



**Service Release:** 11.15 r42964  
**Datum:** Februar 2019

### Voraussetzungen

#### Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 10, 32/64 Bit (bis einschließlich Version 1809)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

### Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden zentralen Komponenten:

- NCP Secure Enterprise Management: Version 4.05 oder neuer
- NCP Management Console: Version 5.0
- Client Configuration Plug-in: Version 11.10 oder neuer
- License Plug-in: Version 11.10 oder neuer
- Firewall Plug-in: Version 10.11 mind. r33042
- Update Client: Version 6.01

## 1. Neue Leistungsmerkmale und Erweiterungen

Keine.

## 2. Verbesserungen / Fehlerbehebungen

### Unterbrechung des VPN-Tunnels bei genutzter Mobilfunkverbindung

Nach kurzer Zeit wurde der VPN-Tunnel über eine genutzte Mobilfunkverbindung wegen Dead Peer Detection unterbrochen. Dieses Problem wurde behoben.

### PKI-Error bei Verwendung einer SmartCard

Bei der Verwendung einer SmartCard trat im Client ein PKI-Error auf. Dieses Problem wurde behoben.

## 3. Bekannte Einschränkungen

Keine.



**Service Release:** 11.14 r42039  
**Datum:** Dezember 2018

### Voraussetzungen

#### Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 10, 32/64 Bit (bis einschließlich Version 1809)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

### Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden zentralen Komponenten:

- NCP Secure Enterprise Management: Version 4.05 oder neuer
- NCP Management Console: Version 5.0
- Client Configuration Plug-in: Version 11.10 oder neuer
- License Plug-in: Version 11.10 oder neuer
- Firewall Plug-in: Version 10.11 mind. r33042
- Update Client: Version 6.01

## 1. Neue Leistungsmerkmale und Erweiterungen

### Neuer Update-Client 6.01

Unter bestimmten Umständen konnte es im Falle eines Software-Updates durch das zentrale NCP Management vorkommen, dass der Update-Client nicht beendet wurde. Dieser Fehler ist nun behoben. Es wird empfohlen vor dem Software-Update mit diesem Client den Update-Client auf die Version 6.01 zu aktualisieren.

## 2. Verbesserungen / Fehlerbehebungen

### Prüfung eines Verbindungsmediums auf Internetverfügbarkeit

Die ständige Prüfung eines Verbindungsmediums auf Internetverfügbarkeit mittels periodisch abgesetzter Pings auf 8.8.8.8 wurde auf maximal vier Pings begrenzt.



### Optimierungen im Bereich HotSpot-Anmeldung

Es wurden verschiedene Optimierungen im Bereich der HotSpot-Anmeldung vorgenommen, insbesondere bei der Verwendung von Seamless Roaming in den Profileinstellungen.

### Credential Provider – Sicherheitslücke

Bei der Verwendung des NCP Credential Providers konnte ein Anwender über das Log-Fenster und den darin enthaltenen „Öffne Datei“-Button Zugriff auf den Windows-Explorer bekommen. Darüber war es möglich sich administrative Rechte in der PowerShell zu verschaffen. Dieses Problem ist behoben.

### Deinstallation des Clients

Unter bestimmten Umständen konnte es vorkommen, dass der Filtertreiber des VPN Clients nicht korrekt deinstalliert wurde. Dieses Problem ist behoben.

### Software-Update via NCP Management

Bei der Verwendung großer Updatepakete konnte es vorkommen, dass der Update-Client nicht beendet wurde, wodurch der Update-Vorgang abbricht. Dieser Fehler ist nun behoben. Bei der Installation wird ein neuer Update-Client 6.01 installiert.

### Software-Update über andere NCP-OEM Clients ist nicht gesperrt

Beim Durchführen eines Clientupdates muss die OEM-Variante des Clients übereinstimmen. Der Versuch eines Updates muss für diesen Fall verriegelt sein. Dieser Fehler ist nun behoben.

