

## Next Generation Network Access Technology

## Allgemeines

Das NCP Secure Enterprise Management ist der zentrale Baustein der NCP Next Generation Network Access Technology. Als "Single Point of Administration" schafft es die erforderliche Transparenz für Netzwerkadministratoren um mobile und stationäre Telearbeitsplätze sowie remote VPN-Gateways beispielsweise in Filialnetzen zentral zu verwalten. Das NCP Software-Tool bietet alle Funktionalitäten und Automatismen, die für die Inbetriebnahme und den Betrieb eines Remote Access-Projektes erforderlich sind.

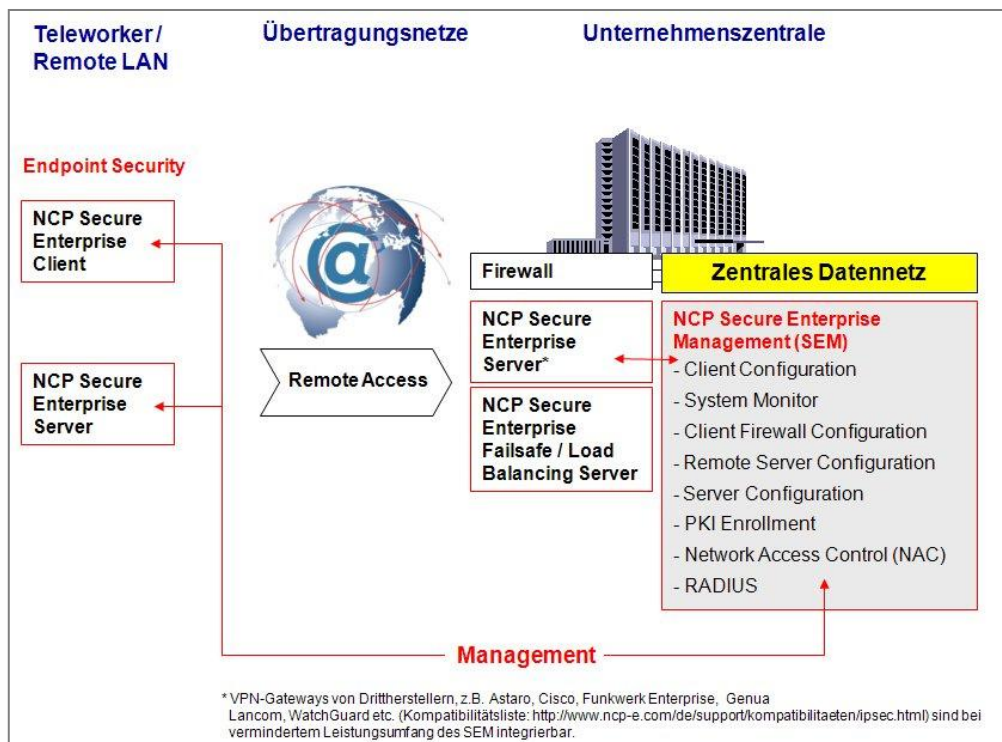


Abb1: NCP Secure Enterprise Management – Funktionsübersicht

## Highlights

- Network Access Control (NAC) – Schutz der Endgeräte durch zentrale Überprüfung
- Minimierung des Aufwandes bei Massen-Rollout und Betrieb der remote Systeme
- Zentrale Ausstellung und Verwaltung von Zertifikaten
- Minimierung der Betriebskosten (TCO-Total Cost of Ownership)
- Durchgängige Transparenz für den Administrator durch umfangreiches System-Monitoring
- Risikominimierung von Fehlkonfigurationen und Fehlbedienungen
- Hohe Ausfallsicherheit (Backup) und Vermeidung redundanter Datenhaltung
- Hohe Skalierbarkeit (Planungssicherheit)
- Integration in vorhandene VPN-Infrastrukturen (Investitionsschutz)
- Integrierter RADIUS-Server

