller the Client sets up a VPN tunnel to the central VPN gateway. Thus all the logon data are already encrypted for secure transmission.

The user doesn't "notice" the Client software at all during his remote access session. The Client software monitors and secures every data connection of the respective application, automatically in background.

### IPsec Compatibility

Compatible IPsec gateways: ARKOON, Astaro, Bintec, Check Point, Cisco, Concept04, Cosine, D-Link, F-Secure, Fortinet, FreeSwan, Genua, Intermate, Lancom, Linksys, NCP, Netgear, Netscreen, OpenBSD, OpenSwan, Panda, 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

|  |   |
|--|---|
| <b>System Requirements</b>                     | Windows (32 Bit): Windows Vista (x86), Windows 2000, Windows XP (inkl. SP2)<br>Windows Vista (x64) i.V.<br>64 MB RAM, min. 10 MB free on HD; WAN and/or LAN adapter   |
| <b>Security Features</b>                       | The Entry Client supports all IPsec standards as set in the RFCs. The product meets the highest security requirements.  |
| <b>Personal Firewall</b>                       | 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 applications, protocols, ports, addresses and links; LAN adapter protection  |
| <b>Virtual Private Networking</b>              | 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;  |
| <b>Encryption</b>                              | Supported Symmetric Ciphers: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits<br>Dynamic key exchange protocols: RSA up to 2048 bits; Diffie-Hellman groups 1,2,5<br>Seamless rekeying (PFS); Hash process: SHA1, MD5   |
| <b>Authentication Methods</b>                  | IKE (aggressive and main mode), Quick Mode; XAUTH for extended user authentication;<br>IKE config mode for dynamic allocation of a virtual address from the internal address range (private);<br>PAP/CHAP, MS CHAP V.2; PFS;<br>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);<br>Support of certificates in a PKI: Soft Certificates, Smart Cards & USB Tokens;<br>Pre-shared secrets; One-Time Passwords & Challenge Response systems; RSA SecurID Ready. |
| <b>Strong Authentication Standards</b>         | X.509 v.3 certificate format, also Entrust Ready;<br>PKCS#11 interface for cryptographic tokens (USB and Smart Cards); Smart Card OS: TCOS 1.2 and 2.0; Smart Card reader interfaces: PC/SC, CT-API;<br>PKCS#12 interface for private keys stored in Soft Certificates;<br>PIN policy; administrative rule for any complex PIN entry;<br>Revocation: EPRL (End-entity Public-key Certificate Revocation List, <i>formerly CRL</i> ), CARL (Certification Authority Revocation List, <i>formerly ARL</i> ), OCSP.  |
| <b>Networking Features</b>                     | LAN Emulation: virtual Ethernet adapter with NDIS interface   |
| <b>Dialer</b>                                  | NCP Secure Dialer, Microsoft RAS Dialer (for ISP dial-in via dial-in script);<br>International dial-in via GoRemote (formerly GRIC), UuNet, Infonet, MCI  |
| <b>IP Address Allocation</b>                   | DHCP (Dynamic Host Control Protocol), DNS: dial into the central gateway with changing public IP addresses through IP address query via a DNS server  |
| <b>Communications Media</b>                    | Wired: PSTN, ISDN, xDSL, Cable, LAN;<br>Wireless: WLAN, GSM (incl. HSCSD), GPRS, UMTS; HSDPA; Internet.   |
| <b>Line Management</b>                         | DPD for connection monitoring; Shorthold mode; WLAN Roaming (handover);<br>Channel bundling (dynamic in ISDN) with freely configurable threshold value, short hold, timeout (controlled by time and charges); budget manager;   |
| <b>Compression</b>                             | IPCOMP (lzs), Deflate   |
| <b>Point-to-Point Protocols</b>                | PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet;<br>LCP, IPCP, MLP, CCP, PAP, CHAP, ECP   |
| <b>Additional Features</b>                     | Voice over IP priority (QoS), UDP encapsulation   |
| <b>Internet Society RFCs and Drafts</b>        | RFC 2401 –2409 (IPsec), RFC 3498, RFC 3947:<br>IP Security Architecture, ESP, HMAC-MD5-96, HMAC-SHA-1-96, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT traversal, UDP encapsulation (NAT-T), IPCOMP  |
| <b>Client Monitor Graphical User Interface</b> | Multilingual (German, English, Polish); intuitive operation; configuration connection management and monitoring, connection statistics, log files, trace tool for error diagnosis; traffic light icon displays the connection states; integrated support of Mobile Connect Cards (PCMCIA).<br>Configuration and profile management with password protection, authorizations adjustable per function, display and show parameter fields.   |

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