### VLS-Lizenzierung – Inbetriebnahme

Unter bestimmten Umständen war es nicht möglich dem NCP Secure Client mit der Installation eine VLS-Initialisierungsdatei mitzugeben. Dieses Problem ist nun behoben.

### Adresszuweisung auf NCP Netzwerkadapter

Bei Verwendung eines Juniper-Gateways konnte unter bestimmten Umständen dem NCP Netzwerkadapter keine Netzwerkadresse zugewiesen werden. Dieses Problem ist nun behoben.

### Das Handling verfügbarer Verbindungsmedien nach dem Aufwachen aus dem Sleep-Mode wurde verbessert.

### IKEv1 / Aggressive Mode

Bei der Verwendung von IKEv1 mit Aggressive Mode konnten in Verbindung mit einer automatischen IKE-Richtlinie Probleme auftreten. Dieser Fehler ist behoben.

## 3. Bekannte Einschränkungen

Keine.



**Service Release:** 11.13 r41436  
**Datum:** Oktober 2018

### Voraussetzungen

#### Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 10, 32/64 Bit (bis einschließlich Version 1809)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

### Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden zentralen Komponenten:

- NCP Secure Enterprise Management: Version 4.05 oder neuer
- NCP Management Console: Version 5.0
- Client Configuration Plugin: Version 11.10
- License Plugin: Version 11.10
- Firewall Plug-in: Version 10.11 mind. r33042
- Update Client: Version 6.0

## 1. Neue Leistungsmerkmale und Erweiterungen

### Anpassung an Windows 10 Version 1809 – Treiberinstallation

Aufgrund Microsoft-interner Änderungen war es mit vorhergehenden Clients nicht möglich eine Installation auf Windows 10 Version 1809 durchzuführen. Dieses Problem wurde behoben.

## 4. Verbesserungen / Fehlerbehebungen

### Erkennung des Friendly Net Detection Servers

In Netzwerken mit Network Access Control und Wechsel des IP-Segments nach erfolgreicher Authentisierung, wurde die Erkennung des Friendly Net Detection Servers verbessert.



### Performanceoptimierung des Datentransfers außerhalb des VPN-Tunnels

### Optimierung des Client Updateprozesses im Falle eines Major-Updates

Die Erkennung eines Major-Updates innerhalb des MSI-Installationsprozesses wurde verbessert. Ebenso wurde ein Problem mit der Umgebungsvariable `NcpClntInstallPath` behoben, die unter Umständen nach dem Update des Clients gelöscht war.

### Anzeige des VPN-Clients in der Taskleiste

Wird die Client-GUI geschlossen, so wird das entsprechende Icon nicht mehr in der Taskleiste angezeigt. Dieses Verhalten entspricht dem Verhalten der Clientversionen vor 11.0.

### Verbesserung bei Seamless Roaming

Bei Verwendung von VRRP konnte der Client im Seamless Roaming-Betrieb unter bestimmten Umständen nicht korrekt zwischen Mobilfunk und WLAN wechseln. Dieses Problem wurde behoben.

### Diagnosedaten im Installationsverzeichnis

Im Falle der aktivierten Full trace-Funktion oder einer konfigurierten HotSpot-Erkennung wurden fälschlicherweise Diagnosedateien in das Installationsverzeichnis des Clients geschrieben. Dieser Fehler wurde behoben.

### Verbesserung der Silent Installation

Unter bestimmten Umständen konnte das REBOOT Property während der Installation des Clients überschrieben werden. Dieses Problem ist nun behoben.

### Verbesserung der Kompatibilität zu DHCP-Servern

Bei einem DHCP-Request ist die Angabe des Hostnamens zwar optional, jedoch kommen nicht alle DHCP-Server mit dem Weglassen des Hostnamens zurecht. Aus diesem Grunde wird ab dieser Release immer der Hostname mitgeschickt.

### Verbesserung der Kompatibilität zu Fremdgateways

Innerhalb der IKE-Verhandlung wurde die Kompatibilität zu Fremd-Gateways verbessert.