**Leistungsumfang**

Das NCP Secure Enterprise Management besteht aus dem Management Server und der Management Console. Der Management Server ist ein datenbankbasiertes System und korrespondiert mit nahezu jeder Datenbank über ODBC (z.B. Oracle, MySQL, MS SQL, MS Access, MaxDB). Mit der Management Console als Front-End werden User-Daten abgerufen oder Konfigurationen und Zertifikate gespeichert. Alle relevanten Informationen werden in der Datenbank abgelegt und sind üblicherweise in den Backup-Prozess des VPN-Betreibers eingebunden. Der Multi-Company Support (Mandantenfähigkeit) prädestiniert das Secure Enterprise Management für den Einsatz bei Managed Security Service Providern (MSSP) in sog. „Managed VPNs“ oder in Remote Access-Strukturen, wo mehrere Firmen gemeinsam eine VPN-Plattform nutzen (VPN Sharing).

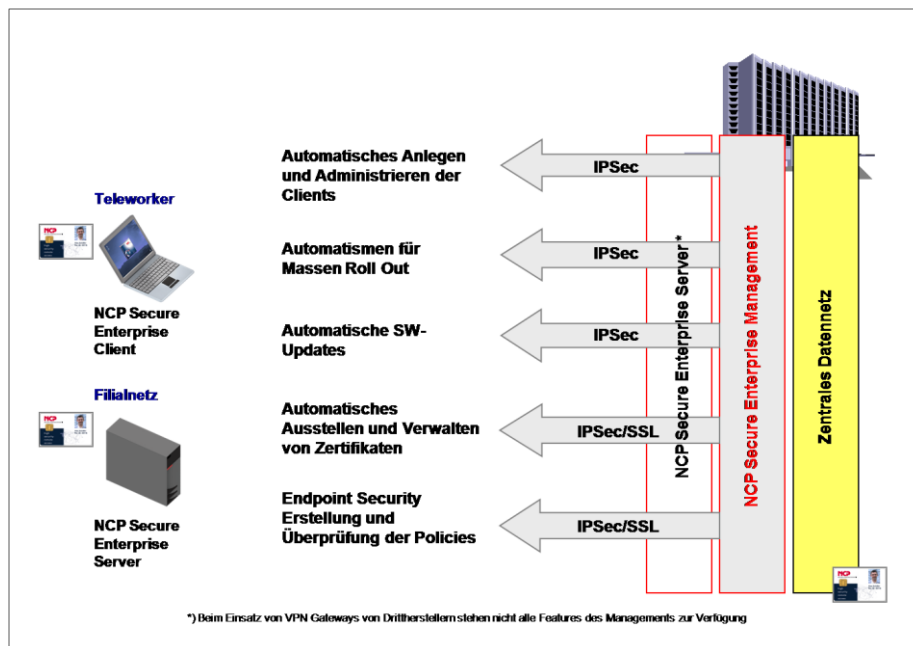


Abb 2: Überblick – Funktionalitäten des zentralen Managements

In all diesen Fällen müssen Administratoren rechtlich selbständiger Firmen ihr „anteiliges“ VPN managen können. Dies erfolgt durch Gruppenzuordnung und eine komfortable Rechtevergabe. Die Administratoren werden so angelegt, dass jeder ausschließlich Zugriff auf seinen Bereich, sprich seine zu verwaltenden Einheiten hat. Ein Übergriff auf Daten anderer Mandanten in deren geschützten Bereichen ist ausgeschlossen.

Das automatische Update-Verfahren ermöglicht dem Administrator für alle entfernten NCP Secure Clients unter Windows, zentral Software-Updates bereitzustellen, die bei der nächsten VPN-Verbindung automatisch auf dem einwählenden System installiert werden. Sollte es während der Übertragung zu Störungen kommen, bleiben der bereits vorhandene Softwarestand sowie die Konfiguration unberührt. Erst nach komplettem, fehlerfreiem Transfer aller vordefinierten Dateien findet das Software-Update statt. Alle Daten werden hochsicher d.h. verschlüsselt im VPN-Tunnel übertragen. Das Update kann auch ohne VPN-Verbindung durchgeführt werden, sofern sich der Client PC im heimischen Firmennetz befindet. Ein integrierter RADIUS-Server dient zur Ablage und Verwaltung aller Client-Link-Profile.

