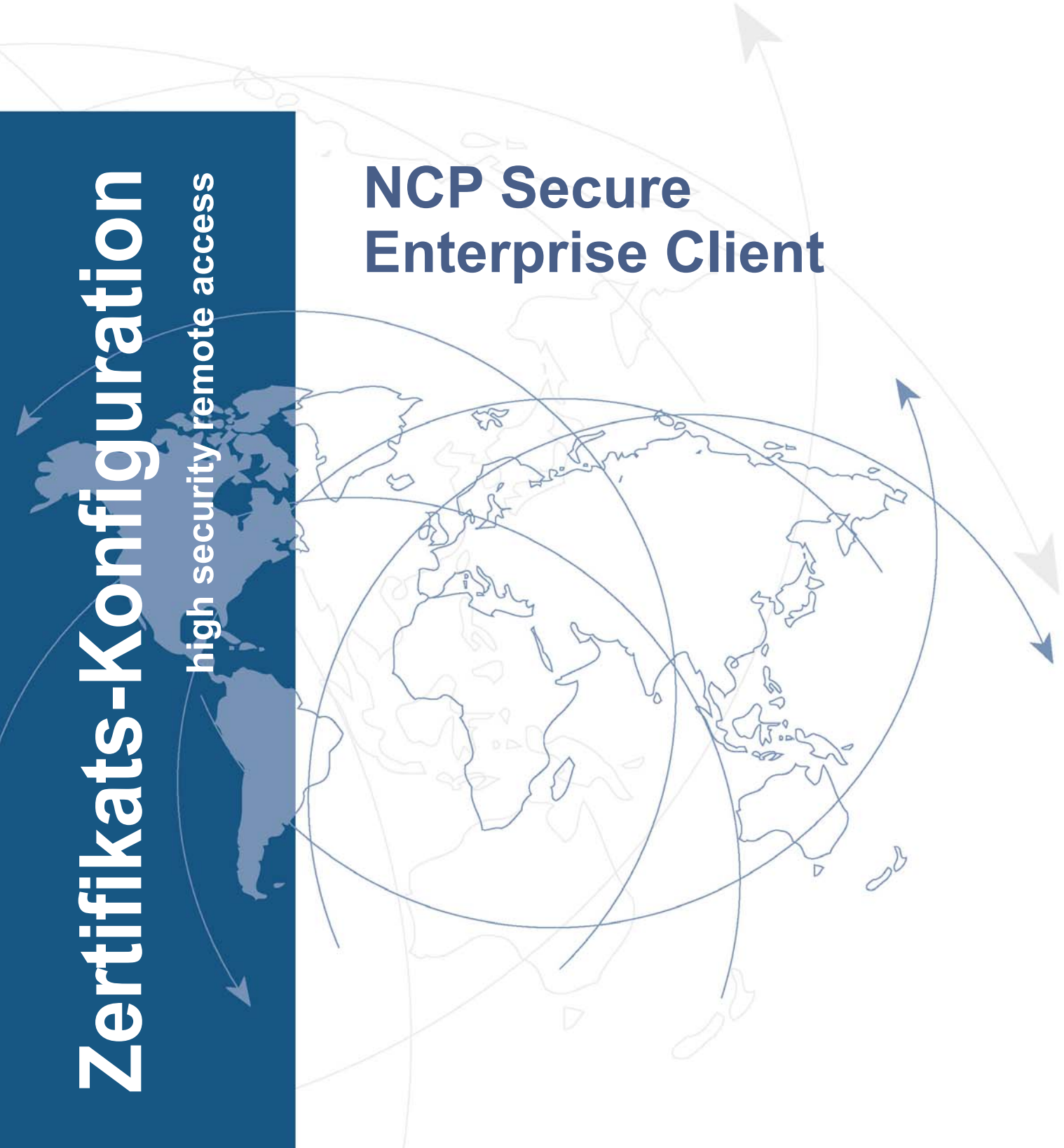


Zertifikats-Konfiguration

high security remote access

NCP Secure Enterprise Client





Zertifikate

am Secure Enterprise Client

NCP Hotline auf Abruf

Sie erreichen unsere NCP Experten unter folgenden Hotlines:

Kunden mit Hotline Service Vertrag

Sie erhalten sofortigen Support unter der vertraglich angegebenen Rufnummer.

Ihnen steht das komplette Serviceportfolio zur Verfügung.

Kunden ohne Hotline Service Vertrag

Sie können wählen zwischen:

Kostenpflichtige Service-Rufnummer 09001996800 (-,80 Euro / Minute)

E-Mail an support@ncp-e.com

Dienstleistungsauftrag (Berechnung nach Aufwand)

mit festen Reaktionszeiten und Zusatzservices.

Bitte nutzen Sie zur Anfrage das NCP Service-Formular von der Website

<http://www.ncp-e.com/de/service-support/support.html>

Sie möchten mehr über den NCP Hotline Service Vertrag wissen?

Bitte senden Sie eine E-Mail an:

vertrieb@ncp-e.com



Network

Communications

Products engineering GmbH

Dombühler Str.2

D-90449 Nürnberg

Tel.: 0911 / 99 68-0

Fax: 0911 / 99 68-299

internet [http:// www.ncp-e.com](http://www.ncp-e.com)

E-mail: info@ncp-e.com

Copyright

Alle Programme und diese Beschreibung wurden mit größter Sorgfalt erstellt und nach dem Stand der Technik auf Korrektheit überprüft. Alle Haftungsansprüche infolge direkter oder indirekter Fehler, oder Zerstörungen, die im Zusammenhang mit den Programmen stehen, sind ausdrücklich ausgeschlossen.

Die in diesem Handbuch enthaltene Information kann ohne Vorankündigung geändert werden und stellt keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Ohne ausdrückliche schriftliche Erlaubnis von NCP engineering GmbH darf kein Teil dieser Beschreibung für irgendwelche Zwecke oder in irgendeiner Form elektronisch oder mechanisch, reproduziert oder übertragen werden.

Microsoft® und Windows® sind eingetragene Warenzeichen der Microsoft Corporation in den USA und/oder anderen Ländern. Alle anderen genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

© NCP engineering, Januar 2010

Zertifikate am Enterprise Client	5
Soft-Zertifikate und Chipkarten	6
Schnittstellen des Clients und PKI-Features	6
Zertifikate zur Authentisierung verwenden	6
Sicherheitsrichtlinien für die PIN-Eingabe	6
CA-Zertifikate	7
Verwendung einer Sperrliste (CRL)	7
Zertifikatskonfiguration	7
Zertifikatsverteilung mit dem Secure Enterprise Management (SEM)	8
Verwendungszwecke der Zertifikate	8
Manuelle Konfiguration	9
Multi-Zertifikatskonfiguration	9
Zertifikatskonfiguration	10
Benutzer-Zertifikat	10
Benutzer-Zertifikat: Entrust Profil	10
Zertifikat aus Chipkartenleser (PC/SC)	11
Zertifikat aus PKCS#12-Datei	12
Zertifikat über CSP	13
Zertifikat aus CSP Benutzer-Zertifikatsspeicher	13
Zertifikat über PKCS#11-Modul	13
Entrust-Profil	13
PIN-Richtlinie	14
Zertifikatsverlängerung	14
Hardware-Zertifikat	15
Zertifikate anzeigen	16
Anzeige von Erweiterungen bei eingehenden und CA-Zertifikaten	18
PIN-Eingabe	20
Sicherung der PIN-Benutzung	20
PC-Sharing (Nutzung mehrerer Soft-Zertifikate an einem PC)	22
Accounting am VPN Gateway	23

Zertifikate am Enterprise Client

Dieses Dokument beschreibt wie Aussteller- und Benutzer-Zertifikate am Secure Client eingespielt werden, wie sie für den gewünschten Verwendungszweck über den Client Monitor konfiguriert werden und welche Auswertungen durch den Client vorgenommen werden können.

Inhaltsübersicht

- Zertifikate am Secure Client
- Manuelle Konfiguration
- Zertifikatskonfiguration
- Benutzer-Zertifikat
- Entrust-Profil
- PIN-Richtlinie
- Zertifikatsverlängerung
- Hardware-Zertifikat
- Zertifikate anzeigen
- PIN-Eingabe
- PC-Sharing
(Nutzung mehrerer Soft-Zertifikate an einem PC)



Weiterführende Beschreibungen zu einem Corporate Network mit Public Key Infrastructure sowie Zertifikats-Rollout und -Updates finden Sie in der Beschreibung zum **Secure Enterprise Management** (PKI Plug-in).



Eine Übersicht bietet die **Enterprise Suite Navigation**. In dieser PDF-Datei sind alle aktuell verfügbaren Dokumente zu Ihrem Client verzeichnet.

Vom Navigator aus können Sie alle relevanten Dokumente direkt anspringen und – falls sie noch nicht in Ihrem Navigatorverzeichnis gespeichert sind – von der NCP Homepage herunterladen.

Soft-Zertifikate und Chipkarten

Zertifikate werden von einer CA (Certification Authority) mittels PKI-Manager Software ausgestellt. Sie können als Soft-Zertifikat in Dateiform erstellt werden oder auf Smartcard (Chipkarte) bzw. USB-Token gespeichert werden. Wie Zertifikate mit dem **Secure Enterprise Management** erstellt werden ist in der Beschreibung zum PKI Plug-in dokumentiert. Prinzipiell können mit dem Secure Client Zertifikate eingesetzt werden, die einen privaten Schlüssel bis zu einer Länge von 4096 Bits haben.

Schnittstellen des Clients und PKI-Features

Der Secure Client kann in Public Key Infrastrukturen nach **X.509 V.3** Standard eingesetzt werden. Die Enterprise-Version besitzt außerdem die Entrust Ready-Funktionalität, womit der Client alle wichtigen Richtlinien von Entrust hinsichtlich des Zertifikatseinsatzes und deren Benutzung unterstützt (siehe die Beschreibung **Entrust-Ready**).