### Firewall-Einstellung: Ausnahme für VPN Path Finder

Wurde in den Firewall-Einstellungen die Option „IPsec-Protokoll (ESP, UDP 500) und VPN Path Finder (TCP 443) zulassen“ konfiguriert, so waren Ziele durch den VPN-Tunnel via HTTPS-Port 443 erreichbar obwohl dies durch keine weitere Firewall-Regel erlaubt war. Dieser Fehler wurde behoben.

### Länge des Namens einer PKCS#11-Datei

Die Länge des Eingabefeldes in der PKI-Konfiguration des Clients für das PKCS#11 Modul wurde auf 255 Zeichen erhöht.



### Nachladen von DLLs

Verbesserung des DLL-Ladevorganges zur Erhöhung der Sicherheit vor manipulierten DLLs.

## 5. Bekannte Einschränkungen

### NCP Demo-Benutzerzertifikate

Die "NCP Demo-Benutzerzertifikate", die mit bisherigen Client-Versionen installiert wurden, verlieren ihre Gültigkeit am 9. Oktober 2018. Damit werden existierende Test-Profile, z.B. zum NCP Demo-Server "vpntest.ncp-e.com", ab diesem Zeitpunkt nicht mehr funktionieren. Ab dieser Clientversion steht bei Neuinstallationen die automatische Einrichtung dieser Test-Profile mit Zertifikat nicht mehr zur Verfügung. Es existiert ausschließlich die Möglichkeit, Test-Profile mit der VPN Konfiguration "Pre-shared key" zu erstellen.

Neue Zertifikate mit verlängerter Gültigkeit befinden sich nach der Installation im Unterverzeichnis *certs*. Bisher waren sie immer direkt im Installationsverzeichnis abgelegt.



**Major Release: 11.10 r39552**

**Datum: Mai 2018**

### Voraussetzungen

#### Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 10 32/64 Bit (bis einschließlich Version 1803)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Unterstützung für Windows Vista, 32/64 Bit entfällt ab dieser Version

### Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden zentralen Komponenten:

- NCP Secure Enterprise Management: Version 4.05 oder neuer
- NCP Management Console: Version 5.0
- Client Configuration Plugin: Version 11.10
- License Plugin: Version 11.10
- Firewall Plug-in: Version 10.11 mind. r33042
- Update Client: Version 6.0

## 1. Neue Leistungsmerkmale und Erweiterungen

### Biometrische Authentisierung (z.B. Fingerabdruck- oder Gesichtserkennung) vor VPN-Verbindungsaufbau

Zur Absicherung vor einem VPN-Verbindungsaufbau durch nicht autorisierte Dritte wurde im NCP Secure Client eine optionale biometrische Authentisierung vor der VPN-Einwahl integriert. Die Konfiguration dieser Option findet sich unter „Profil-Einstellungen ⇒ Erweiterte Authentisierung ⇒ Authentisierung vor VPN ⇒ Fingerabdrucksensor / biometrische Authentisierung“. Bei gesetzter Option erfolgt direkt nach dem Klick auf den Verbinden-Button in der Client-GUI die Aufforderung zur Benutzerauthentisierung. Der VPN-Verbindungsaufbau wird daraufhin erst nach positiver Authentisierung gestartet. Voraussetzung für die biometrische Authentisierung ist die Windows Hello-Funktionalität ab Windows 8.1 oder neuer. Für ältere Betriebssysteme oder nicht vorhandene biometrische Hardware wird bei gesetzter Konfigurationsoption eine alternative Benutzerauthentisierung, z.B. das Passwort, abgefragt. Diese Option steht nur für die Verbindungsmodi „manuell“ und „wechselnd“ zur Verfügung.



### Modernisierte Client-GUI

Die Client-GUI und das aus der Taskleiste gestartete Tray Popup-Fenster wurde an das aktuelle Windows 10-Design angepasst.

### Komplette 64 Bit Umsetzung des NCP Secure Clients

Ab dieser Version sind alle Komponenten des NCP Secure Clients in 64 Bit-Ausführung enthalten.

