NCP

SECURE COMMUNICATIONS

Secure Entry CE Client

NCP

SECURE COMMUNICATIONS

Secure Entry CE Client

Version 2.33
July 2007

Disclaimer

Considerable care has been taken in the preparation and publication of this manual, errors in content, typographical or otherwise may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP as desired.
NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or use for any particular purpose. Furthermore NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes.

Copyright

Trademarks

Network
Communications
Products engineering GmbH

GERMANY
Headquarters:
Dombühler Straße 2
D-90449 Nürnberg
Tel.:+49-911-99680
Fax: +49 - 911 - 9968 299
Internet http://www.ncp.de
E-mail: info@ncp.de

Support

NCP offers support for all international users by means of Fax and Internet Mail.

Fax Hotline Number

+49 911 99 68 458

Internet Mail Address

support@ncp.de

When contacting NCP with your problems or queries please include the following information:
– exact product name
– serial number
– Version number
– Accurate description of your problem
– Any error message(s)

NCP will do its best to respond as soon as possible, but we do not guarantee a fixed response period.

Contents

1. Overview

This manual describes Installation, Configuration, Features and User Interface of the NCP Secure Communication Components

- **NCP Secure Entry CE Client**
- **NCP Secure Entry CE Client Configurator**

The NCP Secure Client Software works according to the principle of Ethernet LAN emulation and supports the routable protocol TCP/IP.

Additional information on upgrades and product variants are available on the NCP website: http://www.ncp.de

1.1 Using this manual

The structure of this manual is presented below to help you quickly find what you need in this documentation.

The manual is subdivided into six larger sections that offer step-by-step descriptions, or that describe the structure of the graphic user interface according to the respective object. Two appendices providing additional information and definitions of specialized terms follow these sections.

1. Product overview with brief description of the performance range of the software
2. Installation instructions
3. Description of the graphic user interface
4. Description of the configuration possibilities
5. Description of the parameters listed in the configurator
6. Description of a connection establishment
7. Examples and explanations, particularly for IPsec

– Appendices with a glossary (abbreviations and terms) and an index

Cross references appear in the text in parenthesis and cite the reference with the title, or after a comma, with the subtitle. An exclamation mark in the margin indicates that the text so marked is of particular significance.

Naturally the software also offers context-sensitive help.

1.2 NCP Secure Entry Client – universal IPsec client

The NCP Secure Entry Client can be used in any VPN environment. The client communicates on the basis of the IPsec standard (see → Examples and explanations, Security, IPsec) with the gateways provided by a wide variety of vendors* and is the alternative to the uniform IPsec client technology offered on the market. The Secure Entry Client has additional features that introduce the user into a holistic remote access VPN solution.

The NCP Secure Entry Client offers:

☑ Support of all major operating systems

☑ Dial-in over all transmission networks

☑ Compatibility with VPN gateways from a wide variety of vendors*

☑ Integrated personal firewall for more security

☑ Dialer protection (no misuse by third parties)

☑ Convenient operation (graphic interface)

☑ Central management**

**) Compatibility list available on the NCP website www.ncp.de*
***) optional*

1.3 Performance range

The NCP Secure Entry Client supports all major operating systems (Windows 98se, ME, NT, 2000, XP, Windows CE, and Linux). Dial-in to the corporate network is media-type independent (see → Configuration parameters, Telephone book, Destination system), e.g. when using the Secure Entry CE Client in addition to PSTN analog telephone network, GSM, GPRS also LAN technologies such as WLAN (on the corporate campus and hotspots) or local area networks (branch office network) are supported.

A possible scenario: an employee must access the corporate network from various locations with one and the same end device:

– in the branch office via WLAN
– in the corporate headquarters via LAN
– on the road at hotspots and at customer sites via WLAN or GPRS

1.3.1 Client Monitor – graphic user interface

The graphic user interface of the Secure Entry Client provides transparency during the dial-in process and data transfer. Among other things it provides information on:

– actual data throughput,
– time remaining until the next timeout (Short Hold Mode),
– connection direction (outgoing or incoming)

The user knows whether his PC is online at all times, and in the end where the charges are incurred.

1.3.2 NCP Dialer

The system’s own dialer replaces the otherwise usual Microsoft Dialer. This offers advantages in several areas:

– intelligent line management (Short Hold Mode) in dial-up networks
– integrated personal firewall mechanism
– protection against “automatic dialers”

1.3.3 Line Management

In order to guarantee fast and cost effective data communications, active connections are automatically disconnected, if there is no data flow. If new communication data arrive, the suspended connection will be activated without intervention of the user. Communication costs only occur during data flow.