Der Software Update-Service organisiert auch die zentrale Verteilung aller Remote Access relevanten Parameter wie:

- Konfigurationen (Profile)
- Software (Updates, Upgrades)
- Softzertifikate (PKCS#12-Dateien) als User- oder Maschinen-Zertifikat
- Aussteller Zertifikate (Root-Zertifikate)
- Internationale Telefonbücher (z.B. GoRemote (vorm. GRIC), Infonet, Uunet, iPass, MCI...)

Für die Hochverfügbarkeit des Management-Servers sorgt optional der Backup Management-Server, der durch einen integrierten Replikationsdienst immer über den aktuellen Datenbestand verfügt.

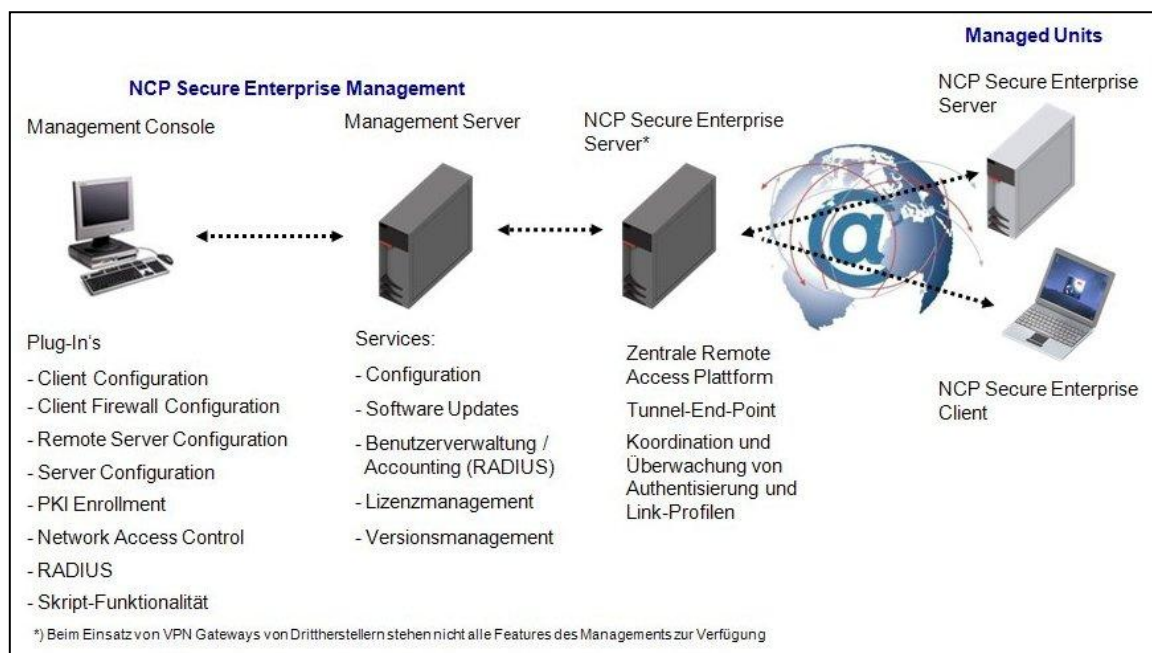


Abb 3: Komponenten und Funktionalitäten eines managed VPN

Die Eingabe und Übernahme aller relevanten Daten kann interaktiv über die NCP Management Console oder skriptgesteuert erfolgen, d.h. Benutzerdaten, Lizenzkeys, Providerkennungen etc. können beispielsweise bei einem Rollout, automatisiert je remote System (= Managed Unit) in den Management Server übernommen werden. Als VPN-Gateway kann der NCP Secure Enterprise Server oder das eines beliebigen Herstellers eingesetzt werden (siehe Kompatibilitätsliste unter [www.ncp-e.com](http://www.ncp-e.com)). Das Secure Enterprise Management ist somit in jede vorhandene IT-Infrastruktur integrierbar und ermöglicht den Betrieb auch in komplexen VPN-Umgebungen.