### Neue GUI des Credential Providers inkl. HotSpot-Anmeldefunktionalität

Ist der NCP Secure Client für den VPN-Tunnelaufbau vor der Benutzeranmeldung am Windows System konfiguriert, so erscheint die Client-GUI in reduzierter Funktionalität im Vergleich zum Standard-Betrieb. Des Weiteren ist es nun möglich bereits vor der Benutzerauthentisierung am Windows System eine HotSpot-Anmeldung durchzuführen. Diese geschieht analog zur bereits bekannten HotSpot-Anmeldung des Clients. Die Icons des NCP Credential Providers zeigen durch Ihre rote oder grüne Einfärbung den VPN-Tunnelstatus an.

### Endpoint Policy: Neue Konstante DNS\_HOSTNAME

Die Konstante DNS\_HOSTNAME gibt den DNS-Hostnamen wie unter ipconfig /all angezeigt, zurück. Die alte Konstante HOSTNAME hingegen gibt den NetBIOS-Namen zurück (nur Großbuchstaben, maximal 15 Zeichen).

### IKEv2-Authentisierung nach RFC 7427

Bei Bedarf kann der Client für den IKEv2-Verbindungsaufbau das Padding-Verfahren gemäß RFC 7427 verwenden. Voraussetzung ist, dass die Gegenstelle diese Authentisierung für IKEv2, einschließlich des Padding-Verfahrens, unterstützt und akzeptiert.

Konfiguration:

Neben der Aktivierung des neuen Expertenparameters „Aktiviere Verhandlung nach RFC 7427“ (in der Voreinstellung bereits aktiv) in der Expertenkonfiguration unter „Erweiterte IPsec-Optionen“, kann unter der gleichen Rubrik das „RFC 7427 Padding-Verfahren“ gewählt werden: PKCS#1 v.1.5 Padding oder RSASSA-PSS.

### IKEv2 RSA-Authentisierung mit alternativem Hash-Algorithmus

Der neue Expertenparameter „IKEv2 RSA Authentisierung mit PRF-Hash“, zu finden im Parameterfeld „Erweiterte IPsec-Optionen“, gestattet bei der IKEv2 RSA-Authentisierung einen anderen Hash-Algorithmus einsetzen zu können, als den durch RFC empfohlenen Standard (SHA-1).

Dies erfolgt durch Voreinstellung eines alternativen Algorithmus (z.B. „HMAC SHA2 256 Bit“) für die „Pseudorandom-Funktion“ in der Konfiguration der „IKEv2-Richtlinie“.

Konfiguration:

Zunächst den Algorithmus für die „Pseudorandom-Funktion [IKEv2-Richtlinie]“ wählen, danach die Funktion „IKEv2 RSA Authentisierung mit PRF-Hash“ im Parameterfeld „Erweiterte IPsec-Optionen“ der Expertenkonfiguration aktivieren.





## 6. Verbesserungen / Fehlerbehebungen

### Integration des Update-Clients im Installer

Bei einem Software-Update über das NCP Secure Enterprise Management (SEM) wird nun der zur Clientversion zugehörige Update-Client mit installiert.

### MSI-Updates über das NCP Secure Enterprise Management

Voraussetzung ist der Einsatz eines Update-Clients der Version 6.0.

### Konfiguration des VPN-Tunnelendpunktes

Ab dieser Version können mehrere VPN-Tunnelendpunkte mit Ihrem Domainnamen konfiguriert werden.

### Optimierung der DPD-Funktionalität

#### FIPS-Inside

Innerhalb der Installationsroutine kann bei Neu-Installation oder bei Ändern der Installation der FIPS-Modus ein- oder ausgeschaltet werden. Über die Kommandozeile kann der FIPS-Modus wie folgt konfiguriert werden:

Hinzufügen: ADDLOCAL=FipsMode; Entfernen: REMOVE=FipsMode

### Erweiterung der Darstellung der Verbindungsinformationen

Auch IPv6-Adressen des Tunnel Endpoints werden nun in den Verbindungsinformationen dargestellt.

