



SECURE COMMUNICATIONS

The background of the slide features a stylized globe with thin grey outlines of continents. Overlaid on the globe are several curved lines representing orbital paths or data routes. Some of these lines have arrows at their ends, pointing in various directions, suggesting global connectivity and data flow. A dark blue vertical bar is positioned on the left side of the slide, containing the text 'Installation and Configuration' and 'high security remote access' in white.

# Installation and Configuration

high security remote access

## Entrust Ready Functionality

**Appendix**  
**NCP Secure Enterprise Client:**

**Entrust Ready Functionality**



Network  
Communications  
Products engineering GmbH

GERMANY  
Headquarters  
Dombühler Str.2  
D-90449 Nürnberg  
Tel.: +49-911-9968-0  
Fax: +49-911-9968-299  
internet [http:// www.ncp.de](http://www.ncp.de)  
E-mail: [info@ncp.de](mailto:info@ncp.de)



# Inhalt

- 1. Entrust Ready functionality . . . . . A61**
  - 1.1 Installed Components for Entrust Support . . . . . A61
  - 1.2 EntrustEntelligence Client with the EntrustIPSec Negotiator Toolkit . . A61
    - Entrust DesktopDesigner . . . . . A61
    - VPN/PKI Client . . . . . A62
    - NCP Service Pack . . . . . A62
  - 1.3 NCP Service Pack “Entrust Ready” . . . . . A62
    - VPN/PKI Secure Client . . . . . A62
    - NCP Service Pack . . . . . A62
  
- 2. Download Entrust Profile . . . . . A63**
  - 2.1 Certificates – User certificates – Entrust profile . . . . . A63
  - 2.2 Download Entrust Profile . . . . . A64
  - 2.3 Dial-in to a Destination System . . . . . A68
  - 2.4 Certificate Management . . . . . A68
  - 2.5 Log Entries . . . . . A68



# 1. Entrust Ready functionality

The NCP Entrust Ready certification has been granted for the NCP Secure Client versions 7.03 and version 7.22. Thus the NCP Secure Windows Client supports all the important guidelines from Entrust relative to the implementation of certificates and their use.

## 1.1 *Installed Components for Entrust Support*

The following are prerequisites for using the Entrust functionality to its full extent for NCP Secure Windows Clients:

- ☒ the Entrust INI file must be loaded on the user PC

and the following components must be installed on the PC:

- ☒ either the EntrustEntelligence Client with the EntrustIPSec Negotiator Toolkit
- ☒ or the NCP “Entrust Ready” Service Pack

According to your version of the Secure Client, you then have received the VPN/PKI Secure Client 7.22 without Service Pack.

## 1.2 *EntrustEntelligence Client with the EntrustIPSec Negotiator Toolkit*

The “EntrustEntelligence Client” can be configured for the user with the DeskTopDesigner from Entrust, which enables functionalities for the user such as the request of a certificate profile, or the extension or restoration of certificates.

### ***Entrust DesktopDesigner***

For this it is absolutely necessary that the administrator when creating the Entrust/Entelligence Client in the Entrust DeskTopDesigner has selected

- ☒ Entrust/Entelligence

as well as

- ☒ EntrustIPSec Negotiator Toolkit

and furthermore

supplies the Entrust INI file. The administrator receives the Entrust INI file from the CA, from whom the certificate will be requested. (The INI file as in the Windows directory of the installed CA as standard location. On the user side, it is installed with the EntrustEntelligence Client and loaded into the Windows directory.

Insure that the “Fips mode” (American certification standard for software), is set to “0” if present in the INI file. Change the value to “0” if it does not equal “0”.

The administrator distributes the EntrustEntelligence Client to the users. The IPsec Toolkit, the INI file and the Entrust libraries are set up automatically during the installation.

### ***VPN/PKI Client***

Install the VPN/PKI Client after setting up the EntrustEntelligence Clients on the user PC.

### ***NCP Service Pack***

The appropriate NCP Service Pack (see 1. above) can be installed after the installation of the VPN/PKI Client.

## **1.3 NCP Service Pack “Entrust Ready”**

The “Entrust Ready” NCP Service Pack can also be installed instead of the EntrustEntelligence Client.

Then the ENTRUST.INI file must be loaded. The user receives the file from the administrator and must load it into the system directory. The defaults for dialing into the Entrust CA are stored in the INI file. For the most part, loading the Entrust profile and the certificate management are automated with this file.

If the “Fips mode” option is present in the ENTRUST.INI file its value is set to “0” automatically.

### ***VPN/PKI Secure Client***

The VPN/PKI Secure Client installation can be executed after loading the INI file on the user PC.

### ***NCP Service Pack***

The appropriate NCP Service Pack (see 1. above) can be installed after the installation of the VPN/PKI Secure Client.