Der Secure Client unterstützt folgende Schnittstellen / Formate:

- Smartcards, USB-Token:
- PKCS#11, TCOS 1.2 und 2.0, CSP
- Soft-Zertifikate: **PKCS#12-Datei**
- PC/SC-konforme **Chipkartenleser**:

Die Client Software unterstützt alle Chipkartenleser, die PC/SC-konform sind. Diese Chipkartenleser werden in einer Liste des Clients aufgenommen, wenn der Leser angeschlossen und die zugehörige Treiber-Software installiert wurde.

– **Automatische Erkennung des angeschlossenen PC/SC-Lesers**: Ist für das PKI-Umfeld die Verwendung eines PC/SC Chipkartenlesers am Client konfiguriert, so erkennt und verwendet der Client automatisch den jeweils angeschlossenen.

Durch diesen Automatismus wird das Anlegen von Profilen am Enterprise Management-System vereinfacht, da in der zentralen Zertifikats-Konfiguration keine benutzerspezifischen Chipkartenleser vorkonfiguriert werden müssen.

Erhält der Benutzer vom Management System eine Konfiguration ohne Eintrag für einen Chipkartenleser und ist ein Zertifikat vorkonfiguriert, so liest der Client automatisch die Daten des PC/SC-Lesers ein, der am Benutzer-PC installiert ist und verwendet diesen Leser.

Dieses Feature ist nur nutzbar in Verbindung mit Smartcards die ohne Schnittstellen-Software direkt angesprochen werden können, wie NetKey-Chipkarten (Telesec).

– **PKCS#11-Modul**: Mit der Software für die Smartcards oder den Tokens werden Treiber in Form einer PKCS#11-Bibliothek (DLL) mitgeliefert. Diese Treiber-Software muss zunächst installiert werden. Anschließend kann über einen Assi-

stenten das entsprechende PKCS#11-Modul selektiert werden.

Der Secure Client verfügt außerdem über folgende Leistungsmerkmale:

- **Automatischer Download der Sperrliste** von der CA (Certification Authority): Der Client unterstützt die **Zertifikatserweiterung CDP** (Certificate Distribution Point), wodurch ein automatische Download der Sperrliste angeregt wird und eingehende Zertifikate daraufhin überprüft werden, ob sie in der CRL geführt sind.
- **PIN-Richtlinie**: Der Administrator kann Bedingungen für die Eingabe beliebig komplexer PINs vorgeben. Sie treten dann in Kraft wenn der Benutzer die PIN ändern möchte.
- **Zertifikats-Überprüfung**: Am Secure Client kann pro Link-Profil festgelegt werden, welche Einträge in einem Zertifikat der Gegenstelle vorhanden sein müssen damit eine Verbindung hergestellt wird.
- **Zertifikatsverlängerung**: Der Administrator kann vorgeben ob und wie viele Tage vor Ablauf der Gültigkeit des Zertifikats eine Meldung ausgegeben werden soll, die vor dem Ablauf der Gültigkeit warnt. Bei Einsatz des Enterprise Clients kann die Verlängerung der Gültigkeitsdauer eines Zertifikats bzw. ein **Zertifikats-Update** automatisiert werden.

Zertifikate zur Authentisierung verwenden

Um für IPsec-Verbindungen Zertifikate zur Authentisierung verwenden zu können, darf für die IKE-Richtlinie (Phase 1-Verhandlung) kein Pre-shared Key eingetragen sein. Nur dann können auch zertifikatsbasierte Vorschläge (Proposals) mit RSA-Signatur zur Gegenstelle geschickt werden. (Am Enterprise Client wird dies unter **Security** konfiguriert.) Für IPsec-Verbindungen ist der **automatische Modus** die Standardeinstellung, ansonsten wird die Verschlüsselung für IPsec-Verbindungen in der **IPsec-Konfiguration** definiert.

Für **L2sec-Verbindungen** mit dem Enterprise Client wird das Verschlüsselungsverfahren im Konfigurationsfeld Security bestimmt.

Sicherheitsrichtlinien für die PIN-Eingabe

Um ein Zertifikat einsetzen zu können, muss immer auch eine PIN eingegeben werden. Für diese **PIN-Eingabe** und für die Dauer der Gültigkeit wurden spezielle Sicherheitsrichtlinien implementiert. So wird z. B. der **PIN-Status** im Monitor des Clients

dargestellt. Die PIN kann manuell über das Monitor-menü oder nach Entfernen des Zertifikats zurückgesetzt werden. So überwacht die Client Software, ob eine PKCS#12-Datei vorhanden ist. Wird eine PKCS#12-Datei (Soft-Zertifikat) eingesetzt, z. B. auf einem USB-Stick oder einer SD-Karte gespeichert, so wird nach dem Ziehen der SD-Karte die PIN zurückgesetzt und eine bestehende Verbindung abgebaut. Dieser Vorgang entspricht dem **Verbindungsabbau bei gezogener Chipkarte**, der bei Verwendung einer Chipkarte im Monitor-menü unter "Konfiguration / Benutzer-Zertifikat" eingestellt werden kann. Wird später die SD-Karte wieder gesteckt, kann nach der erneuten PIN-Eingabe die Verbindung wieder hergestellt werden.

CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies geschieht dadurch, dass er die CA-Zertifikate seiner Wahl in das Installationsverzeichnis unter <CACERTS> einspielt. Das Einspielen kann bei der Software-Distribution automatisiert stattfinden, wenn sich die Aussteller-Zertifikate bei der Installation der Software von einem Datenträger dort im Verzeichnis <DISK1> befinden. Beachten Sie dazu die Beschreibung zur erweiterten Installation in der **Enterprise-Installationsbeschreibung**.

Nachträglich können Aussteller-Zertifikate automatisch über den Secure Management Server (nur zu Enterprise Clients) verteilt werden oder, sofern der Benutzer über die notwendigen Schreibrechte in genanntem Verzeichnis verfügt, von diesem selbst eingestellt werden.

Derzeit werden die Formate *.pem und *.crt für Aussteller-Zertifikate unterstützt. Sie können im Monitor unter dem Hauptmenüpunkt "Verbindung / Zertifikate / **CA-Zertifikate anzeigen**" eingesehen werden.

Wird am Secure Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der NCP Client den Aussteller indem er das Aussteller-Zertifikat, zunächst auf Smartcard bzw. USB-Token oder in der PKCS#12-Datei, anschließend im Installationsverzeichnis unter <CACERTS> sucht. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande. Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

Werden Soft-Zertifikate mit dem PKI Plug-in des Management Servers erstellt, so wird das Aussteller-Zertifikat in der PKCS#12-Datei gespeichert.

Verwendung einer Sperrliste (CRL)

Zu jedem Aussteller-Zertifikat kann dem Secure Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Installationsverzeichnis unter <CRLS> gespeichert. Ist eine CRL vorhanden, so überprüft der Secure Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Der Client lädt die zugehörige CRL automatisch herunter wenn das eingehende Benutzer-Zertifikat des Servers die **Zertifikatserweiterung CDP** enthält.

Werden Sperrlisten eingesetzt, so werden *normalerweise dann keine Meldungen ausgegeben, wenn am Client keine Sperrliste für eingehende Zertifikate hinterlegt ist*. Soll in solchen Fällen dennoch eine Meldung ausgegeben werden, muss die Datei NCPPKI.CONF editiert werden. Sie befindet sich im Installations-Verzeichnis. Der Standardeintrag im Abschnitt [General] lautet:

```
Enablecrlinfo = 0
```

Dies bewirkt, dass keine Meldungen ausgegeben werden, wenn zu einem Zertifikat der Gegenstelle keine Sperrliste am Client gefunden wird. Soll eine Meldung ausgegeben werden, so muss diese Einstellung abgeändert werden auf:

```
Enablecrlinfo = 1
```

Zertifikatskonfiguration

In der Konfiguration des Clients kann eine Vielzahl individueller Zertifikateinstellungen als **Multi-Zertifikatskonfiguration** hinterlegt werden. Aus den verschiedenen Zertifikatskonfigurationen kann pro Profil jeweils eine selektiert werden. Dadurch besteht die Möglichkeit unterschiedlicher Authentisierung mit verschiedenen Zertifikaten gegen verschiedene VPN-Gegenstellen, z. B. zu VPN Gateway 1 mit Softzertifikat und zu Gateway 2 mit einem auf Smartcard gespeicherten Zertifikat.

Die Zertifikatskonfiguration eines Clients älter als Version 9.1 wird bei einem Update auf diese Version automatisch in die **Standard Zertifikatskonfiguration** konvertiert. Ebenso wird die Standard-Zertifikatskonfiguration nach einer Erstinstallation der Version 9.1 eingerichtet wenn eine Testverbindung mit Zertifikat angelegt wird.

Eine spezielle Funktion zur **Soft-Zertifikatsauswahl** gestattet **PC-Sharing** für mehrere Benutzer, wobei jeder Benutzer des PCs mit seinem eigenen Zertifikat arbeitet.

In der Zertifikats-Konfiguration können für die Pfad-Angaben die Umgebungsvariablen des Betriebssystems am Benutzer-PC eingesetzt werden. Die Variablen werden beim Schließen des Dialogs und beim Einlesen der Profil-Einstellungen umge-

wandelt und in die Konfiguration zurück geschrieben. Existiert eine Umgebungsvariable nicht, wird sie aus dem Pfad beim Umwandeln entfernt und ein Log-Eintrag ins Logbuch geschrieben. Fehlt ein %-Zeichen (Syntax), bleibt die Variable stehen und es wird ebenfalls ein Log-Eintrag geschrieben.

Der VPN-Benutzername muss mit der Profil-Einstellung in der Client Software (siehe **Tunnel-Parameter**) übereinstimmen. Dieser Eintrag wird in der Client-Konfiguration des SEM "ID für personalisierte Profil-Einstellungen" (**RSU-ID**) eingegeben und mit dem PIN-Brief an den Erstbenutzer verteilt.



Zertifikatsverteilung mit dem Secure Enterprise Management (SEM)

Die automatische Zertifikatsverteilung ist nur mit dem Secure Enterprise Management für Enterprise Clients möglich. Zwischen Update Client und Management Server wird dafür zusätzlich der Port 829 (TCP) benötigt. Die PIN für das Benutzer-Zertifikat wird vor dem Speichern der PKCS#12-Datei abgefragt. Beim Hardware-Zertifikat wird diese durch die Hardware automatisch ermittelt.



