NCP
SECURE COMMUNICATIONS

Installation und Konfiguration

high security remote access

Entrust Ready Funktionalität

Anhang zu
NCP Secure Client:

Entrust Ready Funktionalität

NCP
SECURE COMMUNICATIONS

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

Inhalt

1. 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. Damit unterstützt der NCP Secure Windows Client alle wichtigen Richtlinien von Entrust hinsichtlich des Zertifikatseinsatzes und deren Benutzung.

1.1 *Installierte Komponenten für die Entrust-Unterstützung*

Um die Entrust-Funktionalität in vollem Umfang nutzen zu können, wird folgendes vorausgesetzt:

☑ die Entrust-INI-Datei muss auf dem Benutzer-PC eingespielt sein

und folgende Komponente muss auf dem Benutzer-PC installiert sein:

☑ entweder der EntrustEntelligence Client mit dem EntrustIPSec Negotiator Toolkit

☑ oder das NCP Service Pack “Entrust Ready”

Sie haben dann die Entrust-Funktionalität erhalten mit:
Enterprise Client 7.22 ohne Service Pack.

1.2 *EntrustEntelligence Client mit dem EntrustIPSec Negotiator Toolkit*

Mit dem DesktopDesigner von Entrust kann der “EntrustEntelligence Client” für den Benutzer konfiguriert werden, der ihm Funktionalitäten wie die Anforderung eines Zertifikats-Profils, die Verlängerung oder die Wiederherstellung von Zertifikaten ermöglicht.

Entrust DesktopDesigner

Dazu ist es jedoch unbedingt erforderlich, dass der Administrator bei der Erstellung des EntrustEntelligence Clients im DesktopDesigner von Entrust sowohl

☑ Entrust/Entelligence

als auch

☑ EntrustIPSec Negotiator Toolkit

auswählt und außerdem

die Entrust-INI-Datei mitgibt. Die Entrust-INI-Datei erhält der Administrator von der CA, von der die Zertifikate angefordert werden sollen. (Die INI-Datei steht standardmäßig im Windows-Verzeichnis der installierten CA. Auf Seiten des Benutzers wird sie mit dem EntrustEntelligence Client installiert und im Windows-Verzeichnis eingespielt.)

Achten Sie darauf, dass die Option “Fips Mode” (amerk. Zertifizierungstandard für Software), sofern vorhanden in der INI-Datei auf “0" gestellt ist. Ändern Sie den Wert auf “0", wenn er ungleich ”0" gesetzt ist.

Der EntrustEntelligence Client wird vom Administrator an die Benutzer verteilt. Bei der Installation werden automatisch das IPSec Toolkit, die INI-Datei und Entrust-Bibliotheken eingerichtet.

Enterprise Client

Installieren Sie den Enterprise Client nach der Einrichtung des EntrustEntelligence Clients auf dem Benutzer-PC.

NCP Service Pack

Nach der Installation des Enterprise Clients kann das entsprechende NCP Service Pack (siehe oben 1.) installiert werden.

1.3 *NCP Service Pack “Entrust Ready”*

Anstatt des EntrustEntelligence Clients kann auch das NCP Service Pack “Entrust Ready” auf dem Benutzer-PC eingespielt werden.

Dannach muss die Datei ENTRUST.INI eingespielt werden. Der Benutzer erhält die Datei vom Administrator und muss sie in das Systemverzeichnis einspielen. In der INI-Datei sind die Vorgaben zur Anwahl an die Entrust CA abgelegt. Mit Hilfe dieser Datei wird das Laden des Entrust Profils und das Zertifikats-Management weitgehend automatisiert.

Falls in der Datei ENTRUST.INI die Option “Fips Mode” vorhanden ist, wird deren Wert automatisch auf “0" gestellt.

Enterprise Client

Die Installation des Enterprise Clients kann nach dem Einspielen der INI-Datei auf dem Benutzer-PC erfolgen.

NCP Service Pack

Nach der Installation des Enterprise Clients kann das entsprechende NCP Service Pack (siehe oben 1.) installiert werden.