## 2. Download Entrust Profile

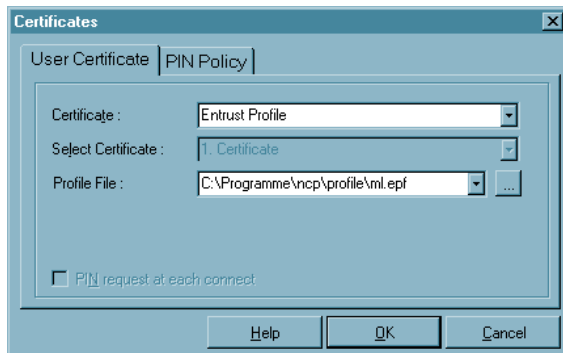
If the Entrust Ready functionality is available, then this can be seen on the NCP Secure Windows Client screen when operating. The “Download Entrust profile” and “Certificates – User Certificate – Entrust profile” menu items are visible under the main menu item “Configuration” in the monitor screen.

### 2.1 Certificates – User certificates – Entrust profile



Under this menu item you specify whether an Entrust profile will be used for this destination system.

If this is the case, then select the “Entrust profile” under the “Certificate” heading.

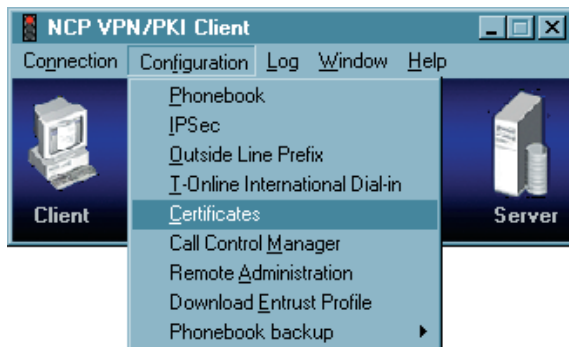


It is not necessary to enter the file name, as the assistant will request it again after the “Load Entrust profile” menu item has been selected. This name will then be entered automatically after downloading the profile. (If required you can select between the profile of a file on the hard disk (\*.EPF) or from the profile on a token (\*.TKN).

The “Load Entrust profile” is only selectable after the “Entrust profile” has been set.

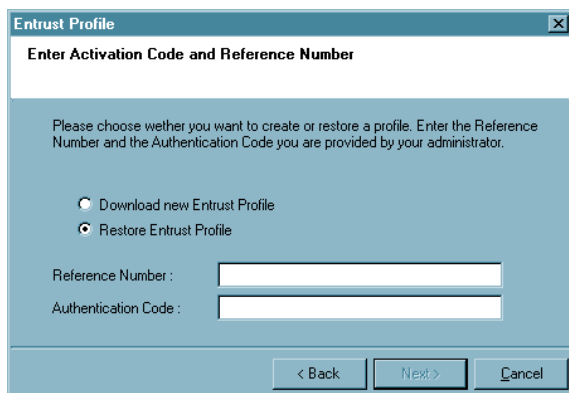


## 2.2 Download Entrust Profile



This menu item starts an assistant for loading or restoring a profile. The VPN connection to the Entrust CA is established in background according to the specifications of the ENTRUST.INI file and the above “Entrust profile”. Take notice, that there is a VPN- connection to the corporate network.

### Restore Entrust Profile:



If the profile has been deleted unintentionally, then the administrator can request a replacement. After communicating with the administrator about the loss of the profile, the user will receive the PIN letter, a new reference number, and a new authentication code from the administrator. If the profile must be restored, select the appropriate function and enter a new reference number and a new authentication code. The then renewed download or the restoration is executed exactly as described under “Create new Entrust profile”. (In this case, the new profile is identical to the old lost profile).

## Create Entrust Profile:

The screenshot shows a dialog box titled "Entrust Profile" with a close button (X) in the top right corner. The main heading is "Enter Activation Code and Reference Number". Below this, a message reads: "Please choose whether you want to create or restore a profile. Enter the Reference Number and the Authentication Code you are provided by your administrator." There are two radio buttons: "Download new Entrust Profile" (which is selected) and "Restore Entrust Profile". Below these are two text input fields: "Reference Number :" and "Authentication Code :". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

The menu item “Load Entrust profile” can be selected after the user has received the PIN letter with reference number and authentication code, and has set “Entrust profile” as the desired certificate (see above).

Select the “Download new Entrust Profile” in the first window of the assistant (illustration left) and enter a unique reference number and authentication code. (Upper and lower case characters have no significance for this entry.) Afterwards click on the “Next” button.