Hardware-Zertifikate können über das CMP (Certificate Management Protocol) vom Secure Enterprise Management automatisiert verteilt werden. Dabei ist das erstmalige Herunterladen nur bei der ersten Verbindung eines **Init-Benutzers** mit dem Management-System möglich. In der Zertifikatskonfiguration des Init-Benutzers, der am Management-System für Rollout-Zwecke erstellt wird, muss vor dem Herunterladen ein Dateiname für die PKCS#12-Datei angegeben sein, auch wenn diese Datei noch nicht vorhanden ist. Ist keine Zertifikatskonfiguration definiert, wird auch kein Zertifikat heruntergeladen.

Nach dem Verbindungsaufbau zum Management Server und der Eingabe des Benutzernamens sowie des Authentisierungsschlüssels wird das Hardware-Zertifikat heruntergeladen und in der angegebenen Datei gespeichert. Nach dem erfolgreichen Herunterladen kann das Zertifikat im Client-Monitor unter Menüpunkt "Verbindung / Zertifikate / **Hardware-Zertifikat**" angezeigt werden.

Verwendungszwecke der Zertifikate



Der Verwendungszweck des Zertifikats kann bei der Erstellung am SEM als **VPN-Zertifikat** (Benutzer-Zertifikat) oder **Hardware-Zertifikat** festgelegt werden. Die am SEM erstellten Zertifikate können direkt in der Datenbank des Management Servers hinterlegt werden. Mit **VPN-Benutzername** aus Zertifikat ist die Zuordnung des Zertifikats zum jeweiligen Benutzer eindeutig. Diese ID kann sich zum Beispiel aus dem Common Name oder dem E-Mail-Namen des Zertifikats und einem Suffix zusammensetzen. (Der Suffix kann z. B. bei Namensgleichheit verwendet werden, oder um Gruppenzugehörigkeiten zu unterscheiden.)

Multi-Zertifikatskonfiguration



Der Standardpfad für Soft-Zertifikate ist das Installationsverzeichnis der Client Software. Dies ist auch der Standardpfad für Soft-Zertifikate, die bei einem Rollout oder bei einem Zertifikats-Update vom Management-System heruntergeladen werden. Im Installationsverzeichnis befinden sich immer auch Test-Zertifikate für den Benutzer (Client1.p12 bis Client4.p12) sowie ein CA-Zertifikat für Testzwecke (NCPSupportCA.pem).

Der Standardpfad für Zertifikate, insbesondere für Zertifikate auf Tokens oder Smartcards, kann unter Verwendung von Systemvariablen (am SEM) oder unter manueller Eingabe von Pfad und Dateinamen geändert werden.

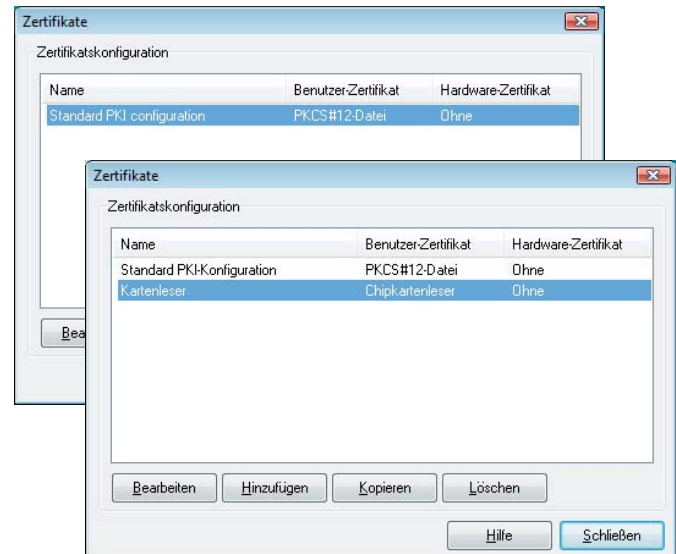
Manuelle Konfiguration



Die manuelle Zertifikatskonfiguration erfolgt am Secure Client im wesentlichen genauso wie im Client Configuration Plug-in des Enterprise Managements unter "PKI-Konfiguration" in der Client-Vorlage, wo mehrere verschiedene Zertifikatskonfigurationen angelegt werden können. (Dies gilt für SEM-Versionen ab 2.02 und Client-Versionen ab 9.10.)

Auch am Secure Client können mehrere verschiedene Zertifikatskonfigurationen angelegt werden, nachdem Sie im Konfigurationsmenü des Client-Monitors das Untermenü "Zertifikate" selektiert haben (Abb. oben). Prinzipiell kann eine Vielzahl von Zertifikatskonfigurationen unter einem jeweils eigenen Namen hinterlegt werden.

Nachdem "Zertifikate" selektiert wurde, wird eine Standard PKI-Konfiguration angezeigt (Abb. unten). Betätigen Sie den Bearbeiten- oder Hinzufügen-Button und Sie können eine neue Zertifikatskonfiguration mit neuem Namen hinzufügen (unten "Kartenleser") oder eine bestehende ändern (siehe nächste Seite).



Name und "Standard Zertifikatskonfiguration"

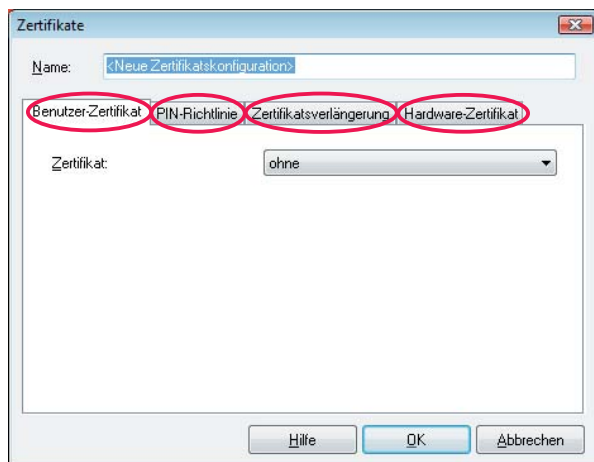
Die Zertifikatskonfiguration eines Clients älter als Version 9.1 wird bei einem Update auf 9.1 automatisch in die "Standard-Zertifikatskonfiguration" konvertiert. Ebenso wird die "Standard-Zertifikatskonfiguration" nach einer Erstinstallation der Version 9.1 eingerichtet.

Aus den verschiedenen Zertifikatskonfigurationen kann pro Profil jeweils eine selektiert werden. Dadurch besteht die Möglichkeit der Authentisierung mit verschiedenen Zertifikaten gegen unterschiedliche VPN-Gegenstellen, z. B. zu VPN Gateway 1 mit Softzertifikat und zu Gateway 2 mit einem auf Smartcard gespeicherten Zertifikat.



Im Konfigurationsfeld **Security** kann das Zertifikat dieser Zertifikatskonfiguration für die Verschlüsselung und Authentisierung im **Security-Modus L2sec** oder für die **erweiterte Authentisierung** (Extended Authentication) im **Security-Modus IPsec** selektiert werden.

Zertifikatskonfiguration



Nachdem Sie den Bearbeiten- oder Hinzufügen-Button betätigt haben, können Sie die Standardkonfiguration ändern und der Zertifikatskonfiguration einen neuen Namen geben.

Zunächst wird festgelegt, ob Zertifikate zur Authentisierung des Clients eingesetzt werden und wo die **Benutzer-Zertifikate** hinterlegt werden.

In weiteren Konfigurationsfeldern werden die **Richtlinien zur PIN-Eingabe** festgelegt und das Zeitintervall eingestellt, in dem vor dem Ablauf des Zertifikats gewarnt und somit auf eine anstehende **Zertifikatsverlängerung** aufmerksam gemacht wird.

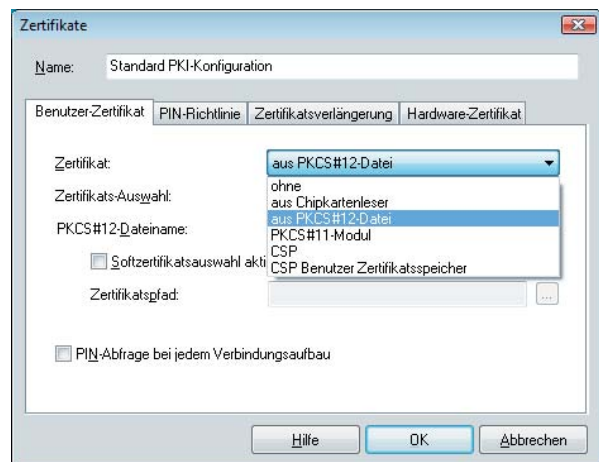
Zusätzlich kann ein **Hardware-Zertifikat** konfiguriert werden.

Benutzer-Zertifikat: Entrust Profil



Beachten Sie hierzu bitte die Beschreibung zur **Entrust Ready-Funktionalität**.

Benutzer-Zertifikat



ohne

Wählen Sie in der Listbox "Zertifikat" die Einstellung "ohne", so wird kein Zertifikat ausgewertet und die erweiterte Authentisierung findet nicht statt.

aus Chipkartenleser

Wählen sie "aus Chipkartenleser" in der Listbox, so werden bei der erweiterten Authentisierung die Zertifikate von der Smartcard in ihrem Chipkartenleser ausgelesen.

aus PKCS#12-Datei

Wählen Sie "aus PKCS#12 Datei" aus der Listbox, so werden bei der erweiterten Authentisierung die Zertifikate aus einer Datei auf der Festplatte Ihres Rechners gelesen.

über PKCS#11-Modul

Wählen Sie "aus PKCS#11-Modul" aus der Listbox, so werden bei der erweiterten Authentisierung die Zertifikate aus einem Token über ein PKCS#11 Modul gelesen.