1.3.4 Personal Firewall

The NCP Secure Entry Client provides all personal firewall functionalities to fully secure the PC workstation against attacks from the Internet, a wireless LAN, or the local network. The integrated NCP dialer protects the PC against ISP kidnapping (redirecting calls).

This shield consists of IP-NAT (Network Address Translation) and various IP-protocol filters. NAT is a security standard that prevents exposing the internal private IP address to the Inter-net by translating it to a legal or public IP address, thus enabling the host (e.g. user PC) to communicate safely across the Internet. Incoming packets are checked for precisely defined properties (address and protocol) in ac-cordance with a sophisticated filter, which rejects any non-conform packets. Source ports are also screened to prevent any masquerading. This means: The Internet port of the respective computer is thoroughly protected, and the building of any unwanted links is prevented.

1.3.5 PKI Support

Strong authentication through digital certificates as soft certificates (PKCS#12) or on smart cards (PKCS#11, CT-API, PC/SC) increases the security for the PC as well as the corporate network. The NCP Secure Entry Client becomes part of a Public Key Infrastructure (PKI).

Public-Key Infrastructure

PKI consists of a combination of standards, products, guidelines, and procedures. As such it provides the basic security platform for eCommerce business transactions, so those users (un)known to each other can safely com-municate. PKI is a globally recognized and applied technology for security.

PKI includes the use of digital certificates that act as personal “electronic ID’s” and are issued by a Certificate Authority (CA) or Trust Center. Security experts and the IETF (Internet Engineering Task Force) have concluded that an effective protection against man-in-the-middle attacks can only be achieved by using Smart Cards with certificates.

Thus, a trust relationship, as we know it in the traditional world of paper-based business, can also be established in the world of global electronic information exchange. A digital signature in combination with data encryption is the electronic equivalent to a written signature and proves the validity and origin of messages in a similarly secure manner.

Smart Card

Smart Cards are the ideal enhancement for high security Remote Access solutions. They provide two-fold security for Log-in purposes, which includes the PIN (Personal Identification Number) as well as the actual possession of the Smart Card itself. The User identifies himself as the Smart Card’s rightful owner by entering its assigned PIN (Strong Security). The PIN substitutes the entering of Password and User-ID (basis for Single-Sign-On). The User identifies himself only to the Smart Card. The validation against the network is negotiated between the Smart Card and the corresponding Security (Authentication) system. All security related processes are executed inside the card, thus not in the PC. Smart Cards also provide the technological basis for multi-functional applications, e.g. Company Card, etc.. Biometric processes can also be integrated.

1.4 Optional extensions

1.4.1 Administration

Optional high-performance tools are available for administration of the remote PC workstations (Secure Client Manager, Secure Update Server, Secure PKI Manager). These offer all functionalities necessary for establishing and operating a professional remote access VPN.

Essentially these involve rollout and operation.

Rollout:
– creating the user configurations
– initialization with first dial-in
– issuing and distributing certificates

Operation:
– User administration
– software updates
– certificate management
– remote help desk (remote control)

1.4.2 NCP Secure High Availability Services

High Availability Services, consisting of the Secure Failsafe Server and Load Balancing Server ensure failsafe security and uniform load distribution of multiple NCP Secure VPN Gateways. While the Secure Failsafe Server offers backup functionality for a VPN Gateway, the Load Balancing Server distributes the VPN connections (tunnels) uniformly over all available NCP Secure VPN systems.

2. Installation

The installation of the Secure Entry CE Client software is conveniently carried out via setup for all Windows systems. The installation procedure is identical for all versions of the Secure Client.

Before you install the software, the installation prerequisites must be fulfilled for full functionality, as described in the following chapter.

Also please be aware that the NCP Secure Entry CE Client software consists of two components that must be installed separately.

■ PC component

The PC component has the NCP Secure Entry CE Client Configurator for creating the profile settings. From this Configurator, the profile is copied onto the PDA via Active-Sync.

■ PDA component

The PDA component consists of the NCP Secure CE Client Service that analyses the data for the modem, (or mobile phone), or a LAN adapter and the chip card reader, and the NCP Secure CE Client Configurator (NCP Client Configurator) for selection of the destination system and the connection establishment to the destination system.