Ein weiteres wesentliches Feature des Management Servers ist die Lizenzverwaltung der Managed Units. Alle Lizenzen werden in einen Pool übernommen und nach festgelegten Richtlinien automatisiert verwaltet. Funktionsbeispiele:

- Übernahme in eine Konfiguration pro remote Client bzw. Gateway
- Rücknahme bei Ausscheiden eines Mitarbeiters
- Meldung für den Fall, dass keine Lizenzen mehr verfügbar sind.

## Management Server

Der Management Server dient der Konfiguration und Administration aller daran angebundener NCP-Komponenten. Das betrifft sowohl die NCP Secure Enterprise Clients als auch NCP Secure Enterprise Server.

Hierfür stehen leistungsfähige Plug-ins zur Verfügung:

- Client Configuration
- System Monitor
- Client Firewall Configuration
- Server Configuration
- Remote Server Configuration
- Network Access Control (NAC)
- PKI Enrollment
- RADIUS

Als Frontend steht dem Administrator eine Management Console mit grafischer Oberfläche zur Verfügung. Die Installation der Management Console kann bei Bedarf an mehreren Administratorarbeitsplätzen erfolgen. Voraussetzung ist eine Netzwerkverbindung zum Management Server

## System Monitor Plug-in

Dieses Plug-in dient der schnellen Information über alle wichtigen Ereignisse innerhalb einer VPN-Installation als Balken- oder Linien-Diagramme. Der Administrator kann über den System Monitor je nach Bedarf aktuelle Status-Informationen in Echtzeit abrufen bzw. auf bereits gespeicherte Datenbestände der Remote Access-Umgebung zugreifen.

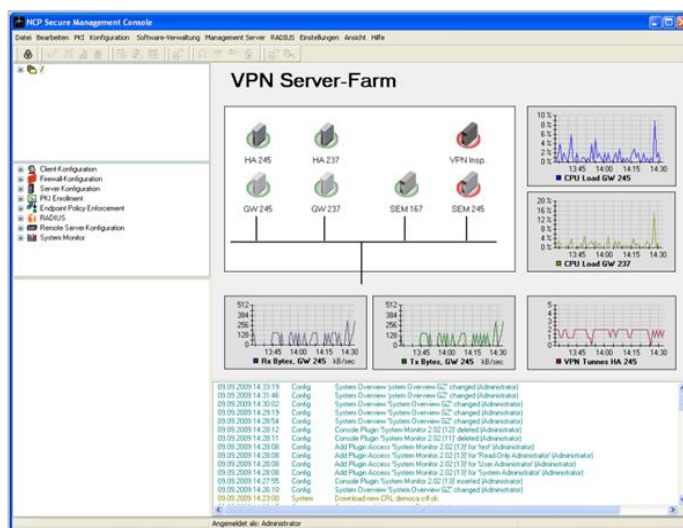


Abb 4: Grafische Oberfläche (Single Point of Administration)

### Anzeigen:

#### 1. Status-Informationen

Folgende Ereignisse können gruppenbezogen angezeigt werden:

- System Neustarts
- Administrator-Anmeldungen (z.B. erfolgreich, abgelehnt)
- Client Update-Anmeldungen (z.B. erfolgreich, abgelehnt)
- Software Downloads pro Package
- RADIUS-Anmeldungen (z.B. erfolgreich, abgelehnt)

Die Anzeige von Verhältniszahlen zweier Ereignisse ist möglich.