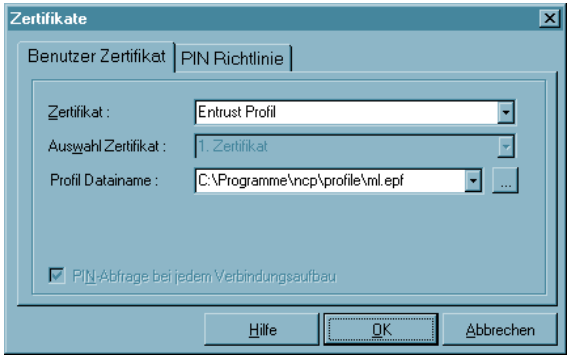
2. Lade Entrust Profil

Steht die Entrust Ready-Funktionalität zur Verfügung, so ist dies an der Oberfläche des Clients bei der Bedienung zu erkennen. Die Menüpunkte “Lade Entrust Profil” und “Zertifikate – Benutzer-Zertifikate – Entrust Profil” unter dem Hauptmenüpunkt “Konfiguration” in der Monitor-Oberfläche sind sichtbar.

2.1 *Zertifikate – Benutzer-Zertifikat – Entrust Profil*

Unter diesem Menüpunkt wird eingestellt, ob für dieses Zielsystem ein Entrust Profil genutzt wird.

Wählen Sie hier unter der Rubrik “Zertifikat” das “Entrust Profil”, wenn dies der Fall ist.



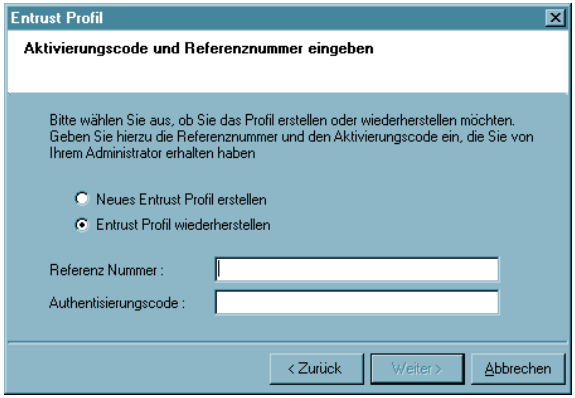
Die Angabe eines Profil-Dateinamens ist nicht nötig, da dieser nochmals vom Assistenten verlangt wird, nachdem der Menüpunkt “Lade Entrust Profil” gewählt wurde. Dieser Name wird dann automatisch nach dem Herunterladen des Profiles eingetragen. (Ggf. kann an dieser Stelle zwischen dem Profil von einer 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.

2.2 *Lade Entrust Profil*

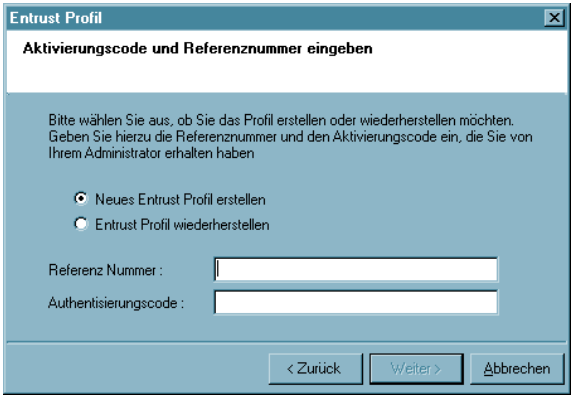
Mit diesem Menüpunkt wird ein Assistent gestartet, über den ein Profil geladen oder wieder hergestellt wird. Die VPN-Verbindung zur Entrust CA wird nach den Vorgaben der Datei ENTRUST.INI und der obigen Einstellung “Entrust Profil” im Hintergrund automatisch aufgebaut. Beachten Sie, dass eine VPN-Verbindung zum Firmennetz besteht.