Sequence from installation to starting operation

Please follow the sequence!

☑ Installation of the PC component

☑ Installation of the chip card reader on the PDA (if Smart Cards are implemented)

☑ Installation of the PDA component

☑ Start the NCP Client Service on the PDA (if the Strong Security version is implemented)

☑ Configuration of the destination system on the PC

☑ Transfer of the telephone book (and the certificate for the Strong Security version)

☑ Starting operation on the PDA

2.1 Installation prerequisites

Operating system

The PC component of the Secure Entry CE Software can be installed on computers with the operating systems Microsoft Windows 98se, Windows NT (4.0) from Service Pack 5 on (6a is recommended), or Windows 2000 /XP. (Other operating systems on request.)

The Microsoft ActiveSynch program, 3.0 or higher, must have been previously installed on the PC. The PDA component is installed via this program and the data transfer between PDA and PC is effected via this program.

Local system

The dial-up to the destination system is handled via a PDA (Personal Digital Assistant) with Windows CE. Because the NCP dialer as well as the Microsoft RAS dialer can be used for dial-in, all marketable combinations of PDAs and mobile phones are supported. The prerequisites are appropriate CE compatible drivers.

■ Analogue modems and mobile phones

For communication via modem (or mobile phone), the modem must have been correctly recognized by Windows CE.

Drivers for modems that support the Hayes command set are integrated in Windows CE. Likewise Windows CE supports most mobile phones with IR interface or Bluetooth and built-in modem.

The modem data will be downloaded by the PDA when starting the PC component (see → Client Configurator, Configuration). Please insure that an ActiveSynch connection between PC and PDA exists at this point in time.

■ LAN adapter (LAN over IP)

In order to operate the client software with the connection type “LAN over IP” in a local area network, a LAN adapter (Ethernet or Wireless LAN) must be installed on the PDA.

Prerequisites for the Strong Security Version

If you use the VPN/PKI/ CE Client software (Strong Security version of the client), that supports certification (X.509), then either a chip card reader must be connected to the PDA or a soft certificate must be loaded on it.

■ Chip Card reader (PC/SC conformant)

The client software automatically supports all chip card readers that are PC/SC conformant. These chip card readers will only be listed after the reader is connected and the associated driver software has been loaded. When starting the “NCP Client Service” on the PDA, the chip card reader is searched in the system. Consequently it is absolutely necessary that the card reader be installed and connected at this point in time!

Certificate configuration

Please note: Before you undertake a certificate configuration with the PC component of the Client (see → Client Configurator of the PC component, configuration, certificates), the information about available chip card readers must have been transferred from the PDA to the PC. Because the NCP Client Service creates these, the NCP Client Service must have been loaded before starting the PC component. An existing ActiveSynch connection is required to transfer this data.

■ Chip cards (Smart Cards)

The Strong Security version of the client supports chip cards from Signtrust, NetKey 2000 and TC Trust (CardOS M4). NCP continuously strives to support the new chip card readers and chip cards. Refer to the NCP website to check the most current list of supported products.

■ Chipcard or Token (PKCS#11)

The PKCS#11 Modules of other manufacturers are supported by their driver librairy (DLL).

■ Soft certificates (PKCS#12 file)

Instead of reading out the certificate of a Smart Card via a chip card reader, a soft certificate (PKCS#12 file) can also be used.

Certificate configuration

Please note: Path and name of the PKCS#12 file required for the configuration (see → Client Configurator of the PC component, configuration, certificates) must agree with the location of the file on the PDA!

The menu item “Configuration – transfer PKCS#12 file to the PDA” in the Configurator of the PC component can be used for transferring the PKCS#12 file. If this function is used, then the path can be specified as follows:

```
%INSTALLDIR%\certs\<PKCS#12-file name>
```

2.2 Installation of the PC component

There is no difference in the software installation procedure used under the operating systems Windows 2000/XP or Vista. However please note whether you are installing from the hard disk, from the CD, or from the diskette. If you have already installed an older version of the software then please see the chapter “Update and Uninstall”. For installing the software and using the PC componente (Configurator) under Windows Vista you need administrator rights.