## 2. History

Anzeige aller Ereignisse innerhalb eines bestimmten Zeitraumes:

- Stunde; letzte Stunde oder die letzten 2, 3, 4, 6, 12 oder 24 Stunden
- Tag; die letzten 2 oder 4 Tage
- Woche; die letzte Woche
- Monat; letzter oder vorletzter Monat
- Aktueller Tag, aktuelle Woche, aktueller Monat

Im angezeigten Diagramm kann im jeweiligen Zeitraum beliebig zurück bzw. vorwärts geblättert werden. Die Farben und Ansichten der Diagramme sind frei wählbar.

## Client Configuration Plug-in

Dieses Plug-in ermöglicht die Konfiguration und Verwaltung von NCP Secure Enterprise Clients.

Alle relevanten Parameter werden vordefiniert und in Vorlagen (Templates) abgelegt.

Einzelne Leistungsmerkmale im Überblick:

- Zuweisung der Lizenzen (Seriennummer / Aktivationskey)
- Vergabe der Authentisierungs-Codes für Erstverbindungen während des Rollouts
- Anlegen und Verwalten von User-Profilen
- Einzelne Menüpunkte und Konfigurationswerte können für den Anwender als „nicht sichtbar“ oder „nicht veränderbar“ eingestellt werden
- Automatische Konfiguration der User-Profile für Zentralkomponenten (RADIUS, LDAP, SNMP)
- Voreinstellung der Personal Firewall, nicht manipulierbar durch den remote User
- Umfassendes Logging (Versionsstände, Zeitstempel für Konfigurations-änderungen, automatischer Upload von Client-Logdateien...)
- Voreinstellung von VPN-Profilen
- Medien-abhängiges Update (GPRS, UMTS, DSL, WLAN, etc.)
- Konfigurations- und Software-Update im LAN – ohne VPN Tunnel

## Client Firewall Configuration Plug-in

Die NCP Secure Client Software verfügt über eine integrierte Personal Firewall, die bei den Enterprise-Versionen zentral administrierbar ist. Das Client Firewall Configuration Plug-in ermöglicht eine granulare Einstellung von Firewallregeln pro Telearbeitsplatz.

Folgende Konfigurationsparameter können gesetzt werden:

- Applikations- und verbindungsabhängige Filterregeln
- Protokoll-, port- und adressbezogene Filterregeln
- Vorgaben für die Erkennung von „friendly networks“ (IP-Adresse Netzwerk, Netzwerkmaske, IP-Adresse des DHCP-Server, MAC-Adresse)
- Logging-Einstellungen
- Zentrale Vorgabe der Zugangsmöglichkeiten auf die Firewallkonfiguration für den Benutzer
- FND-Serverkonfiguration (Friendly Net Detection)

## Server Configuration Plug-in\*

Dieses Plug-in dient zur Konfiguration und Verwaltung von zentralen NCP Secure Enterprise Servern. Der Funktionsumfang entspricht einem nicht gemanagten NCP Secure Enterprise Server über dessen WEB-Interface.

Es werden Vorlagen erstellt, die als Grundlage für individuelle VPN Gateway-Konfigurationen dienen. Folgende Parameter-Gruppen können vordefiniert bzw. konfiguriert werden:

- Link-Profile
- SSL VPN
- Network Access Control / Endpoint Security
- Firewall-Filterregeln
- IKE- und IPsec-Richtlinien

- Routing-Informationen / statische Routen
- Erstellung von Zertifikaten (Maschinen-Zertifikate)
- Lizenz- und Versionsmanagement

Dieses Plug-in ermöglicht das einfache Management einer NCP Secure Enterprise Server Farm.