Entrust Profil wieder herstellen:



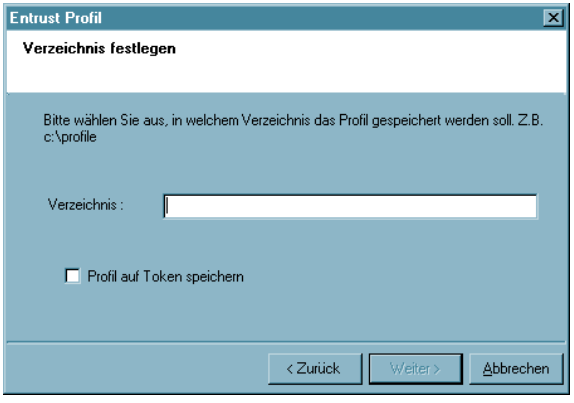
Wurde z.B. das Profil versehentlich gelöscht, so kann beim Administrator ein Ersatz angefordert werden. Nach einer Mitteilung an den Administrator über den Verlust des Profils erhält der Benutzer per PIN-Brief von dort eine neue Referenznummer und einen neuen Authentisierungscode. Soll das Profil wieder hergestellt werden, wird die entsprechende Funktion selektiert und anschließend neue Referenznummer und neuer Authentisierungscode eingegeben. Das dann erfolgende erneute Herunterladen bzw. das Wiederherstellen erfolgt genauso wie unter “Neues Entrust Profil erstellen” beschrieben. (Das neue Profil ist in diesem Fall identisch mit dem alten, verloren gegangenen.)

Neues Entrust Profil erstellen:



Nachdem der Benutzer den PIN-Brief mit Referenznummer und Authentisierungscode erhalten hat und als gewünschtes Benutzer-Zertifikat “Entrust Profil” eingestellt hat (siehe oben), kann der Menüpunkt “Lade Entrust Profil” selektiert werden.

Im ersten Fenster des Assistenten selektieren Sie die Funktion “Neues Entrust Profil laden” (Bild links) und geben einmalige Referenznummer und Authentisierungscode ein. (Groß- und Kleinschreibung ist bei dieser Eingabe nicht von Bedeutung.) Danach klicken Sie den Weiter-Button.



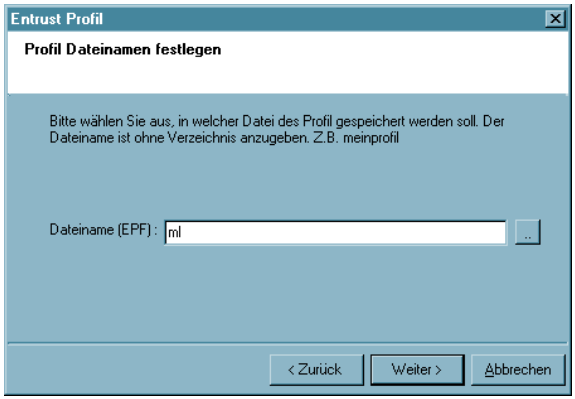
Im folgenden Fenster geben Sie das Verzeichnis an, wo das Profil gespeichert werden soll. Dieses Verzeichnis muss auch dann angegeben werden, wenn das Profil alternativ auf einen Token geschrieben werden soll.

Wichtig: Dieses Verzeichnis muss bereits angelegt worden sein. Das Windows-Verzeichnis kann mit Hilfe des Platzhalters “%SYSTEMROOT%” angeben werden

(z.B. c:\%SYSTEMROOT%\ncple\profiles).

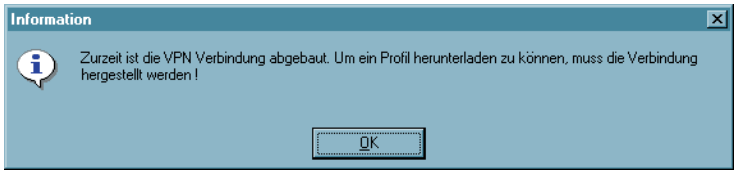
Um das Profil auf einem Token zu speichern, muss zusätzlich die Funktion “Profil auf Token speichern” aktiviert werden.

Klicken Sie anschließend auf “Weiter”.



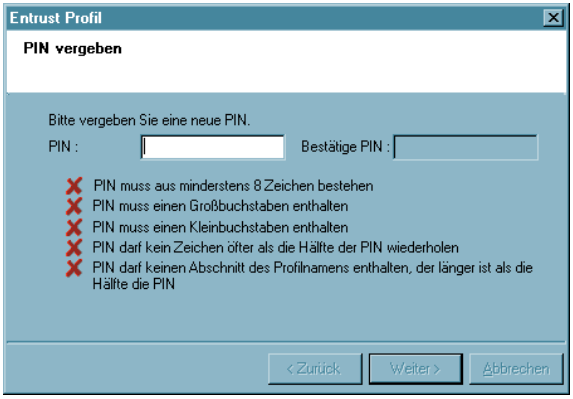
Im darauf geöffneten Fenster können Sie einen beliebigen Namen ohne Dateiendung für das Profil angeben. Die Dateiendung wird automatisch angehängt – EPF für ein Profil auf Festplatte, TKN für ein Profil auf Token. Klicken Sie anschließend auf “Weiter”.