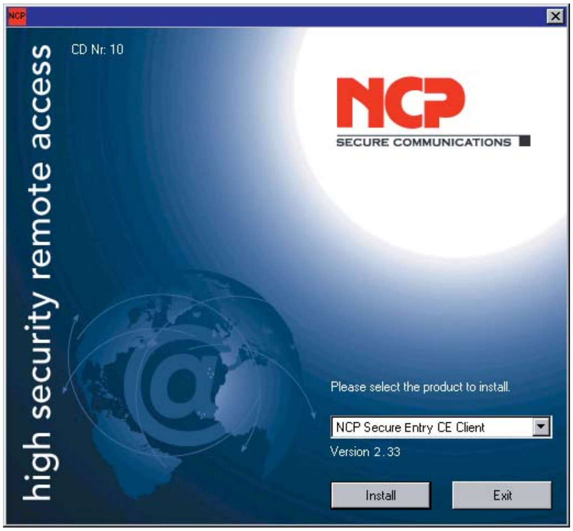
Installation and Licensing

First the NCP Secure Entry Client is installed as a test version. If you posess a license, you can enter the license data after a reboot of the software by selecting the monitor menu option “License Info and Activation”. The test version is valid for 30 days. Without software activation or licensing it will no longer be possible to setup a connection after this 30-day period expires. When 10-days validity remain, a message box will be displayed to remind you that the software has not yet been licensed. For licensing the software please refer to the chapter “Licensing” in the handbook.

Installation from the Hard Disk

If you would like to install the software after a download from the NCP FTP server, then unpack the ZIP file first. The directories “DISK1”, “DISK2”, “DISK3” will automatically be created while unpacking. If the request message “Install program from diskette or CD” appears when starting the installation, then click “Next” and afterwards click “Browse” in order to select SETUP.EXE in the “DISK1” directory. All further installation procedures are identical to those described in the section “Installation from diskette”.

Installation from CD


CD Nr: 10

Please select the product to install.

NCP Secure Entry CE Client

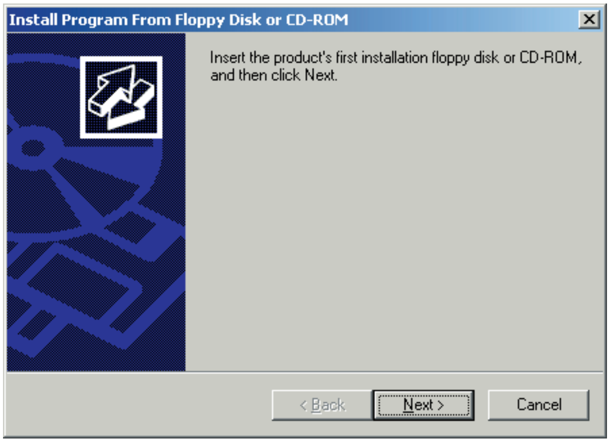
Version 2.33

After you have inserted the CD in the drive of your computer, after a few seconds the NCP greeting screen automatically appears on your monitor (see graphic to the left).

Select which product you would like to install and then click on “Install”. The subsequent procedure is identical with the diskette installation from the point “Select the setup language”.

2.2.1 Default Installation

If you should get pre-configured installation diskettes from your system administrator, then please follow his installation instructions.


Install Program From Floppy Disk or CD-ROM

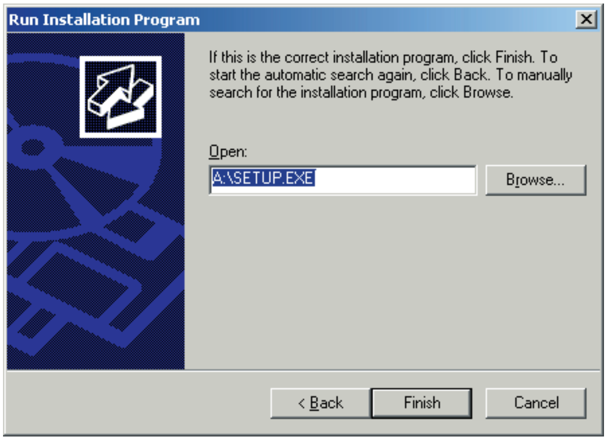
Insert the product's first installation floppy disk or CD-ROM, and then click Next.

The first installation step is to select “Start / Settings / Control Panel” in the main Windows menu.

Select “Add/Remove Programs" in the Control Panel.

Then click on the “Install...” button in the “Install/Uninstall” tab.

