NCP Secure Entry Windows Mobile Client

Next Generation Network Access Technology

Universal IPsec Client software for Windows Mobile operating systems

- ▶ **Integrated, dynamic personal firewall**
- ▶ **Compatible with VPN gateways from different manufacturers**
- ▶ **Worldwide dial-in over all public radio networks**
- ▶ **End-to-end security principle even at hotspots**
- ▶ **Strong authentication**
- ▶ **Compatible with VPN gateways from different manufacturers**
- ▶ **Free 30 day full version**

Universality

The NCP Secure Entry Client for Windows Mobile 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 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 can access central data repositories and applications via PDA, MDA, or TabletPC from any location. Another interesting area of application is mobile data acquisition, e.g. taking stock in the warehouse with PDAs via an integrated barcode reader and data transfer via WLAN.

Security

Universal implementation possibilities require security mechanisms that repel attacks in any remote access environment. Even at hotspots during the logon and logoff processes of the teleworker. 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" (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 are always executed by the administrator - they cannot be changed by the user.

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. Thus the teleworker can always be reached.

IPsec compatibility

See
http://www.ncp-e.com/en/support/compatibility.html

NCP engineering, Inc. ▪ Mountain View, CA 94041 Phone: +1 650 316 6273 ▪ Email info@ncp-e.com
DS EYWM 2.2 ▪ Technical specifications subject to change
Page 1 of 2

Technical data

System Requirements	
Mobile End Device	Operating system: Windows Mobile 2003 for PocketPC, 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;
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 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
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-conformant; IPsec proposals can be determined through the IPsec gateway (IKE, IPsec Phase 2); Event log; block and central tunneling; 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; Pre-shared secrets, one-time passwords, and challenge response systems; RSA SecurID ready.
Strong Authentication - Standards	X.509 v.3 standard; PKCS#11 interface encryption tokens (smart cards and MMC Flash Memory Cards); smart card operating systems: TCOS 1.2 and 2.0; smart card reader interfaces: PC/SC, CT-API; PKCS#12 interface for keys in soft certificates
Networking Features	LAN emulation: virtual Ethernet adapter with NDIS interface or transparent mode
Network Protocols	IP
Dialers	PPC Connection Manager, 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 via infrared or Bluetooth).
Line Management	DPD with configurable time interval; WLAN roaming (handover);
Data Compression	Stac (lzs), deflate
Point-to-Point Protocols	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); connection statistics, log files, trace tool for error diagnosis; stop light icon for display of connection status. Configuration management and profile management with password protection

You can try out a free, 30-day full version of Secure Entry Windows Mobile Client here:
http://www.ncp-e.com/en/downloads/software.html

NCP engineering, Inc. ▪ Mountain View, CA 94041 Phone: +1 650 316 6273 ▪ Email info@ncp-e.com
DS EYWM 2.2 ▪ Technical specifications subject to change
Page 2 of 2