

Universelle VPN Client Software für mobile Endgeräte mit dem Betriebssystem Symbian

- ▶ **Secure Mobile Computing**
- ▶ **Kompatibilität zu VPN Gateways unterschiedlicher Hersteller**
- ▶ **Starke Authentisierung**
- ▶ **Integrierte, dynamische Personal Firewall**
- ▶ **Weltweite Einwahl über alle öffentlichen Funknetze**
- ▶ **Ende-zu-Ende Sicherheit auch an Hotspots**
- ▶ **Intelligentes Verbindungs-Management für transparentes Arbeiten auch bei Unterbrechungen der Funkstrecke**



Universalität

Der NCP Secure Symbian Client ist eine Kommunikationssoftware für die universelle Einwahl in das Firmennetz auf Basis eines Virtual Private Networks (VPN). Teleworker können mit ihrem mobilen Endgerät von jedem beliebigen Standort hochsicher auf zentrale Datenbestände und Ressourcen zugreifen. Als Gegenstelle können neben dem NCP Secure Enterprise Server alle VPN Gateways, die auf dem IPSec-Standard nebst allen Protokollerweiterungen basieren, eingesetzt werden. Der Secure Symbian Client unterstützt entsprechend der universellen Produkt- und ganzheitlichen Lösungsphilosophie von NCP den Datentransfer über alle öffentlichen Netze. Welches Übertragungsmedium genutzt wird hängt letztlich von der Leistungsfähigkeit des jeweiligen mobilen Endgerätes und dem Einsatzszenario ab. Wie beispielsweise Remote Access am Hotspot, im Auto, beim Kunden oder auf dem Firmengelände

Sicherheit

Insbesondere bei mobiler Datenkommunikation sind umfangreiche Sicherheitsmaßnahmen zur Abwehr von Angriffen gefordert. Es gilt, die Vertraulichkeit der Daten zu gewährleisten und das Firmennetz gegen Angriffe z.B. durch Backdoors zu schützen. Diese Forderung besteht insbesondere während des An- und Abmeldevorganges eines mobilen Teleworkers an einem Hotspot. Der NCP Secure Symbian Client setzt auch hier Maßstäbe. Er verfügt über alle erforderlichen Sicherheitsmechanismen für die Umsetzung eines Ende-zu-Ende-Sicherheitskonzeptes. Die wichtigsten, integrierten Security-Bausteine sind neben dem VPN-Tunneling: Datenverschlüsselung, eine dynamische Personal Firewall, die Unterstützung von

OTP-Token (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure). Die Personal Firewall gestattet die Definition von Regelwerken für: Ports, IP-Adressen und Segmente. Friendly Net Detection ermöglicht die automatische Erkennung von sicheren und unsicheren Netzen.

Komfort

„Easy-to-use“ – d.h. einfache Installation und Bedienung der Client Software. Dafür stehen der integrierte Konfigurations-Assistent für den Konfigurations-PC und eine intuitive, grafische Benutzeroberfläche am mobilen Endgerät. Der mobile Teleworker arbeitet in der gewohnten Weise wie an einem Büroarbeitsplatz. Unterbrechungen einer Funkverbindung während eines Datentransfers z.B. bei Funkausfällen oder beim Wechsel von Access Points im WLAN bleiben ohne Auswirkungen. Der User bleibt davon unberührt. Im Falle von E-Mail-Polling / Pushdiensten sorgt ein spezieller Verbindungsmodus für den automatischen Wiederaufbau des VPN-Tunnels zum zentralen VPN-Gateway. Der mobile Teleworker ist somit immer erreichbar.

Zentrales Management

Der NCP Secure Symbian Client steht in den Varianten Entry und Enterprise zur Verfügung. Beide verfügen über den gleichen Leistungsumfang. Der NCP Secure Enterprise Symbian Client ist zudem zentral managebar und in ein umfassendes Endpoint Security-Konzept integrierbar.

Technische Daten

System Anforderungen Mobiles Endgerät Konfigurations-PC	Betriebssystem: Symbian OS ab V. 9.0 S60 3rd Edition Betriebssystem: Windows 2000, XP (32/64 Bit), Vista (32/64 Bit); 32 MB RAM Ausstattung: min. 10 MB Arbeitsspeicher, Nokia PC Suite
Security Features	Der Secure Symbian Client unterstützt alle IPSec Standards nach RFC und erfüllt auch die höchsten Sicherheitsanforderungen.
Personal Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); differenzierte Filterregeln bezüglich: Protokolle, Ports und Adressen; Friendly Net Detection (i.V.)
Firewall Configuration	Firewall Configuration Plug -In* (i.V.)
Virtual Private Networking (VPN)	IPSec (Layer 3 Tunneling), RFC-konform; IPSec-Proposals können determiniert werden durch das IPSec -Gateway (IKE, IPSec Phase 2); Event log; Block und Central Tunneling; MTU Size Fragmentation und Reassembly, DPD; NAT-Traversal (NAT-T); IPSec Modes: Tunnel Mode, Transport Mode
Verschlüsselung (Encryption)	Symmetrische Verfahren: AES 128,192,256 Bits; Blowfish 128,448 Bits; Triple-DES 112,168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 2048 Bits; Diffie-Hellman Groups 1,2,5 Seamless Rekeying (PFS); Hash Algorithmen: SHA1, SHA256, SHA384, SHA512, MD5
Authentisierungsverfahren	IKE (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP); PFS; MS CHAP V.2*; Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate (i.V.); Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready.
Starke Authentisierung	X.509 v.3 Standard; PKCS#12 Interface für Private Schlüssel in Soft-Zertifikaten;
Endpoint Security	Endpoint Policy Enforcement * (i.V.);
Networking Features	
Netzwerkprotokolle	IP
Dialer	Symbian integrated
IP Address Allocation	DHCP (Dynamic Host Control Protocol); DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server
Übertragungsmedien	WLAN (WiFi), GSM (incl. HSCSD), GPRS, UMTS; Internet; analoge Modems (Mobiltelefone über Infrarot oder Bluetooth); nutzbare Übertragungsmedien sind abhängig vom eingesetzten Endgerät
Line Management	DPD mit konfigurierbarem Zeitintervall; WLAN-Roaming (Handover)
Datenkompression	IPCOMP (Izs), Deflate
Internet Society RFCs und 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 Grafische Benutzeroberfläche	Mehrsprachig (Deutsch, Englisch); Verbindungsstatistik, Log-Files, Trace-Werkzeug für Fehlerdiagnose; Konfigurations- und Profil-Management mit Passwortschutz
Produktvarianten	NCP Secure Entry Symbian Client , NCP Secure Enterprise Symbian Client (zentral managebar*)

* Voraussetzung: NCP Secure Enterprise Management

Eine 30-Tage Vollversion des Secure Entry Clients können Sie hier kostenlos testen:
<http://www.ncp-e.com/de/downloads/software.html>

IPsec Kompatibilitätsliste: <http://www.ncp-e.com/de/service-support/kompatibilitaeten/ipsec.html>