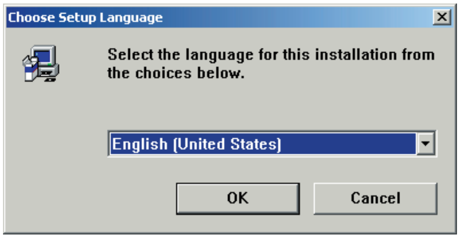
Now insert the first diskette with the client software in the drive of your computer (see the figure to the left), if you have not already done so, and click “Next...”


Run Installation Program

If this is the correct installation program, click Finish. To start the automatic search again, click Back. To manually search for the installation program, click Browse.

Open: A:\SETUP.EXE

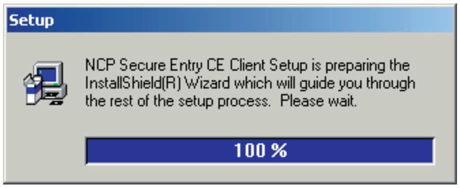
When “SETUP.EXE” is displayed, click on “Finish”.


Choose Setup Language

Select the language for this installation from the choices below.

English (United States)

In the next window you can select the setup language. Then click on “OK”.

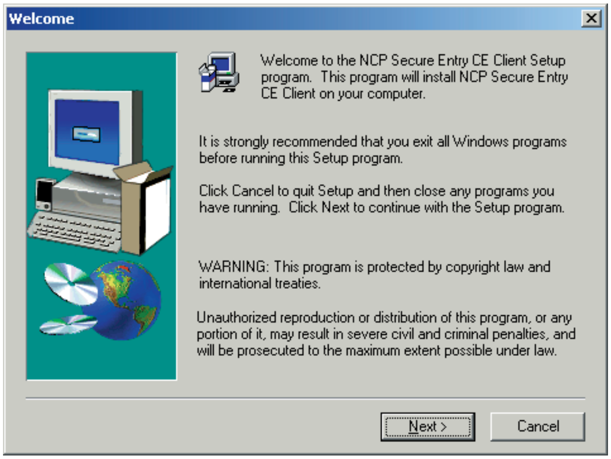

Setup

NCP Secure Entry CE Client Setup is preparing the InstallShield(R) Wizard which will guide you through the rest of the setup process. Please wait.

100 %

Then the setup program prepares the install shield assistant, with whose help the installation is continued.

→ *next page*



Welcome

Welcome to the NCP Secure Entry CE Client Setup program. This program will install NCP Secure Entry CE Client on your computer.

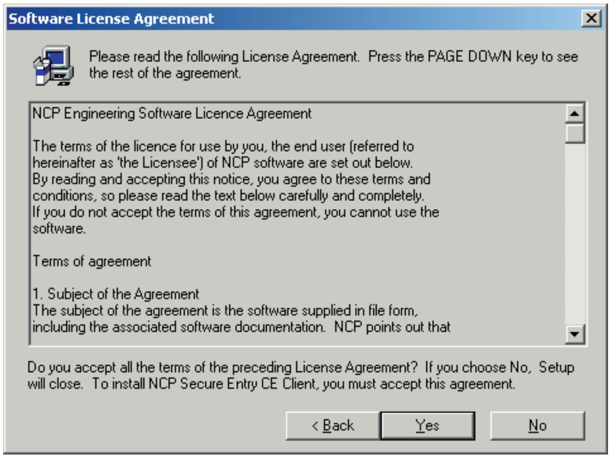
It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Please read the instructions in the welcome window of the setup program before you click on “Next”.



Software License Agreement

Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

NCP Engineering Software Licence Agreement

The terms of the licence for use by you, the end user (referred to hereinafter as 'the Licensee') of NCP software are set out below. By reading and accepting this notice, you agree to these terms and conditions, so please read the text below carefully and completely. If you do not accept the terms of this agreement, you cannot use the software.