### Erweiterung des Client Info Centers

Ein neuer Abschnitt mit Treiber-Informationen zeigt im Client Info Center folgende direkt von der Registry übernommene Werte: Name, Version, IfType, InfPath, MtU, NetCfgInstanceId

Für ein Windows 10 Betriebssystem wird nun zusätzlich die Version und der Build im Client Info Center mit angezeigt.

### Verbesserung der HotSpot-Funktionalität

Die Kompatibilität zu HotSpot-Anmeldeseiten wurde weiter ausgebaut.

Das während der Anmeldung am HotSpot erscheinende Browserfenster wird nach dem in der NCPMON.INI konfigurierbaren Timeout ([HOTSPOTBROWSER] Timeout=300; Standardwert) automatisch geschlossen. Einhergehend wird die Proxy-Konfiguration im Betriebssystem wieder aktiv, die dynamischen Firewall-Regeln zur HotSpot-Anmeldung gelöscht und ggf. die WLAN-Verbindung abgebaut.



## 7. Bekannte Einschränkungen

### NCP Demo-Benutzerzertifikate

Die "NCP Demo-Benutzerzertifikate", die mit bisherigen Client-Versionen installiert wurden, verlieren ihre Gültigkeit am 9. Oktober 2018. Damit werden existierende Test-Profile, z.B. zum NCP Demo-Server "vpntest.ncp-e.com", ab diesem Zeitpunkt nicht mehr funktionieren. Ab dieser Clientversion steht bei Neuinstallationen die automatische Einrichtung dieser Test-Profile mit Zertifikat nicht mehr zur Verfügung. Es existiert ausschließlich die Möglichkeit, Test-Profile mit der VPN Konfiguration "Pre-shared key" zu erstellen.

Neue Zertifikate mit verlängerter Gültigkeit befinden sich nach der Installation im Unterverzeichnis *certs*. Bisher waren sie immer direkt im Installationsverzeichnis abgelegt.



## 8. Hinweise zum NCP Secure Enterprise Client (Win32 / 64)

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:

<http://www.ncp-e.com/de/downloads/download-vpn-client/versionsinformationen.html>

Weitere Informationen zum NCP Secure Enterprise Client (Win32/64) finden Sie hier:

<http://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/managed-vpn-client-suite.html>

Weitere Unterstützung bei Fragen zum Enterprise Client, erhalten Sie über die Mail-Adressen auf folgender Seite:

<http://www.ncp-e.com/de/unternehmen/kontakt.html>

## 9. Leistungsmerkmale

### Zentrale Verwaltung

Das NCP Secure Enterprise Management (SEM) bietet als Single Point of Administration alle Funktionalitäten und Automatismen für Rollout, Lizenzierung, Inbetriebnahme und den wirtschaftlichen Einsatz eines Secure Enterprise Clients. Das Secure Enterprise Management (SEM) versorgt den Enterprise Client über die VPN-Verbindung oder LAN (im Firmennetz) automatisch mit

- Lizenzierung (alternativ auch über VLS)
- Konfigurations-Updates
- Zertifikats-Updates
- Software-Update des Clients

### Network Access Control / Endpoint Security

Die Richtlinien für eine Endpoint Security (Endpoint Policy Enforcement) werden am Secure Enterprise Management (SEM) zentral erstellt. Entsprechend der erstellten Regeln erhält der Enterprise Client Zugang zum Firmennetz.

### High Availability Services

Der NCP Secure Enterprise Client unterstützt die NCP HA Services, die nach dem Client Server-Prinzip arbeiten und in unterschiedlichen Betriebsmodi (Load Balancing- und Failsafe-Modus) eingesetzt werden können. Die VPN-Verbindung wird für den Anwender des Enterprise Clients im Hintergrund auch bei hohem Lastaufkommen oder einem Serverausfall ohne zeitliche Verzögerung sicher ins Firmennetz aufgebaut.



### Betriebssysteme

Beachten Sie dazu die "Voraussetzungen" auf Seite 1.