\* Verfügbar ab Secure Enterprise Server V 8.0

## Remote Server Configuration Plug-in

Dieses Plug-in dient zur Konfiguration und Verwaltung von dezentralen NCP Secure Enterprise Servern. In Analogie zum Client Configuration Plug-in werden allgemeine Vorlagen erstellt, die als Grundlage für individuelle VPN Gateway-Konfigurationen herangezogen werden. In ganzheitlichen Remote Access VPN-Lösungen gilt es neben den einzelnen Telearbeitsplätzen auch geografisch verteilte VPN-Gateways zu managen. Folgende Parameter-Gruppen können vordefiniert bzw. konfiguriert werden:

- Link-Profile
- Firewall-Filterregeln
- IKE- und IPsec-Richtlinien
- Routing-Informationen / statische Routen
- Erstellung von Zertifikaten (Maschinen-Zertifikate)
- Lizenz- und Versionsmanagement
- Log-Dateien vom NCP Secure Enterprise Server laden

## PKI Enrollment Plug-in

Dieses Funktionsmodul ist das Bindeglied zwischen einer Public Key-Infrastruktur (PKI) und der Remote Access VPN-Umgebung. Das PKI Enrollment Plug-in fungiert als Registration Authority (RA) und managed im Zusammenwirken mit unterschiedlichen Certification Authorities (CA) die Erstellung sowie Verwaltung von elektronischen Zertifikaten (X.509 v3). Als CAs werden unterstützt: T-Telesec NetPass, Microsoft, NCP Demo-CA, weitere z.B. RSA Keon sind über CMP (Certificate Management Protocol) möglich. Eine erzeugtes Zertifikat kann wahlweise als Softzertifikat (PKCS#12) oder auf Hardware z.B. Smart Card oder USB-Token (PKCS#11) abgelegt werden. Die im Lieferumfang enthaltene NCP Demo-CA kann während der Testphase für die Abbildung einer PKI genutzt werden, ist jedoch nicht für den produktiven Einsatz vorgesehen. Die Umstellung auf eine externe CA ist problemlos möglich

Die wichtigsten Funktionalitäten:

- Erstellen von Zertifikaten (auch Bulk-Mode)
- Verlängern von Zertifikaten (PKCS#7)
- Sperren von Zertifikaten
- Verteilung der Zertifikate (auch Multi-Clientzertifikate) über den NCP Secure Management Server
- Anlegen der Benutzerkonfiguration über LDAP im Verzeichnisdienst
- Erstellen eines PAC-Briefes (Personal Authentication Code) für die Erstverbindung (Initialisierung, Lizenzierung)

## Network Access Control Plug-in (Endpoint Security)

Mit Hilfe dieses Plug-ins werden alle sicherheitsrelevanten Parameter definiert, die vor einem Zugriff auf das Firmennetz überprüft werden sollen. Die Einhaltung der vorgegebenen Sicherheitsrichtlinien ist zwingend und von dem Anwender nicht umgeh- bzw. manipulierbar.

Folgende Client-Parameter können überprüft werden:

- Betriebssystem-Informationen z.B. Version, Hotfixstand
- Softwarestand Secure Enterprise Client
- Dienste-Informationen
- Datei-Informationen
- Status eines Virenschanners

- Inhalte bestimmter Registry-Werte
- Inhalte von Zertifikaten (Benutzer- und Hardwarezertifikat)

Abweichungen von den Sollvorgaben werden protokolliert und können unterschiedliche Meldungen bzw. Aktionen auslösen, wie beispielsweise:

- Anzeige einer Meldung am Client
- Ausgabe einer Meldung im Log des Monitors
- Senden einer Meldung zum Management Server
- Senden einer Meldung zu einem Syslog Server
- Freischalten aller oder einer bestimmten Firewall-Regel(n)
- Trennung der VPN-Verbindung

## **RADIUS Plug-in**

Für die Konfiguration der Managed Units (Benutzern) in den zentralen VPN-Gateways steht optional die RADIUS-Schnittstelle zur Verfügung.