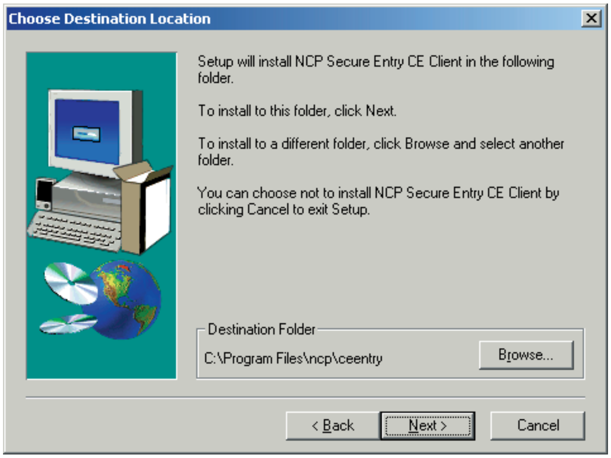
Terms of agreement

1. Subject of the Agreement
The subject of the agreement is the software supplied in file form, including the associated software documentation. NCP points out that

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install NCP Secure Entry CE Client, you must accept this agreement.

Then the licence conditions are displayed. If you agree with the contract, then select “Yes” otherwise the installation will be aborted.

(The licensing is done first on your PDA device.)



Choose Destination Location

Setup will install NCP Secure Entry CE Client in the following folder.

To install to this folder, click Next.

To install to a different folder, click Browse and select another folder.

You can choose not to install NCP Secure Entry CE Client by clicking Cancel to exit Setup.

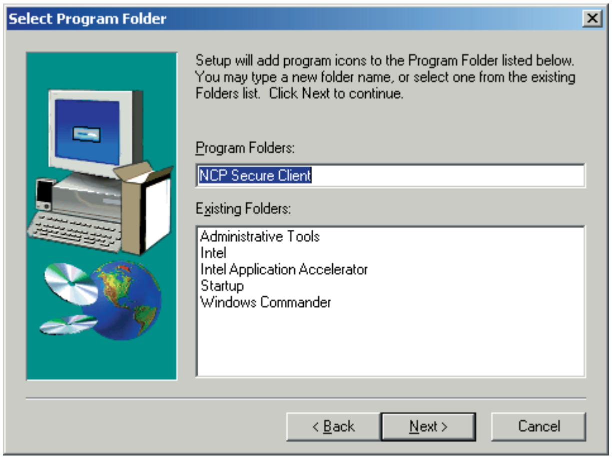
Destination Folder
C:\Program Files\ncp\ceentry

This is where you specify the destination directory for the client software.

(Standard is programs\ncp\ceclient).

→ *next page*

Otherwise you can specify the program folder.

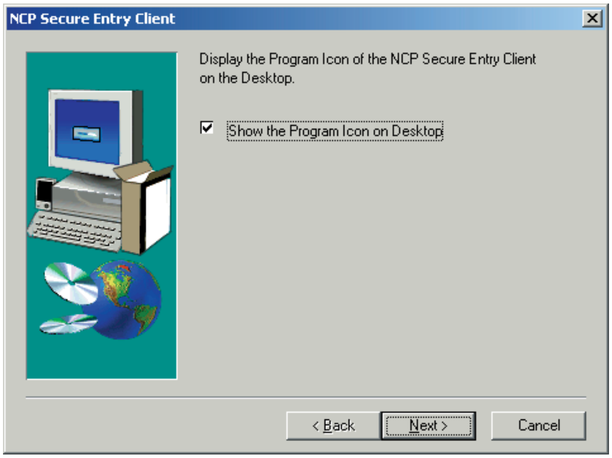

Select Program Folder

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.

Program Folders:
NCP Secure Client

Existing Folders:
Administrative Tools
Intel
Intel Application Accelerator
Startup
Windows Commander

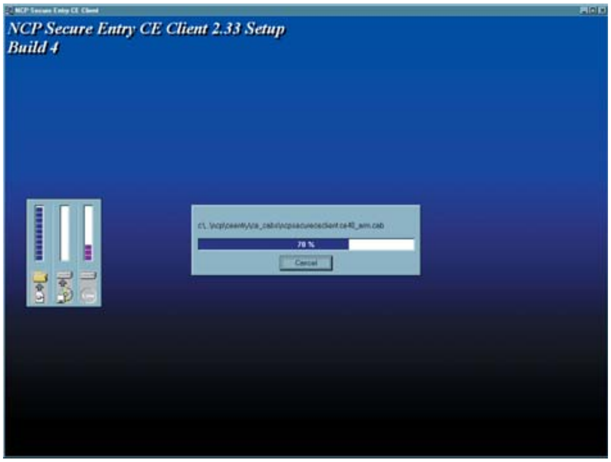
Moreover you can have the program icon displayed on the desktop.


NCP Secure Entry Client

Display the Program Icon of the NCP Secure Entry Client on the Desktop.

