

In North America,
contact DCS LLC
www.dimante.net
sales@dimante.net

Universal IPSec Client software for Windows 32/64-bit operating systems

- ▶ **Highly secure access to the central data network**
- ▶ **Integrated, dynamic personal firewall**
- ▶ **Compatible with VPN gateways from different manufacturers**
- ▶ **Support of all IPSec protocol extensions**
- ▶ **Strong authentication with certificates – software and hardware**
- ▶ **Integrated support of Mobile Connect Cards**
- ▶ **Text field in the Client Monitor can be freely designed**



Universality

The NCP Secure Entry Client for Windows 32 and Windows 64 - operating systems is a communication software product for universal implementation in any remote access VPN environment. Highly secure data connections to VPN gateways from all well-known suppliers can be established on the basis of IPSec standards. Data are transferred independent of media type (any network) via stationary networks, public wireless networks, LANs (e.g. in the branch office network), the Internet, as well as wireless networks such as wireless LANs 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 delay-free and distortion-free communication.

Security

Universal implementation possibilities require security mechanisms that repel attacks in any remote access environment. Even at hotspots during the logon and logoff process. In addition to VPN tunneling the most important integrated components are: data encryption, a dynamic personal firewall, support of OTP (One-Time Password tokens) and certificates in a PKI (Public Key Infrastructure). Use the Personal Firewall to define policies for: Ports, IP addresses and segments, as well as applications. An additional safety criterion is "Friendly Net Detection", i.e. automatic detection of secure and non-secure networks. The appropriate firewall rules are

activated or deactivated depending on whether a friendly net is detected. All configurations are always executed by the administrator - they cannot be changed by the user.

Convenience

"Easy-to-use" - the NCP Secure Entry Client offers simple installation and simple operation. A graphic, intuitive user interface provides information on all connection states. Detailed log information can also be viewed via this interface. The integrated configuration wizard enables easy creation of phonebook entries. Integrated support of Mobile Connect Cards for UMTS, GPRS, and WLAN means that additional installation of the user interface supplied by the card manufacturers is not necessary. The teleworker works transparently and securely at any location (mobile or stationary); in the same manner he/she works at 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.

Technical data

Operating systems	Windows (32-bit): Windows Vista (x86), Windows 2000, Windows XP (incl. SP2) Windows (64-bit): Windows Vista (x64)
Security features	The Entry Client supports all IPSec standards in accordance with RFC and also satisfies the most rigorous security requirements.
Personal Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (analysis of: current network address, IP address and MAC address of the DHCP server); secure hotspot logon; differentiated filter rules relative to: Protocols, ports and addresses, LAN adapter protection
Virtual Private Networking	IPSec (Layer 3 Tunneling), RFC-conformant; IPSec proposals can be determined through the IPSec gateway (IKE, IPSec Phase 2); Event log; communication only in the tunnel; MTU size fragmentation and reassembly, DPD, NAT-Traversal (NAT-T); IPSec modes: tunnel mode, transport mode
Encryption	Symmetric processes: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits; dynamic processes for key exchange: RSA to 2048 bits; Diffie-Hellman Groups 1,2,5 seamless rekeying (PFS); hash algorithms: SHA1, MD5
Authentication processes	IKE (Aggressive mode and Main Mode), Quick Mode; XAUTH for extended user authentication; IKE config mode for dynamic assignment of a virtual address from the internal address pool (private IP); PFS; PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): Extended authentication relative to switches and access points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): Extended authentication relative to switches and access points on the basis of certificates (Layer 2); support of certificates in a PKI: Soft certificates, smart cards, and USB tokens: Pre-shared secrets, one-time passwords, and challenge response systems; RSA SecurID ready.
Strong authentication - standards	X.509 v.3 Standard; Entrust Ready PKCS#11 interface for encryption tokens (USB and smart cards); smart card operating systems: TCOS 1.2 and 2.0; smart card reader interfaces: PC/SC, CT-API; PKCS#12 interface for private keys in soft certificates; PIN policy; administrative specification for PIN entry in any level of complexity; revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly <i>CRL</i>), CARL (Certification Authority Revocation List, formerly <i>ARL</i>), OCSP.
Networking features	LAN emulation: Ethernet adapter with NDIS interface
Dialers	NCP Secure Dialer, Microsoft RAS Dialer (for ISP dial-in via dial-in script) connection manager for international dial-in via GoRemote (formerly <i>GRIQ</i>), UuNet, Infonet, MCI
IP address allocation	DHCP (Dynamic Host Control Protocol), DNS: Dial-in to the central gateway with changing public IP addresses through IP address query via DNS server
Transmission media	Stationary networks: analog telephone network, ISDN, xDSL, LAN wireless networks: WLAN, GSM (incl. HSCSD), GPRS, UMTS, HSDPA, Internet
Line management	DPD with configurable time interval; Short Hold Mode; WLAN roaming (handover); channel bundling (dynamic in ISDN) with freely configurable threshold value; timeout (controlled by time and charges); budget manager
Data compression	Stac (lzs), deflate
Additional features	Prioritization of VoIP (QoS), UDP encapsulation
Point-to-Point Protocols	PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Internet Society RFCs and drafts	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
Client Monitor graphic user interface	Multilingual (German, English, Polish); intuitive operation; configuration, connection management and monitoring, connection statistics, log-files, trace tool for error diagnosis; traffic light icon for display of connection status; integrated support of Mobile Connect Cards (PCMCIA); password protected configuration management and profile management, configuration parameter lock

More information on NCP Secure Communication products is available on the Internet at: www.ncp.de
 You can test a full version of the Secure Entry Linux Client for 30 days, free of charge here:
<http://www.ncp.de/english/download/testsoftware/index.html>