### Security Features

#### Unterstützung aller IPsec-Standards nach RFC.

#### Virtual Private Networking

- RFC-konformes IPsec (Layer 3 Tunneling)
  - IPsec Tunnel Mode
  - IPsec-Proposals können via das IPsec-Gateway (IKE, IPsec Phase 2) determiniert werden
  - Kommunikation nur im Tunnel oder Split Tunneling konfigurierbar
  - Message Transfer Unit (MTU) Size Fragmentation und Re-assembly
  - Network Address Translation-Traversal (NAT-T)
  - Dead Peer Detection (DPD)
  - Anti-Replay Protection

#### Authentisierung

- Internet Key Exchange (IKE):
  - Aggressive Mode, Main Mode, Quick Mode
  - Perfect Forward Secrecy (PFS)
  - IKE-Config-Mode für dynamische Zuteilung einer privaten (virtuellen) Adresse aus IP-Pool
  - Pre-shared Secrets oder RSA-Signaturen (mit entsprechender Public Key Infrastructure)
- Internet Key Exchange v2 (IKEv2):
  - Pre-shared secrets
  - RSA Signatures (und entsprechende Public Key Infrastructure)
  - Extended Authentication Protocol (EAP) – (Benutzername und Passwort für Client-Authentisierung gegenüber Gateway; Zertifikat zur Server-Authentisierung gegenüber Client)
  - EAP unterstützt: PAP, MD5, MS-CHAP v2, TLS (ausgewählt durch Responder/Gateway)
  - IKEv2 Mobility und Multihoming Protokoll (MOBIKE)
  - Perfect Forward Secrecy (PFS)
  - IKE-Config-Mode für dynamische Zuteilung einer privaten (virtuellen) Adresse aus IP-Pool
- Benutzer-Authentisierung:
  - Benutzer-Authentisierung über GINA/Credential Management
    - Windows Logon über VPN-Verbindung
  - XAUTH (IKEv1) für erweiterte Benutzer-Authentisierung
    - One-Time-Passwörter und Challenge Response Systeme
    - Zugangsdaten aus Zertifikaten (PKI)
- Unterstützung von Zertifikaten in einer PKI:



- Soft-Zertifikate, Smart Cards, USB Token: Multi-Zertifikats-Konfiguration
- Seamless Rekeying
- PAP, CHAP, MS-CHAP v2
- HTTP Authentisierung vor VPN
- IEEE 802.1x:
  - Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Erweiterte Authentisierung gegenüber Switches und Zugriffspunkten (Layer 2)
  - Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): Erweiterte Authentisierung an Switches und Zugriffspunkten auf der Basis von Zertifikaten (Layer 2)
  - Extensible Authentication Protocol – Transport Layer Security (MS-CHAPv2): Erweiterte Authentisierung an Switches und Zugriffspunkten auf der Basis von Zertifikaten mit IKEv2 (Layer 2)
- Hotspot Anmeldung mit HTTP oder EAP
- RSA SecurID Ready

### **Verschlüsselung (Encryption)**

Symmetrisch: AES-GCM 128, 256 Bits (nur IKEv2 & IPsec); AES-CTR 128, 192, 256 Bits (nur IKEv2 und IPsec); AES (CBC) 128,192,256 Bits; Blowfish 128,448 Bits; Triple-DES 112,168 Bits

Asymmetrisch: RSA bis 2048 Bits, für dynamischen Schlüsselaustausch

### **Hash / Message Authentisierungs-Algorithmen**

- SHA-1, SHA-256, SHA-384, SHA-512, MD5.
- Diffie Hellman Gruppen 1, 2, 5, 14, 15-18, 19-21, 25, 26, 27-30 für asymmetrischen Schlüsselaustausch und PFS.
- Diffie Hellman Gruppen 19 - 21, 25, 26, 27-30 mit Algorithmus elliptischer Kurven (nur unter IKEv2).