☑ Show the Program Icon on Desktop

Then the files are copied over.

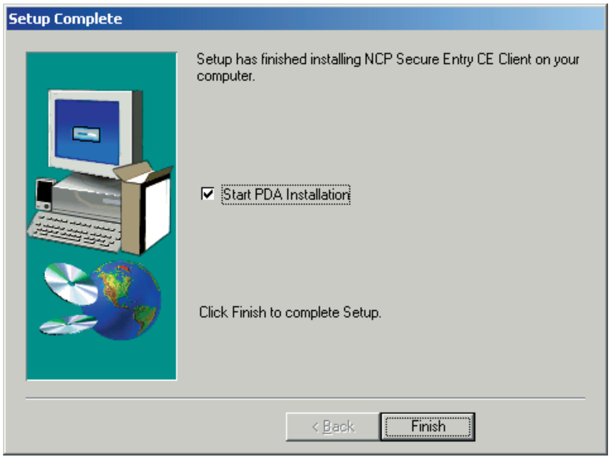

NCP Secure Entry CE Client 2.33 Setup
Build 4

c:\ \ncp\pcentry\ce_cab\ncpsecurececlient.ce40_arm.cab

70 %

(Follow the instructions on the screen and change the diskettes when you are requested to do so.)

→ *next page*



Setup Complete

Setup has finished installing NCP Secure Entry CE Client on your computer.

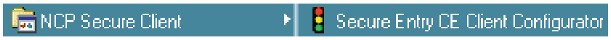
☑ Start PDA Installation

Click Finish to complete Setup.

After all required files have been copied over from the installation diskettes, and the program group has been created, click on “End” to conclude Setup.

Leaving the setting “Start PDA Installation”, the PDA component is automatically installed after finishing the installation of the PC component.
If you here swich off the automatically installation, you can install the PDA component later. For that see chapter

→ *2.6 Installation of the PDA component*

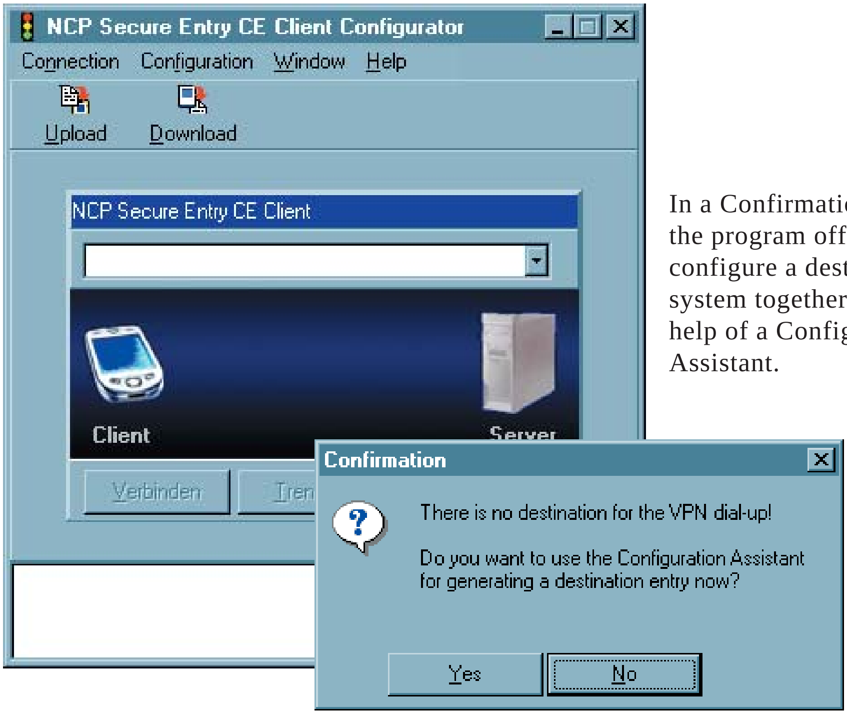


After installation you will find in the Windows start menu, in the program group “NCP Secure Client”, the program “Secure Entry CE Client Configurator”.

The configuration of the destination systems, the composition of the telephone book, and the transmission of the telephone book to the PDA (see → Client Configurator) are executed with this program Configurator.

2.2.2 Before Starting

After installing, the Client Monitor is displayed as shown in the picture below. To use the Secure Entry Client you first have to generate an entry in the phonebook, what means that you have to define a destination system to which an IPSec connection can be established.



