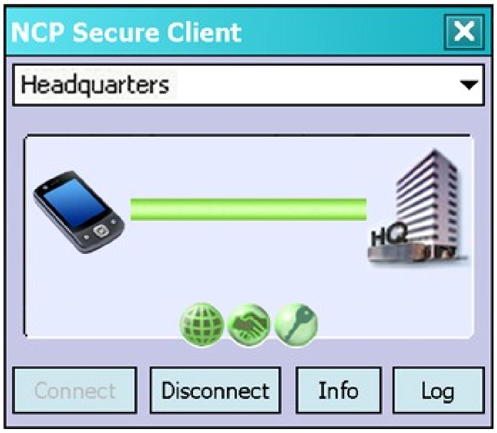
Data Sheet

NCP Secure Enterprise Windows Mobile Client

Universal, centrally manageable IPsec client software for Windows Mobile

- Secure mobile computing
- Integrated, dynamic personal firewall
- Worldwide dial-in to the corporate network
- Compatible with VPN gateways from different manufacturers
- Strong authentication with certificates
- End-to-end security even at hotspots
- Central management



Universality

The NCP Secure Enterprise Windows Mobile Client is a component of the holistic NCP Secure Enterprise Solution. The communication software is used for universal teleworking in any remote access VPN environment. Highly secure data connections, also to VPN gateways from all well-known suppliers, can be established using IPsec standards. The data is transferred over any public wireless network, the Internet, as well as wireless networks such as wireless LANs within his corporate environment and at hotspots. For example mobile teleworkers around the world can access central data repositories and applications via Pocket PCs, handhelds, or Tablet PCs. Another interesting area of implementation is mobile data acquisition, for example using PDAs with integrated barcode reader in warehouses and data transfer via WLAN into the central materials management system.

Security

Universal implementation possibilities require comprehensive security mechanisms for defense against 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). Policies for ports, IP addresses and segments, as well as applications can be defined via the Personal Firewall. An additional security criterion is "Friendly Net Detection" (location awareness) 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 can be entered centrally by the administrator and set so that they cannot be changed by the user. Central management mechanisms (see below) enable automatic transfer of all configuration parameters to the Client. The NCP Dialer also offers protection against cost-intensive outside dialers.

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. 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.

Central management*

NCP Secure Enterprise Management Software offers all functionalities and automation mechanisms for commissioning and operating remote access VPNs from a central point (Single-Point-of-Administration).

*) optional

System Requirements Mobile End Device

Operating system: 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 Pocket PC or for Smartphone, Windows Mobile 6.x, Windows Mobile 7 (i.p.)
Configuration: StrongARM processor (min. 200 MHz); 3.3 MB program memory, 2.1 MB memory; WAN or WLAN adapter

System Requirements Configuration PC

Operating system: Windows 7, Windows Vista, Windos XP (all 32/64 bit); 32 MB RAM,
Configuration: At least 20 MB RAM, MS Active Sync v. 4.x or higher

Security Features

The Enterprise Client supports all major IPsec standards in accordance with RFC

Personal Firewall
Firewall Configuration*

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, central administration with Client firewall configuration plug-in*

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 tunnel 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 PKI Enrollment*	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 CRL), CARL (Certification Authority Revocation List, formerly ARL), OCSP CMP* (Certificate Management Protocol)
Networking Features	LAN emulation: virtual Ethernet adapter with NDIS interface or transparent mode
Network Protocols	IP
Dialers	PPC Connection Manager, NCP Secure Dialer, Microsoft RAS Dialer (for ISP dial-in via dial-in script)
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	WLAN (WiFi), GSM (incl. HSCSD), GPRS, UMTS, Internet, analog modems (mobile phones)
Line Management	DPD with configurable time interval; WLAN roaming (handover)
Data Compression	Stac (lzs), deflate
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 Graphical User Interface	Multilingual (German, English); Intuitive operation; Configuration, connection statistics, log-files, trace tool for error diagnosis; Traffic light icon for display of connection status; Password protected configuration management and profile management.

*) Prerequisite: NCP Secure Enterprise Management