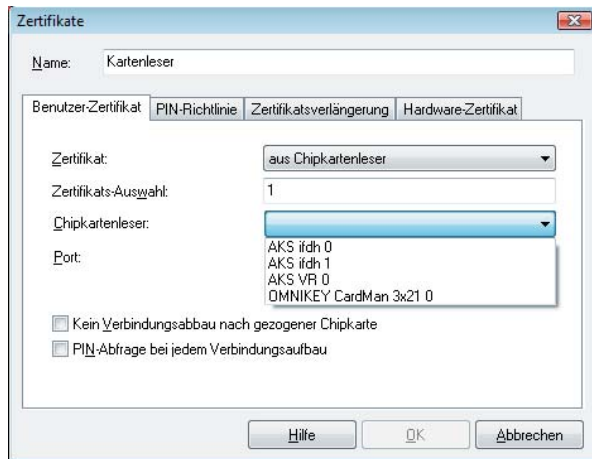
über CSP

Wurde diese Zertifikatsquelle selektiert, so wird das Zertifikat von einer Chipkarte oder von einem Token über den Windows CSP (Certificate Service Provider) gelesen.

aus CSP Benutzer-Zertifikatsspeicher

Wählen Sie den "CSP Benutzer-Zertifikatsspeicher" in der Listbox, so wird zur erweiterten Authentisierung das Zertifikat aus dem CSP Benutzer-Zertifikatsspeicher verwendet.

Zertifikat aus Chipkartenleser (PC/SC)



Wenn Sie die Zertifikate von der Smartcard mit Ihrem Lesegerät nutzen wollen, wählen Sie Ihren Chipkartenleser aus der Listbox. (Siehe auch: PIN eingeben).

Zertifikat aus Chipkartenleser

Die Client Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind und erkennt diese automatisch wenn sie korrekt angeschlossen sind.

Die PC/SC-Schnittstelle wird nur geöffnet, wenn ein Verbindungsaufbau stattfindet, bei dem ein Chipkartenzugriff erfolgt. D. h. auch andere Applikationen können im "exklusiven" Modus die PC/SC-Schnittstelle öffnen.

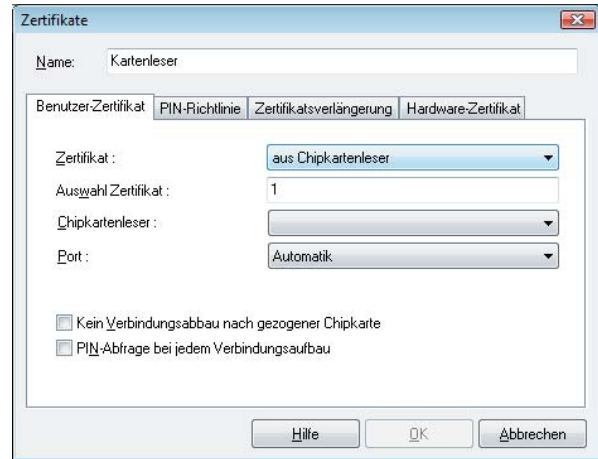


Hinweis: Ist vom Administrator bei der Erstellung der Profile mit dem zentralen Management-System die Verwendung eines Zertifikats über einen PC/SC-Chipkartenleser vorgesehen, so kann folgender Automatismus genutzt werden:

Erhält der Benutzer vom Management System ein Profil ohne Eintrag für einen Chipkartenleser und ist ein Zertifikat vorkonfiguriert, so liest der Client automatisch die Daten desjenigen PC/SC-Lesers ein, der am Benutzer-PC installiert ist und verwendet diesen Leser.

Dieses Feature ist nur nutzbar in Verbindung mit Smartcards die ohne Schnittstellen-Software direkt angesprochen werden können (z. B. TCOS, Netkey von Telesec und TC Trust).

Chipkartenleser



Wird der Chipkartenleser nach dem Client installiert, erkennt der Client den angeschlossenen Chipkartenleser erst nach einem Boot-Vorgang (Abb. oben). Erst dann kann der installierte Leser ausgewählt und genutzt werden.

Auswahl Zertifikat

1. Zertifikat ...4.

(Standard = 1) Aus der Listbox kann aus bis zu vier verschiedenen Zertifikaten gewählt werden, die sich auf der Chipkarte befinden. Die Anzahl der Zertifikate auf der Chipkarte ist abhängig von der Registration Authority, die diese Karte brennt. Wenden Sie sich zu weiteren Fragen bitte an Ihren Systemadministrator.

Auf den Chipkarten von NetKey 2000 befinden sich drei Zertifikate:

- (1) zum Signieren
- (2) zum Ver- und Entschlüsseln
- (3) zum Authentisieren (optional bei NetKey 2000)

Port

Haben Sie oben "aus Chipkartenleser" gewählt, so muss hier der Port für den Chipkartenleser eingegeben werden.

Automatik

Der Port wird bei korrekter Installation des Lesege-
räts automatisch bestimmt.

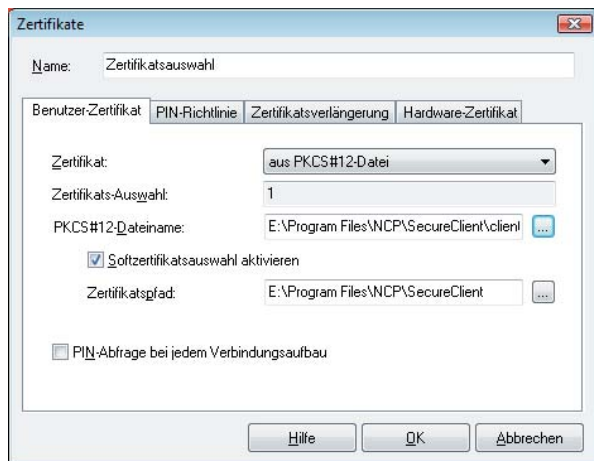
COM1 ... COM4 :

Bei Unstimmigkeiten können die COM Ports 1-4 gezielt angesteuert werden.

Verbindungsabbau bei gezogener Chipkarte

Beim Ziehen der Chipkarte wird nicht unbedingt die Verbindung abgebaut. Ob "Kein Verbindungsabbau bei gezogener Chipkarte" erfolgt, wird an dieser Stelle eingestellt.

Zertifikat aus PKCS#12-Datei



PKCS#12-Dateiname

Nutzen Sie das PKCS#12-Format, so erhalten Sie von Ihrem Systemadministrator eine Datei, die auf der Festplatte Ihres Rechners eingespielt werden muss. In diesem Fall muss Pfad und Dateiname der PKCS#12 Datei eingegeben, bzw. nach einem Klick auf den [...] -Button (Auswahl-Button) muss die Datei ausgewählt werden.

Wichtig: Die Strings für den Dateinamen können mit Variablen eingegeben werden. Dies erleichtert insbesondere das Handling der Konfigurationsdateien mit dem Client Plug-in des SEM, da nun für alle Benutzer die gleichen Strings mit Umgebungsvariablen eingegeben werden können. Zum Beispiel:

```
%SYSTEMROOT% > Windows-Verzeichnis (c:\Windows)
%INSTALLDIR% > NCP Installationsverzeichnis (c:\Programme\NCP\SecureClient)
%PROGDIR% > Windows Programmverzeichnis (c:\Programme)
%windir% > C:\Windows
%NCPUSERDIR% > Mit diesem Platzhalter für die Konfiguration der P12-Datei wird das Benutzer-Verzeichnis (z. B. C:\Dokumente und Einstellungen\UserXY) ersetzt. Somit ist es möglich, dass sich mit dieser Zertifikatskonfiguration der aktuelle Windows-Benutzer mit seinen Zertifikatsdaten am VPN-Gateway anmeldet. (Diese Funktion wird nicht in der NCP GINA unterstützt).
```

Softzertifikatsauswahl aktivieren



Diese Funktion wird nur für PC-Sharing benötigt, wenn die Benutzer des PCs mit Soft-Zertifikaten arbeiten. Beachten Sie dazu unbedingt die Beschreibung weiter unten **Nutzung mehrerer Soft-Zertifikate mit einem Link-Profil**.

Bei Einsatz von Soft-Zertifikaten kann der Zertifikatspfad für die PKCS#12-Dateien festgelegt werden, nachdem die Softzertifikatsauswahl aktiviert wurde. Unter dem Parameterfeld des Monitors erscheint dann ein Auswahlfeld mit allen Zertifikaten unter dem angegebenen Verzeichnis (siehe **Client-Monitor**). Wird ein Soft-Zertifikat ausgewählt, wird die zu diesem Zertifikat gehörige Konfigurati-

on aktiv und entsprechend die Verbindung abgebaut und die PIN zurückgesetzt. Alternativ kann bei einem Benutzerwechsel die PIN über den Button "Abmelden" oder über das Menü "PIN zurücksetzen" zurückgesetzt werden.

Zertifikatspfad

Der Zertifikatspfad wird nur bei PC-Sharing benötigt.

PIN-Abfrage bei jedem Verbindungsaufbau

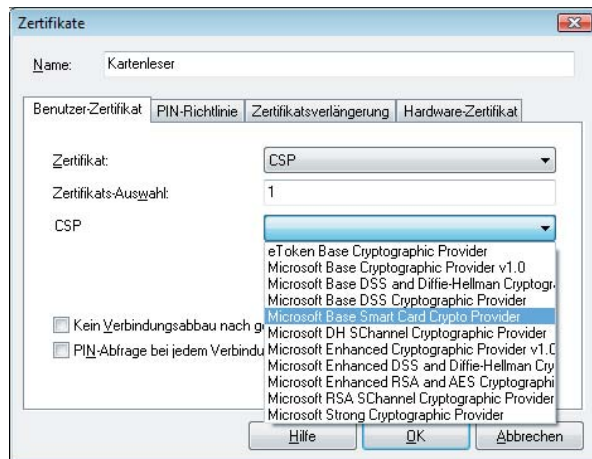
Hier kann eingestellt werden, dass die PIN nicht nur nach jedem ersten Verbindungsaufbau nach dem Booten des PCs sondern vor jedem Verbindungsaufbau korrekt eingegeben werden muss. Diese Funktionalität, die für alle Verbindungsmodi (manuell, automatisch, wechselnd) genutzt werden kann, erfordert, dass der Monitor gestartet ist. Der Monitor darf allerdings minimiert sein.