### **Public Key Infrastructure (PKI) - Starke Authentisierung**

- X.509 v.3 Standard
- Zertifikats-Unterstützung in einer PKI
  - Smart Cards und USB Tokens
    - PKCS#11-Schnittstelle für Verschlüsselungs-Tokens (USB und Smart Cards)
    - Smart Card Betriebssysteme: TCOS 1.2, 2.0 und 3.0
  - Smart Card Reader-Schnittstellen
    - PC/SC, CT-API
  - Soft-Zertifikate
    - PKCS#12-Schnittstelle für private Schlüssel in Soft-Zertifikaten
- PIN Richtlinien: Administrative Vorgabe für die Eingabe beliebig komplexer PINs

Next Generation Network Access Technology



- Certificate Service Provider (CSP) zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher
- Revocation:
  - End-entity Public-key Certificate Revocation List (EPRL vormals CRL)
  - Certification Authority Revocation List, (CARL vormals ARL)
  - Online Certificate Status Protocol (OCSP)
  - Certificate Management Protocol (CMP)<sup>i</sup>

### Personal Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (Automatische Umschaltung der Firewall-Regeln bei Erkennung des angeschlossenen Netzwerkes anhand des IP-Adressbereiches oder eines NCP FND-Servers<sup>j</sup>)
  - FND-abhängige Aktionen starten
- Sicheres Hotspot Anmeldung
- Anwendung starten vor oder nach VPN-Verbindungsaufbau
- Differenzierte Filterregeln bezüglich:
  - Protokolle, Ports, Applikationen und Adressen
  - Schutz des LAN Adapter
- Schutz des VMware Gastsystems
- IPv4- und IPv6-Fähigkeit
- Option: ausgehenden Verkehr mit Reject quittieren oder ohne Rückmeldung verwerfen

### Endpoint Security

- Endpoint Policy Enforcement<sup>ii</sup>

## Networking Features

### Sichere Netzwerk Schnittstelle

- LAN Emulation
  - Virtueller Adapter mit NDIS-Schnittstelle
  - Volle Unterstützung von Wireless Local Area Network (WLAN)
  - Volle Unterstützung von Wireless Wide Area Network (WWAN)

### Netzwerk Protokoll

- IPv4-Protokoll
  - IPv4 für Tunnelaufbau und Datenverkehr innerhalb des VPN-Tunnels;
- IPv6-Protokoll
  - IPv6 für Tunnelaufbau von Client zu NCP Server-Komponenten (Secure Enterprise VPN)

Next Generation Network Access Technology



- Server);
- zur Datenübertragung innerhalb des VPN-Tunnels wird IPv4 genutzt

### Verbindungs-Medien

- LAN
- WLAN
- Mobiles Netzwerk, GSM - LTE
  - Ab Windows 7 – Mobile-Broadband-Fähigkeit
  - SMS-Center (senden und empfangen von SMS)
- xDSL (PPPoE)
- PSTN (analoges Modem)
- ISDN
- Automatic Media Detection (AMD)
- Externer Dialer
- Seamless Roaming (LAN / Wi-Fi / Mobiles Netzwerk)

### Dialers

- NCP Secure Dialer
- Microsoft RAS Dialer (für ISP Einwahl mit Einwahl-Script)

### Verbindungssteuerung

- Dead Peer Detection mit konfigurierbarem Zeitintervall
- WLAN Roaming (handover)
- Modi des Verbindungsaufbaus
  - manuell
  - immer
  - automatisch (Datenverkehr initiiert VPN-Verbindung)
  - wechselnd (automatischen Modus manuell starten)
  - wechselnd (Immer-Modus manuell starten)
- Timeout (für ausgehende, eingehende und bi-direktionale Verbindungen)
- Short Hold Mode
- Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert
- Budget Manager
  - Eigenes Management für WLAN, Mobilfunk, xDSL, ISDN und Modem-Verbindungen
  - Budgets nach Verbindungsdauer oder Volumen
  - Management der Roaming-Kosten (Mobilfunk)
  - Eigenes Management verschiedener WLAN-Zugriffspunkte



### IP Address Allocation

- Dynamic Host Control Protocol (DHCP)
- Domain Name Service (DNS) : Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server