Wichtig: Spätestens zu diesem Zeitpunkt benötigen Sie eine Verbindung zum VPN Gateway, hinter dem sich die Entrust CA befindet, um das Profil herunterladen zu können. Besteht diese Verbindung zu diesem Zeitpunkt nicht, erscheint untenstehende Meldung.



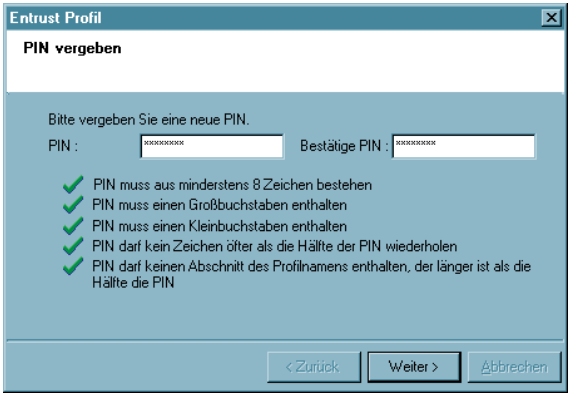
Die VPN-Verbindung kann im Hintergrund hergestellt werden.

Bei bestehender Verbindung wird das Profil heruntergeladen.



Um es nutzen zu können, geben Sie nun eine PIN ein, die die dazu aufgeblendeten PIN-Richtlinien erfüllt.

Diese PIN muss bei jeder Verwendung des Entrust Profils eingegeben werden! Die Richtlinien sind vom Administrator vorgegeben und können nicht geändert werden.



Die bei Eingabe jeweils erfüllte Richtlinie wird grün abgehakt. Ist die PIN komplett eingegeben und bestätigt worden, können Sie auf “Weiter” klicken.

Das Profil wurde nun erstellt und die Verbindung zum Firmennetz bzw. der Entrust CA kann wieder abgebaut werden.

2.3 *Anwahl an ein Zielsystem*

Wird nun ein Zielsystem angewählt, für das die Verwendung des Entrust Profils konfiguriert wurde, so muss die PIN genauso eingegeben werden, wie bei jedem anderen Zertifikat auch.

In der grafischen Oberfläche des Secure Clients wird dazu der PIN-Status angezeigt. Bei korrekt eingegebener PIN erscheint der Schriftzug “PIN” mit einem grünen Haken.

2.4 *Zertifikats-Management*

Die Zeitspanne für die Gültigkeit der PIN für das Entrust Profil (Zertifikat) wird vom Administrator nach Bedarf in der End User Policy der CA festgelegt. Diese und auch weitere PIN-Richtlinien, wie die Art der Festlegung der erlaubten alphanumerischen Zeichen, werden in der Konfiguration des Entrust-Profils in der Oberfläche des Secure Clients dargestellt, können dort aber nicht verändert werden.

Das Zerifikats-Management findet im Hintergrund statt. Es betrifft unter anderem Änderungen des Private Keys und der Zertifikats-Inhalte.

Bei jedem Verbindungsaufbau mit Zertifizierung durch ein Entrust Profil wird im Hintergrund kurzzeitig eine Verbindung zur Entrust CA aufgebaut und das Entrust Profil gegebenenfalls aktualisiert. In der grafischen Oberfläche des Clients erscheint dazu blinkend der Text “Entrust Profile Update”. Während dieser Aktualisierung kann die Verbindung von der Client-Seite aus nicht getrennt werden.

2.5 *Log-Einträge*

Im Log-Buch werden Meldungen bezüglich Entrust Ready eingetragen:

– Entrust Profil wurde erstellt

– Entrust Profil wurde aktualisiert

– Entrust-CA – Verbindungsaufbau

– Entrust-CA – Verbindungsabbau

– Fehlertexte von Entrust