Wichtig: Ist der Monitor nicht gestartet, kann kein PIN-Dialog erfolgen. In diesem Fall wird bei einem automatischen Verbindungsaufbau die Verbindung ohne erneute PIN-Eingabe hergestellt!



Zertifikat über CSP



Wurde diese Zertifikatsquelle selektiert, so wird das Zertifikat von einer Chipkarte oder von einem Token über den Windows CSP (Certificate Service Provider) gelesen, wenn die entsprechende Schnittstelle am CSP installiert und registriert wurde.

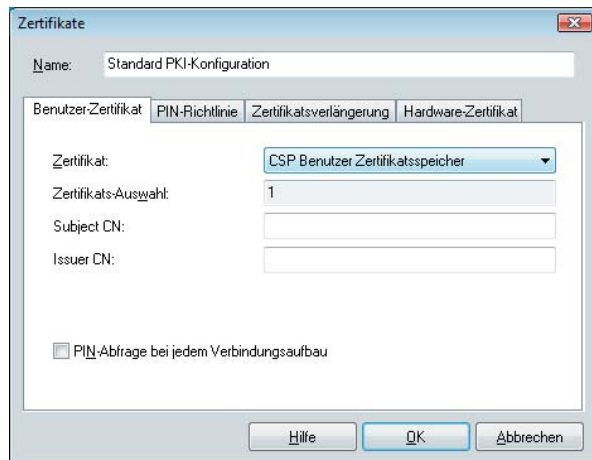


Ist die Zertifikatsnummer "0" konfiguriert, wird das erste gefundene Zertifikat mit der Erweiterung "SSL Client Authentication" verwendet.



Bitte beachten Sie, dass derzeit der Zugriff auf den Benutzer-Zertifikatsspeicher von Windows nicht unterstützt wird.

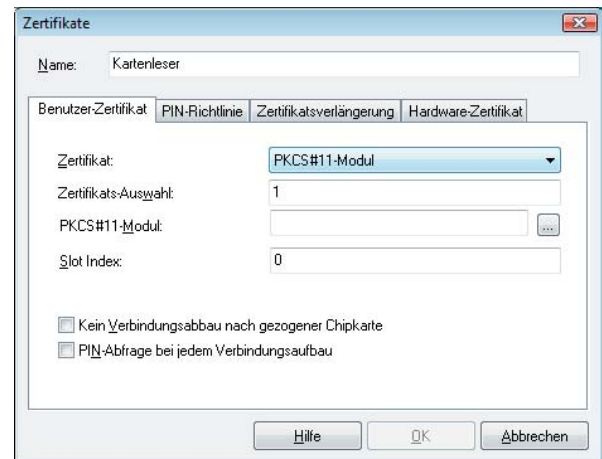
Zertifikat aus CSP Benutzer-Zertifikatsspeicher



Wählen Sie den "CSP Benutzer-Zertifikatsspeicher" in der Listbox, so wird zur erweiterten Authentisierung das Zertifikat aus dem CSP Benutzer-Zertifikatsspeicher verwendet, dessen "Subject CN" und "Issuer CN" Sie in die entsprechenden Felder eintragen.

Da diese Funktionalität erst nach einer Anmeldung des Benutzers am Windows-System zur Verfügung steht, kann sie nicht zur Domänenanmeldung über VPN eingesetzt werden!

Zertifikat über PKCS#11-Modul



Nutzen Sie das PKCS#11-Format, so erhalten Sie eine DLL vom Hersteller des Chipkartenlesers oder des Tokens, die auf der Festplatte Ihres Rechners eingespielt werden muss. In diesem Fall muss Pfad und Dateiname des Treibers eingegeben werden.

Mit Hilfe eines Assistenten können Sie nach installierten PKCS#11-Modulen suchen und das gewünschte Modul mit dem dazugehörigen Slot selektieren. Dazu klicken Sie auf den [...] -Button in der Zeile mit PKCS#11-Modul (siehe Bild oben).

Entrust-Profil



Beachten Sie hierzu bitte die Beschreibung zur **Entrust Ready-Funktionalität**.

Die NCP Entrust Ready-Zertifizierung wurde für den NCP Secure Windows Client der Version 7.03 SP6 und Version 7.22 erteilt.

Wählen Sie "Entrust-Profil" in der Listbox, so wird das zugehörige Zertifikat geladen.

Die Angabe eines Profil-Dateinamens ist nicht nötig, da dieser nochmals vom Assistenten verlangt wird, nachdem der Menüpunkt "Lade Entrust Profil" gewählt wurde. Dieser Name wird dann automatisch nach dem Herunterladen des Profils eingetragen. (Ggf. kann an dieser Stelle zwischen dem Profil von einer Datei auf Festplatte (*.EPF) oder dem von einem Token (*.TKN) gewählt werden.

Wichtig: Erst nachdem als Benutzer-Zertifikat das "Entrust Profil" eingestellt wurde, wird der Menüpunkt "Lade Entrust Profil" selektierbar.

Beachten Sie, dass über den SEM die Eingabefelder im Entrust-Assistenten für den Profilpfad und Profilnamen vorkonfiguriert werden können.

PIN-Richtlinie

Der Administrator (oder Benutzer) kann PIN-Richtlinien festlegen, die bei der PIN-Eingabe oder -Änderung beachtet werden müssen. Die hier ausgewählten Richtlinien erscheinen als Liste von Bedingungen, die bei der Änderung der PIN eingehalten werden müssen (Abb. unten).

Zertifikatsverlängerung

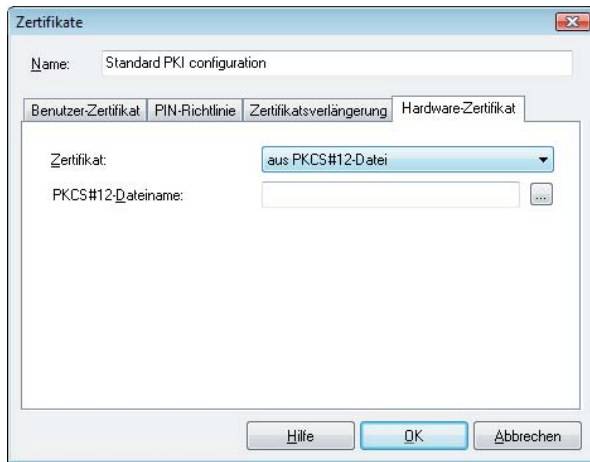
Hier wird eingestellt, ob und wie viele Tage vor Ablauf der Gültigkeit des Zertifikats eine Meldung ausgegeben werden soll, die vor dem Ablauf der Gültigkeit warnt. Sobald die eingestellte Zeitspanne vor Ablauf in Kraft tritt, wird bei jeder Zertifikatsverwendung eine Meldung aufgeblendet, die auf das Ablaufdatum des Zertifikats hinweist.



Gültigkeitsverlängerung von Soft-Zertifikaten über Enterprise Management

Am Enterprise Client wird zunächst die PKCS#7-Datei im RSUDATA-Verzeichnis gespeichert. Nach dem Verbindungsabbau wird überprüft, ob für diesen Benutzer eine PKCS#7 Datei vorhanden ist. Ist dies der Fall, wird das alte Zertifikat unter einem neuen Dateinamen gespeichert und anschließend das neue Zertifikat mit neuem Private-Key in der konfigurierten PKCS#12-Datei mit der eingegebenen PIN gespeichert. Der Benutzer erhält danach einen Hinweis, dass sein Zertifikat erneuert wurde. Voraussetzung ist der Einsatz des PKI-Plug-ins mit dem Secure Enterprise Management.

Hardware-Zertifikat



Die zusätzliche Authentisierung mit einem Hardware-Zertifikat ist nur mit dem Tunnel-Protokoll IPsec möglich. Zur Aktivierung der Funktion muss am Gateway ab Version 6.02 Build 14 die Option "Hardware-Zertifikat CN" unter Link-Profile eingeschaltet werden. Mit einem Hardware-Zertifikat authentisiert sich der Rechner gegenüber dem Gateway. Wird es zusätzlich zu einem Benutzer-Zertifikat eingesetzt, so kann sichergestellt werden, dass sich der Benutzer immer vom gleichen Rechner aus zum Gateway verbindet.

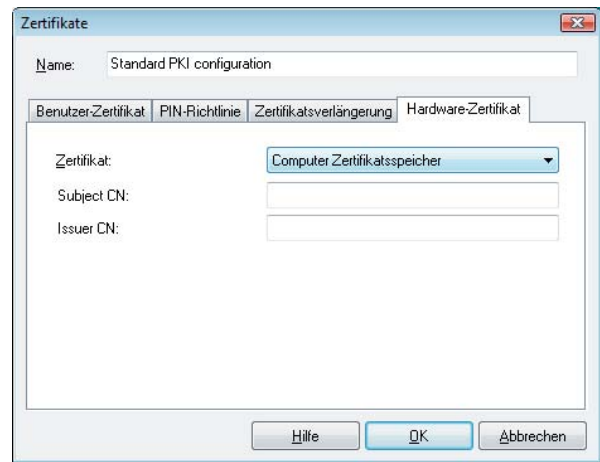
Zertifikat aus PKCS#12-Datei

Ein Hardware-Zertifikat kann als PKCS#12-Datei oder als Entrust-Profil eingespielt werden. Der entsprechende Dateiname ist anzugeben. Die Eingabe einer PIN entfällt bei dem Hardware-Zertifikat. Sie erfolgt automatisch im Hintergrund, ohne dass der Anwender eine Eingabe machen muss. Als PIN für das Zertifikat wird die Seriennummer des Rechners oder der Festplatte verwendet.

Soll ein Entrust-Profil herunter geladen werden, so muss der Common Name des Zertifikats mit dem Wert der System-Umgebungsvariable WS-NAME übereinstimmen. Ansonsten wird das Entrust-Profil nicht geladen. Die PIN-Vergabe erfolgt automatisch.