The screenshot shows a dialog box titled "Entrust Profile" with a close button (X) in the top right corner. The main heading is "Specify directory". Below this, a message reads: "Select a directory for the profile to be saved, e.g. c:\profile". There is a text input field labeled "Directory :". Below this is a checkbox labeled "Save profile on Token". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

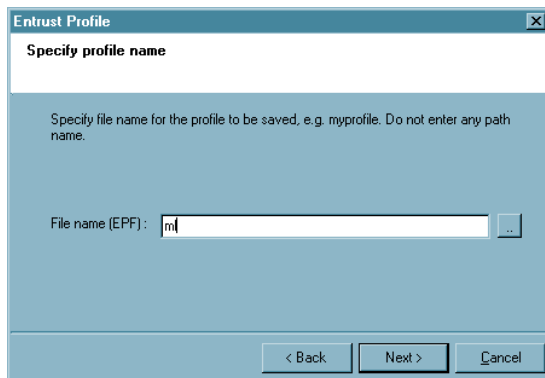
In the following window enter the directory where the profile is to be stored. This directory must also be entered if the profile is to be written on a token as an alternative.

Important: This directory must have been previously created. The Windows directory can be specified using the

(e.g. c:\%SYSTEMROOT%\install  
"%SYSTEMROOT%" placeholder

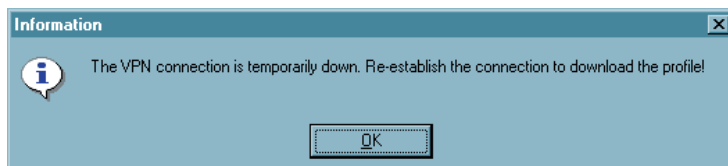
The “Save profile on token” function must be active in order to save the profile on a token.

Then click on “Next”.

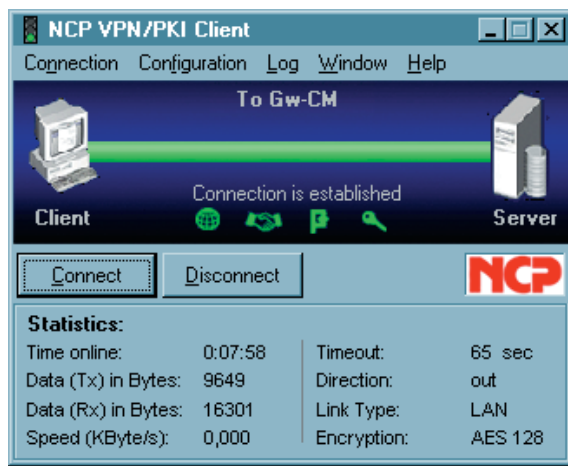


You can enter any name without file ending for the profile in the window that then opens. The file ending is appended automatically – EPF for a profile on the hard disk, TKN for a profile on the token. Then click on “Next”.

Important: By this point at the latest you will require a connection to the VPN gateway, behind which the Entrust CA is located, in order to download the profile. If this connection does not yet exist you get see the following information.



The VPN connection can be created in the background.



If the connection exists, then the profile will be downloaded.

**Entrust Profile**

**Specify PIN**

Enter new PIN.

PIN :  Confirm PIN :

- ✗ PIN must have a minimum of 8 characters
- ✗ No character must be repeated more often than half the characters of PIN
- ✗ must not contain a portion of profile name longer than half its length

< Back   Next >   Cancel

Now enter a PIN that satisfies the displayed PIN guidelines in order to use it.

This PIN must be entered for each use of the Entrust profile! The guidelines are specified by the administrator and cannot be changed.

**Entrust Profile**

**Specify PIN**

Enter new PIN.

PIN :  Confirm PIN :

- ✓ PIN must have a minimum of 8 characters
- ✓ No character must be repeated more often than half the characters of PIN
- ✓ must not contain a portion of profile name longer than half its length

< Back   Next >   Cancel

Each of the guidelines satisfied by the entry will be checked-off in green. If the PIN has been entered completely and has been confirmed, then you can click on “Next”.

The profile has now been created and the connection to the corporate network or the Entrust CA can be dismantled.

### **2.3 Dial-in to a Destination System**

Now if a destination system is selected, for which the use of the Entrust profile has been configured, then the PIN must be entered exactly as it is for any other certificate.

The PIN status is displayed in the graphic interface of the Secure Client. A green “PIN” indicates that the PIN has been entered correctly.

### **2.4 Certificate Management**

This PIN validity period for the Entrust profile (certificate) is specified by the administrator in the End User Policy of the CA, as needed. This and other PIN guidelines, such as the type of specification of the permitted alphanumeric characters, are displayed in the Entrust profile configuration in the Secure Client screen however they cannot be modified there.

The certificate management is executed in the background. Certificate management concerns changes to the private key and the certificate contents among other things.

A connection to the Entrust CA is briefly established and the Entrust profile is updated each time, for each connection establishment, with certification through an Entrust profile. The blinking text “Entrust profile update” appears in the graphic client screen for this. The connection cannot be disconnected during this update from the client side.

### **2.5 Log Entries**

The following messages relative to Entrust Ready are entered in the logbook:

- Entrust profile has been created
- Entrust profile has been updated
- Entrust-CA – connection establishment
- Entrust-CA – connection disconnect
- Entrust error texts