Dieses Plug-in dient der Verwaltung des integrierten RADIUS-Servers und deckt folgende Funktionen ab:

- Automatische Anlage von RADIUS-Accounts über die Client - und Remote Server Configuration Plug-in's
- Unterstützung von PAP/CHAP-Requests
- Erfassung von Accounting-Daten
- Sperren von Usern bei wiederholten fehlerhaften Anmeldungen
- Verwaltung von mehreren RADIUS-Konfigurationen unterschiedlicher Gateways
- RSA Authentication Manager Proxy-Funktionalität

Optional: Redundanz durch Backup RADIUS-Server

Vorteil: Bereits vorhandene RADIUS-Server können zusammengefasst d.h. auf wirtschaftliche Art und Weise abgelöst werden.

## Technische Daten

### Aktuelle Version:

V 2.03

Unterstützte Funktionalitäten / verfügbare Plug-in's:

Automatic Update, Client Firewall Configuration, Client Configuration, Endpoint Policy Enforcement, Lizenzmanagement, PKI, RADIUS, Remote Server Configuration, Server Configuration, Skript und System Monitor.

### Versions-Voraussetzungen für Managed Units:

- Secure Enterprise Client ab V 8.x
- Secure Enterprise Server ab V 7.x

### Lieferumfang:

Management Server (mit allen verfügbaren Plug-in's)

Management Console

(Datenbank-System ist nicht im Lieferumfang enthalten)

Optionen:

- Managed Units
- Secure Enterprise Management Server Backup

### Systemanforderungen:

- Betriebssysteme:  
Management Server: Windows 2000, XP, Vista, 2003 Server,  
Windows 2008 32/64 Bit (ab V2.03), Linux  
Management Console: Windows 2000, XP, Vista, 2003 Server
- Weitere Angaben für Management Server:
  - 512 MB Arbeitsspeicher
  - CPU mind. Pentium III-800 MHz (abhängig von der Anzahl der Managed Units)  
Mit RADIUS Plug-in: Pentium IV-1,5 GHz
  - Festplatte: min. 50 MB freier Speicher zzgl. Speicherplatz für Logdateien und ca. 20 MB pro Software-Paket

### Spez. zu den unterstützten Datenbanken:

Oracle ab Version 9.0

MySQL ab 4.x, 5.0 und 5.1

Microsoft SQL Server 2000 - 2008

### Spez. zu den unterstützten Certification Authorities:

Microsoft Certificate Services:

- als „stand alone CA“: ab Windows 2000 Server
- als „integrierte CA in der Domäne“:  
ab Windows 2000 (Zertifikatsvorlagen können nicht angepasst werden)  
ab Windows 2003 Enterprise Server

## Unterstützte Virens Scanner:

- Unter Windows XP SP2 können alle Virens Scanner abgefragt werden, die ihren Status über WMI (Windows Management Instrumentation) oder NAC (Network Admission Control) an das Security Center liefern.
- Unter allen Windows Betriebssystemen werden unterstützt:
  - H+B Antivirus : Produkt Version und Version der Virusdefinitions-Datei können ermittelt werden
  - MC Afee : Produkt Version und Version der Virusdefinitions-Datei können ermittelt werden

## Unterstützte RFC's und Drafts:

- RFC 2138 Remote Authentication Dial In User Service (RADIUS)
- RFC 2139 RADIUS Accounting
- RFC 2433 Microsoft CHAP
- RFC 2759 Microsoft CHAP V2
- RFC 2548 Microsoft Vendor-specific RADIUS Attributes
- RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)
- RFC 2716 PPP EAP TLS Authentication Protocol
- RFC 2246 The TLS Protocol
- RFC 2284 PPP Extensible Authentication Protocol (EAP)
- RFC 2716 Certificate Management Protocol
- RFC 2511 Certificate Request Message Format
- Draft-ietf-pkix-cmp-transport-protocols-04.txt Transport Protocols for CMP
- Draft-ietf-pkix-rfc2511bis-05.txt Certificate Request Message Format (CRMF)