Vorgaben für die PIN und die Umgebungsvariable sind in der Datei NCPHWINFO.DLL festgelegt. Werden andere Vorgaben erforderlich, muss diese DLL geändert und ausgetauscht werden. Beim Erzeugen eines Hardware-Zertifikats als PKCS#12-Datei muss die PIN manuell vergeben werden. Mit dem Programm HWINFO.EXE kann die Seriennummer des Rechners, welche als PIN verwendet wird, ausgelesen werden. Die PIN ist mindestens 8 und maximal 20 Zeichen lang.

Computer-Zertifikatsspeicher



Mit dieser Einstellung kann der lokale Computer Zertifikatsspeicher von Windows für die Ablage von Zertifikaten genutzt werden. Wurde ein Zertifikat im lokalen Computer-Zertifikatsspeicher von Windows abgelegt, d. h. unter Windows in diesen Zertifikatsspeicher importiert, so kann dieses Zertifikat vom Client zur Authentisierung genutzt werden.



Bitte beachten Sie, dass derzeit der Zugriff auf den Benutzer-Zertifikatsspeicher nicht unterstützt wird.



Im Unterschied zu den benutzerspezifischen Zertifikaten im Zertifikatsspeicher für Windows-Benutzer-Zertifikate, die erst dann eingesetzt werden können, nachdem sich der Windows-Benutzer angemeldet hat, können Hardware-Zertifikate aus dem "Computer-Zertifikatsspeicher" bereits nach dem Booten eingesetzt werden (z. B. für die Domänen-Anmeldung).



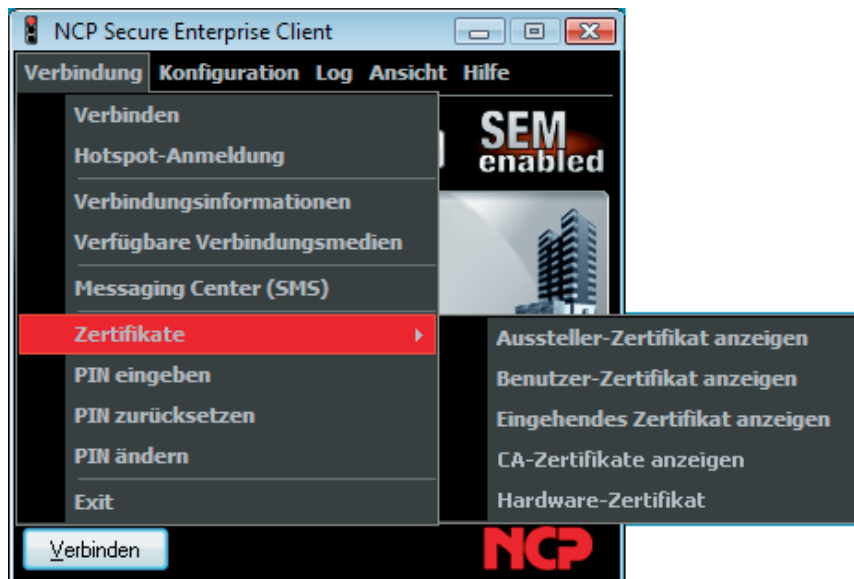
Da ein einmal importiertes Zertifikat nicht mehr exportiert werden kann, kann bei Wahrung der Sicherheitsaspekte auf eine PIN-Eingabe verzichtet werden. Diese Zertifikate können daher auch von Diensten genutzt werden, die die PIN nicht abfragen können.

Die Authentisierung mittels Hardware-Zertifikat ohne PIN-Eingabe ist dann am Client korrekt konfiguriert, wenn nach dem Start des Monitors das grüne PIN-Symbol angezeigt wird (siehe **Client-Monitor**).

Subject CN / Issuer CN

Das jeweilige Zertifikat aus dem Computer Zertifikatsspeicher kann mit dem zugehörigen Common Name von Antragsteller und Aussteller (Subject CN und Issuer CN) selektiert werden, sofern mehrere Zertifikate vorhanden sind.

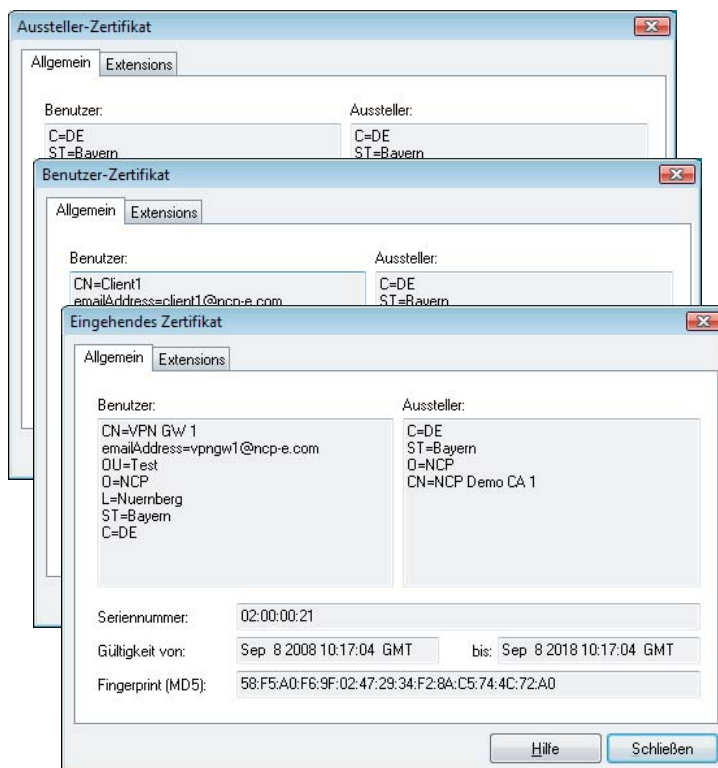
Zertifikate anzeigen



Wenn Sie sich ein Aussteller-, Benutzer- oder Hardware-Zertifikat anzeigen lassen, werden die zur Erstellung des Zertifikats genutzten Merkmale gezeigt, z. B. die eindeutige E-Mail-Adresse.

Das eingehende Zertifikat wird bei der SSL-Verhandlung von der Gegenstelle übermittelt. Sie können z. B. sehen, ob Sie den hier gezeigten Aussteller in der Liste Ihrer CA-Zertifikate aufgenommen haben.

Je nachdem, welche Zertifikate konfiguriert wurden und ob nach einem Verbindungsaufbau bereits ein Zertifikat der Gegenstelle eingegangen ist, können die jeweiligen Zertifikate über das Verbindungs-menü des Monitors betrachtet werden (Abb. oben und unten).



Aussteller (CA)

Benutzer und Aussteller eines Aussteller-Zertifikates müssen für gewöhnlich identisch sein (self-signed certificate).

Der Aussteller Ihres Benutzer-Zertifikates muss mit dem Aussteller des Aussteller-Zertifikates identisch sein.

Seriennummer

Nach der Seriennummer werden die Zertifikate ggf. mit den in der Revocation List der Certification Authority gehaltenen verglichen.

Gültigkeitsdauer

Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit Erlöschen der Gültigkeit geht auch die Funktion des Zertifikats verloren. Mit dem Erlöschen der Gültigkeit des Aussteller-Zertifikats erlischt automatisch die Gültigkeit eines vom gleichen Aussteller ausgestellten Benutzer-Zertifikats.

Fingerprint

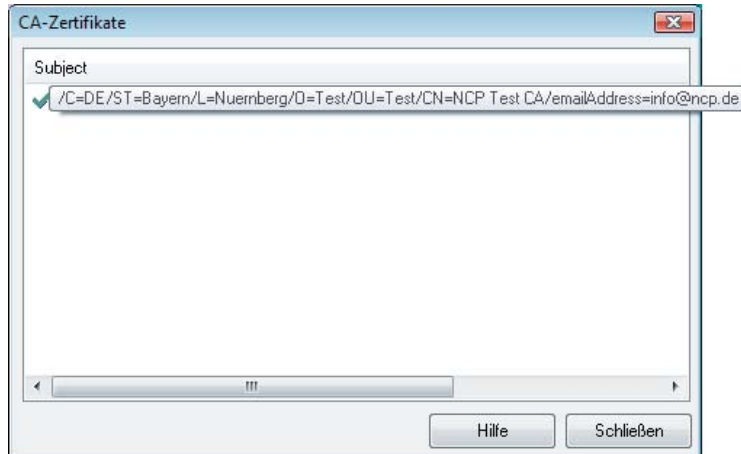
Der Fingerprint ist ein Hash-Wert, der über das Zertifikat gebildet wird, um dessen Eindeutigkeit mit anderen Zertifikaten vergleichen zu können.



Die Anzeigefelder unter "Allgemein" sind für alle Zertifikate außer dem CA-Zertifikat gleich. Daher sind im folgenden diese Felder nur einmal beschrieben.

CA-Zertifikate anzeigen

Die Client Software verfügt über eine Multi CA-Unterstützung. Dazu müssen die Aussteller-Zertifikate im Installations-Verzeichnis unter <CA-CERTS> gesammelt werden. Dies ist dann sinnvoll wenn das Benutzer-Zertifikat einer Gegenstelle von einer anderen CA ausgestellt wurde als das Benutzer-Zertifikat des Clients.



Gültige CA-Zertifikate werden mit einem grünen Haken markiert, ungültige mit einem roten Kreuz (Abb. oben). Mit Doppelklick auf eines der CA-Zertifikate werden die gleichen Anzeigefelder gezeigt wie auf der vorigen Seite beschrieben.

Wird das Zertifikat einer Gegenstelle empfangen, so ermittelt der Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smartcard oder in der PKCS#12-Datei, anschließend im Installations-Verzeichnis unter <CA-CERTS>. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande. Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen. (Siehe oben **CA-Zertifikate**.)