### VPN Path Finder

- NCP Path Finder Technologie
  - Fallback auf HTTPS (port 443) wenn IPsec-Port 500 bzw. UDP Encapsulation nicht möglich ist <sup>iii</sup>

### Datenkompression

- IPsec Kompression

### Link Firewall

Stateful Packet Inspection

### Weitere Features

- VoIP Priorisierung
- UDP Encapsulation
- IPsec Roaming <sup>iii</sup>
- WLAN Roaming <sup>iii</sup>
- WISPr-Unterstützung (T-Mobile Hotspots)
- VPN-Bypass

### Point-to-Point Protokolle

- PPP über Ethernet
- PPP über GSM,
- PPP über ISDN,
- PPP über PSTN,
  - LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

## Unterstützte Standards

### Internet Society RFCs und Drafts

Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409),

- Internet Key Exchange Protocol v1 (IKE) (includes IKMP/Oakley) (RFC 2406),
  - IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
  - Negotiation of NAT-Traversal in the IKE (RFC 3947)

Next Generation Network Access Technology





- Internet Key Exchange Protocol v2 (IKEv2) (RFC 4306, 5996)
  - IKEv2 Mobility and Multihoming Protocol (MOBIKE) (RFC 4555)
- UDP encapsulation of IPsec Packets (RFC 3948),

Zusätzliche Extended Key Usages:

- id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17) nach RFC 4945
- anyExtendedKeyUsage (2.5.29.37.0) nach RFC 4945
- IKEIntermediate (1.3.6.1.5.5.8.2.2) nach draft-ietf-ipsec-pki-req-03

### FIPS Inside

Der Secure Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1051).

Die FIPS-Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt wird:

- Diffie Hellman Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit)
- Hash Algorithmen: SHA1, SHA 256, SHA 384, oder SHA 512 Bit
- Verschlüsselungsalgorithmen: AES mit 128, 192, 256 Bit oder Triple DES

### Benutzerfreundliche Features

#### APN von SIM-Karte

Der APN (Access Point Name) definiert den Zugangspunkt eines Providers für eine mobile Datenverbindung. Die APN-Daten werden bei einem Providerwechsel automatisiert aus der jeweiligen SIM-Karte in die Client-Konfiguration übernommen. Das erleichtert die Nutzung von günstigen lokalen Providern im Ausland.

### Secure Client Monitor

#### Intuitive graphische Benutzeroberfläche

- Mehrsprachigkeit (Englisch, Deutsch, Französisch, Spanisch)
  - Monitor & Setup: en, de, fr, es
  - Online Hilfe und Lizenz en, de
- Icon, das den Verbindungsstatus anzeigt
- Client Info Center – Übersicht über :
  - Allgemeine Informationen - Version, MAC-Adresse, Windows Version und ggf. Build etc.
  - Netzwerk-Treiber Informationen
  - Verbindung – aktueller Status
  - Services/Applications – Prozess-Status
  - Zertifikats-Konfiguration – eingesetzte Zertifikate etc.
- Konfiguration, Verbindungsstatus, Logbuch (mit Farbmarkierungen und Copy&Paste-



### Funktion)

- Unterstützung von Mobilfunk-Hardware
- Passwort-geschützte Konfiguration und Profil-Management
- Trace Tool für Fehlerdiagnose
- Monitor kann firmenspezifisch mit Firmenlogo und Support-Informationen ausgestattet werden
- Hotkey Support für Verbindungsauf- und -abbau.
- Custom Branding Option
- Tests zur Internet-Verfügbarkeit
- Tests zur VPN-Tunnel-Verfügbarkeit (Tunnel Traffic Monitoring)

### Hinweise

- i NCP FND- Server kann kostenlos als Add-On hier heruntergeladen werden:  
<http://www.ncp-e.com/de/downloads/download-software.html>
- ii Voraussetzung: NCP Secure Enterprise Management
- iii Voraussetzung: NCP Secure Enterprise Server V 8.0 und später