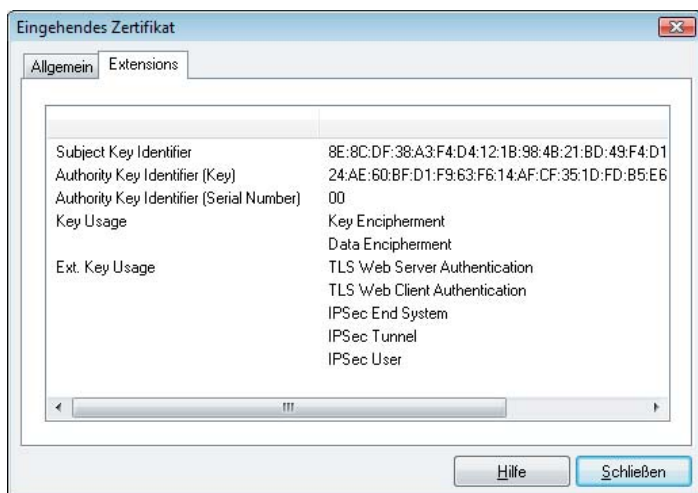
Bitte beachten Sie zum Einspielen eines CA-Zertifikats auch die Beschreibung der erweiterten Installation in der **Enterprise-Installationsbeschreibung**.

Anzeige von Erweiterungen bei eingehenden und CA-Zertifikaten

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zertifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen werden von der ausstellenden Certification Authority in das Zertifikat geschrieben. Für den Secure Client und den Secure Server sind folgende Erweiterungen von Bedeutung:

- KeyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- CDP (Certificate Distribution Point)

Das CA-Zertifikat, dessen Erweiterungen angezeigt werden sollen, muss mit einem Doppelklick im Fenster für CA-Zertifikate (siehe oben) geöffnet werden. Das Ansichtsfeld “Extensions” zeigt die Zertifikatserweiterungen, sofern sie vorhanden sind (Abb. unten).



KeyUsage

Ist in einen eingehenden Zertifikat die Erweiterung KeyUsage enthalten, so wird diese überprüft. Folgende KeyUsage-Bits werden akzeptiert:

- Digitale Signatur
 - Key Encipherment (Schlüsseltransport, Schlüsselverwaltung)
 - Key Agreement (Schlüsselaustauschverfahren)
- Ist eines der Bits nicht gesetzt, wird die Verbindung abgebaut.

extendedKeyUsage

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der Secure Client, ob der definierte erweiterte Verwendungszweck die “SSL-Server-Authentisierung” ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.



Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D. h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck “SSL-Server-Authentisierung” beinhalten muss. Dies gilt auch bei einem Rückruf an den Client über VPN.

Ausnahme: Bei einem Rückruf des Servers an den Client nach einer Direkteinwahl ohne VPN aber mit PKI prüft der Server das Zertifikat des Clients auf die Erweiterung extendedKeyUsage. Ist diese vorhanden, muss der Verwendungszweck “SSL-Server-Authentisierung” beinhaltet sein, sonst wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

subjectKeyIdentifier / authorityKeyIdentifier

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann kein CA-Zertifikat gefunden werden, wird die Verbindung abgelehnt.

CDP (Certificate Distribution Point)

Im Certificate Distribution Point ist die URL für den Download einer CRL hinterlegt. Ist im eingehenden Zertifikat (des Servers) die Erweiterung CDP enthalten, wird nach dem Verbindungsaufbau zum Server die aktuelle CRL nach diesem Zertifikat durchsucht. Dabei prüft der Client zunächst, ob bereits die entsprechende CRL bereits im Installationsverzeichnis vorhanden ist. Ist dies nicht der Fall wird die CRL über die angegebene URL heruntergeladen und überprüft, vorausgesetzt eine Internet-Verbindung ist möglich. Stellt der Client fest, dass das eingehende Zertifikat ungültig ist, wird die Verbindung abgebaut. Die CRL, sofern noch nicht gespeichert, wird dabei unter dem Common-Name der CA im Installationsverzeichnis unter <CRLS> gespeichert.

Überprüfung von Sperrlisten

Der Secure Client kann auch Revocation-Lists auswerten. Folgende Listen werden unterstützt:

- Certificate Revocation List (CRL)
- Authority Revocation List (ARL)

Die CRLs bzw. ARLs müssen in die entsprechenden Unterverzeichnisse des Installationsverzeichnisses nach <CRLS> bzw. <ARLS> kopiert werden.

Zu jedem Aussteller-Zertifikat kann dem Secure Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Ist eine CRL vorhanden, so überprüft der Secure Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Gleiches gilt für eine ARL (Authority Revocation List).

Sind eingehende Zertifikate in den Listen von CRL oder ARL enthalten, wird die Verbindung nicht zugelassen. Sind CRLs oder ARLs nicht vorhanden findet keine diesbezügliche Überprüfung statt.

HTTP Proxy für CRL Download

In der Datei NCPPKI.CONF im Installationsverzeichnis kann in der Gruppe "HttpProxy" ein Proxy für den CRL Download über HTTP konfiguriert werden:

```
[HttpProxy]
#ProxyHost = xxx.xxx.xxx.xxx
#IP Adresse des Proxy Servers für CRL Download über
#HTTP ProxyPort = 80
#Port des Proxy Servers für CRL Download über
#HTTP ProxyUser = xyz
#Benutzername des Proxy Servers für CRL Download über
#HTTP ProxyPw = xxxx
#Passwort des Proxy Servers für CRL Download über HTTP
```

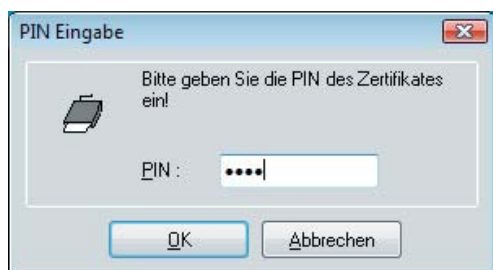
PIN-Eingabe



Die PIN-Eingabe kann über das Verbindungsmenü des Monitors (Abb. oben) vor einem Verbindungsaufbau erfolgen, nachdem der Monitor gestartet wurde. Wird zu einem späteren Zeitpunkt eine Verbindung aufgebaut, die ein Zertifikat erfordert, so kann dann die PIN-Eingabe unterbleiben – es sei denn, die Konfiguration zum Zertifikat verlangt es (siehe **PIN-Abfrage bei jedem Verbindungsaufbau**).

Wenn Sie den Secure Client zur Verwendung einer Smartcard konfiguriert haben, erscheint ein hellblaues Symbol für die Smartcard. Wenn Sie Ihre Smartcard in den Reader gesteckt haben, ändert sich die Farbe von hellblau zu grün (siehe **Client-Monitor**).

Sobald Sie die erste Verbindung aufbauen wollen, für die ein Zertifikat genutzt wird, wird ein Dialog zur PIN-Eingabe geöffnet – sofern Sie die PIN noch nicht vorher eingegeben haben (Abb. unten).



Wird ein Soft-Zertifikat verwendet, so kann die PIN 4-stellig sein. Wird eine Chipkarte verwendet, muss die PIN mindestens 6-stellig sein.



Fehlerhafte Eingaben und falsche PINs werden nach ca. 3 Sekunden mit einer Fehlermeldung quittiert. Ein Verbindungsaufbau ist dann nicht möglich. Nach dreimaliger fehlerhafter Eingabe der PIN, wird die PIN gesperrt! (Dies gilt nicht für Soft-Zertifikate). Wenden Sie sich in diesem Fall an Ihren Administrator.



Wenn die Chipkarte während des laufenden Betriebs entfernt wird, findet u. U. ein Verbindungsabbau statt (siehe oben Verbindungsabbau bei gezogener Chipkarte). (Gleiches gilt für Token auf einem USB Stick.)

Sicherung der PIN-Benutzung

Ist in der Zertifikatskonfiguration die Funktion "PIN-Abfrage bei jedem Verbindungsaufbau" aktiviert, wird der Menüpunkt "PIN eingeben" automatisch inaktiv geschaltet. Die PIN kann über den Monitor-Menüpunkt "PIN eingeben" somit nicht mehr eingegeben werden. Damit ist sichergestellt, dass erst unmittelbar vor dem Verbindungsaufbau die PIN abgefragt wird und eingegeben werden muss.

Bei Aktivierung dieser Funktion ist damit ausgeschlossen, dass ein unbefugter Benutzer bei bereits eingegebener PIN eine unerwünschte Verbindung aufbaut.

Ebenso wird für die Aktivschaltung der Funktion "PIN ändern" nicht mehr die bereits in anderem Funktionszusammenhang abgeforderte PIN verwendet, wie etwa beim Verbindungsaufbau oder im Verbindungsmenü "PIN eingeben". Sondern der Menüpunkt "PIN ändern" ist immer selektierbar, und die neue PIN wird unmittelbar nach der Änderung sogleich wieder zurückgesetzt.

Damit ist sichergestellt, dass bei Konfiguration der "PIN-Abfrage bei jedem Verbindungsaufbau" an einem unbeaufsichtigten Client-Monitor zu keinem Zeitpunkt eine bereits eingegebene PIN von einem unbefugten Benutzer für einen Verbindungsaufbau genutzt werden kann.

PIN zurücksetzen

Dieser Menüpunkt kann gewählt werden, um die PIN zu löschen, d.h. um die aktuell gültige PIN für einen anderen Benutzer unbrauchbar zu machen. Dies kann dann sinnvoll sein, wenn der Arbeitsplatz vorübergehend verlassen wird oder wenn der Benutzer gewechselt wird. Danach muss erneut eine gültige PIN eingegeben werden, um eine Authentisierung durchführen zu können.

PIN-Status im Client Monitor

Wurde die PIN bereits eingegeben, erscheint im Monitor die Einblendung "PIN" mit einem grünen Symbol. Wurde die PIN noch nicht korrekt eingegeben, ist das Symbol grau (Abb. unten).



PIN-Eingabebzwang nach Abmeldung oder Sleep-Mode

Wird unter den Betriebssystemen Windows NT/2000/XP der Benutzer gewechselt, wird der PIN-Status zurückgesetzt und die PIN muss erneut eingegeben werden. Wechselt der Computer in den Sleep-Modus, wird ebenfalls der PIN-Status zurückgesetzt.

Anzeige der Meldungen des ACE-Servers für RSA-Token

Werden vom ACE-Server auf Grund des RSA-Tokens Nachrichten versendet, werden diese am Monitor in einem Eingabefeld angezeigt (z. B. "Ablauf der gültigen PIN").

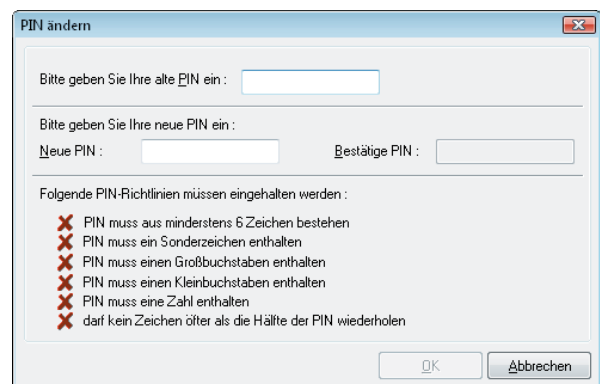
PIN ändern

Unter dem Menüpunkt "PIN ändern" kann die PIN für eine Smartcard oder ein Soft-Zertifikat geändert werden, wenn vorher die richtige PIN eingegeben wurde. Ohne die vorherige Eingabe einer gültigen PIN wird dieser Menüpunkt nicht aktiviert.

Aus Sicherheitsgründen (um die PIN-Änderung nur für den autorisierten Benutzer zuzulassen), muss nach Öffnen dieses Dialogs die noch gültige PIN ein zweites Mal eingegeben werden. Die Ziffern der PIN werden in diesem und den nächsten Eingabefeldern als Sterne "*" dargestellt.

Anschließend geben Sie Ihre neue PIN ein und bestätigen diese durch Wiederholung im letzten Eingabefeld. Mit Klick auf "OK" haben Sie Ihre PIN geändert. Die einzuhaltenden PIN-Richtlinien werden unter den Eingabefeldern eingeblendet. (Siehe auch oben **PIN-Richtlinien**).

Die Richtlinien können für ein Entrust-Profil vom Anwender nicht vorgegeben werden.



Einzuhaltende PIN-Richtlinien werden unter den Eingabefeldern eingeblendet und mit einem roten Kreuz markiert (Abb. oben). Während der Eingabe einer neuen PIN wird vor die jeweils erfüllten Richtlinien das rote Kreuz durch einen grünen Haken ausgetauscht.

PC-Sharing (Nutzung mehrerer Soft-Zertifikate an einem PC)

Soll ein PC-Sharing für mehrere Benutzer, die jeweils ein eigenes Zertifikat einsetzen, eingerichtet werden, so kann dazu eine Konfiguration vorgenommen werden.

Unter “Benutzer-Zertifikat” muss der Menüpunkt “Softzertifikatsauswahl aktivieren” eingeschaltet werden und ein “Zertifikatspfad” angegeben werden. Dieser Pfad kann über den Auswahl-Button gewählt werden, wenn er vorher angelegt wurde (z. B. INSTALDIR\usercert). Unter diesem Pfad müssen anschließend die verschiedenen Benutzer-Zertifikate abgelegt werden.

Werden diese Einstellungen mit “OK” gespeichert, so erscheint unter dem grafischen Feld des Monitors die Zertifikatsleiste mit der Liste aller unter dem Zertifikatspfad gespeicherten Benutzer-Zertifikaten (z. B. Client1 bis Client4).



Hat der Benutzer sein Soft-Zertifikat ausgewählt (z. B. Client2) und stellt eine Verbindung zum zentralen VPN Gateway her, so muss er zunächst seine PIN eingeben. Danach wird die Verbindung zum Zielsystem aufgebaut (Abb. oben).



Verlässt der Benutzer den Arbeitsplatz, so sollte er den Button mit “Abmelden” betätigen (Abb. oben). Dadurch wird die Verbindung vollständig abgebaut und die PIN zurück gesetzt. (Letzteres geschieht auch, wenn bei einer bestehenden Verbindung ein anderes Zertifikat ausgewählt wird). Findet keine Abmeldung statt, können nicht berechtigte Benutzer über die bestehende Verbindung Zugang zum VPN Gateway erhalten!

Ein nachfolgender Benutzer geht genauso vor. Zunächst wählt er sein Zertifikat aus, klickt anschließend die Funktion “Verbinden” und gibt seine PIN ein. Erst dann kann die Verbindung korrekt aufgebaut werden. Wird der Arbeitsplatz verlassen, klickt der Benutzer den Button mit “Abmelden”.



Erzeugung der Profile mit dem SEM und Konfigurations-Update

Zur Erzeugung der Profile (CNF-Dateien) für PC-Sharing mit dem Enterprise Management und einem Zertifikats-Update beachten Sie bitte das gleichnamige Dokument.

Bei einem Zertifikats-Update ist insbesondere darauf zu achten, dass die Zertifikate standardmäßig in das Installationsverzeichnis abgelegt werden. Haben Sie in der Zertifikats-Konfiguration des Clients ein anderes Verzeichnis definiert, so müssen die Benutzer-Zertifikate erst dorthin kopiert werden.

Accounting am VPN Gateway

Die Art des Accountings am VPN Gateway wird über die Profil-Einstellung des Clients definiert. Wichtig ist hier der Parameter "VPN-Benutzername" im Konfigurationsfeld "Tunnelparameter".

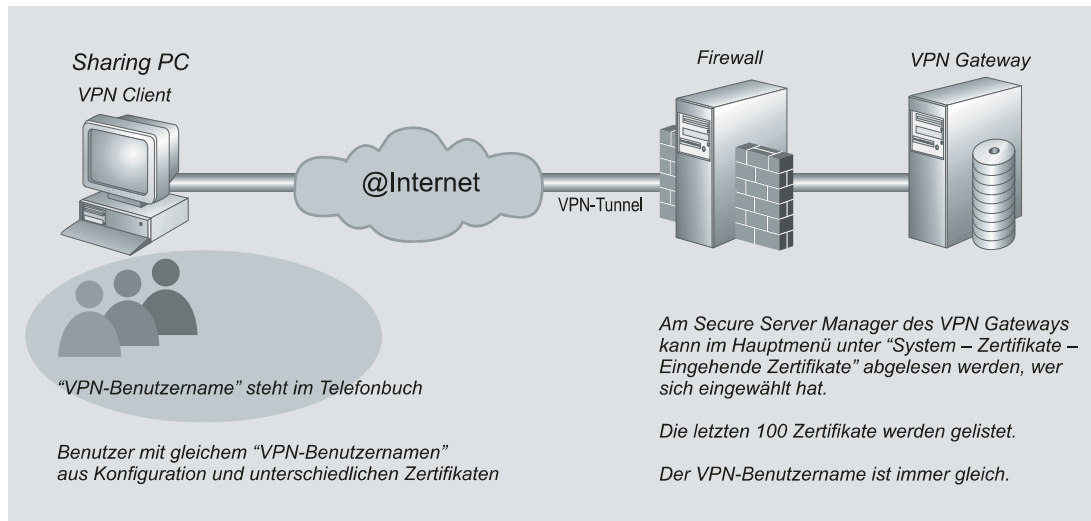


Abb. oben: Wird der "VPN-Benutzername" aus der Konfiguration gewählt (z. B. Sharing-PC1), so erfolgt das Accounting am VPN Gateway für alle Benutzer, die sich an dieses Zielsystem anwählen, unter dem gleichen Benutzernamen mit jeweils unterschiedlichen Zertifikaten. Am VPN Gateway muss dazu nur ein Link angelegt werden. Das zuletzt genutzte Zertifikat zum allgemeinen Benutzernamen für den Arbeitsplatz-PC kann am Server Manager unter "Eingehende Zertifikate" abgelesen werden.

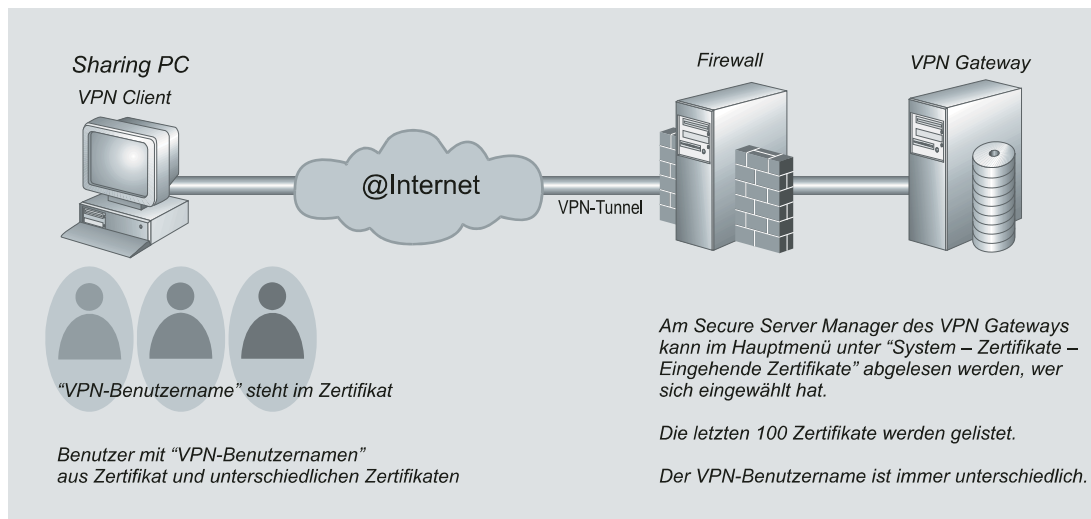


Abb. oben: Wird der "VPN-Benutzername" und das "VPN-Passwort" aus dem Soft-Zertifikat genutzt, so erfolgt ein personalisiertes Accounting am VPN Gateway, da sich mit jedem neu gewählten Zertifikat auch entsprechend "VPN-Benutzername und -Passwort" ändern. Um dieses Accounting nutzen zu können, muss am VPN Gateway für jeden Benutzer ein eigener Link angelegt werden.