There is no destination for the VPN dial-up!

Do you want to use the Configuration Assistant for generating a destination entry now?

In a Confirmation window the program offers to configure a destination system together with the help of a Configuration Assistant.

Click on “Yes” in the Confirmation window and refer the description under “3. Client Configurator” about the configuration and the profile settings.

For further configuration refer to “5. Profile Settings”.

Only if a destination system has been set in the profile settings, a connection to this destination can be made (see → 6. Establishing a Connection).

2.2.3 Transferring the Profiles and the Certificates

- **Profiles**

Before transferring the profiles, the profil setting for the destination system must first be configured and completed in the PC. See the sections “Client Configurator of the PC Component” and “Configuration Parameters” in this manual to do this.

If you are using the Strong Security version of the software with chip card reader, then please note the following: Before you undertake a certificate configuration with the PC component (see → Client Configurator, Configuration, Certificates), the information about available chip card readers must have been transferred from the PDA to the PC. Because the NCP Client Service creates these, the NCP Client Service must have been loaded before the starting the PC component. An existing ActiveSynch connection is required for transferring this data.

The transmission of the profiles is described in the section “Profile Settings Upload”.

- **Certificates**

The supplied test certificates from NCP, CA certificate (ncpsupportca.der) and user certificates (user1.p12 and user2.p12) are already located on the PC and the PDA after the installation of the two software components.

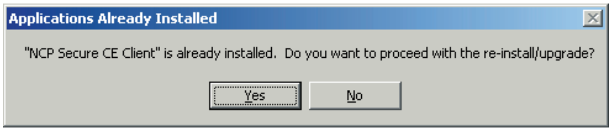
If you are using your own soft certificates, then these must be transferred from the PC via ActiveSync. In this case, insure that the PDA can only read CA certificates in the DER (Distinguished Encoding Rules) format with file endings DER, CER, or CRT! The PEM format is not supported.

The destination directory on the PDA for the CA certificate is:
`\Programs\NCP Secure CE Client\CaCerts`

The destination directory on the PDA for the user certificate is:
`\Programs\NCP Secure CE Client\Certs`

The transfer of the user certificate in its directory can be facilitated by selecting the menu item “Transfer PKCS#12-file to the PDA” in the PC component Configurator (see → Client Configurator of the PC component, configuration).

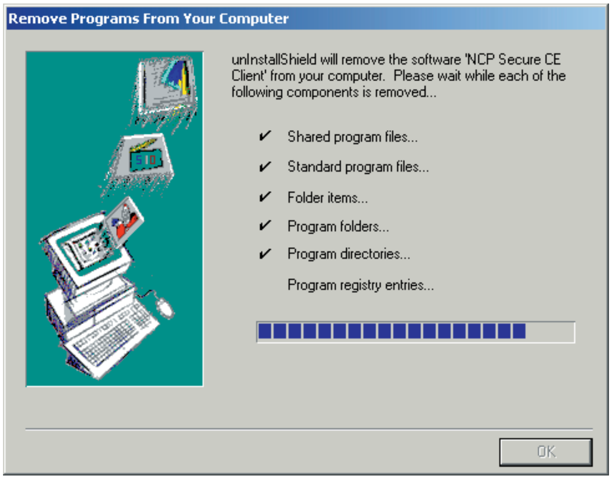
2.3 Update and Uninstalling the PC Component



Applications Already Installed

"NCP Secure CE Client" is already installed. Do you want to proceed with the re-install/upgrade?

If an older version of the client software is found, then it is possible to execute an update. The telephone book will be maintained in the configuration made earlier if you are updating.



Remove Programs From Your Computer

unInstallShield will remove the software 'NCP Secure CE Client' from your computer. Please wait while each of the following components is removed...

- ✓ Shared program files...
- ✓ Standard program files...
- ✓ Folder items...
- ✓ Program folders...
- ✓ Program directories...
- Program registry entries...

To remove the PC component, go to: “Start / Settings / Control panel”. Now click on “Add/Remove Programs” and select “NCP Secure CE Client” from the list. Then click on the “Add/Remove” button. The Uninstall Shield Program now deletes the Client software from your PC.

After the component have been removed, the client’s telephone book remains intact, so that it can be used for newer versions of the Secure CE client. In order to completely delete the file from your PC, you must proceed manually. The telephone book is located in the directory:

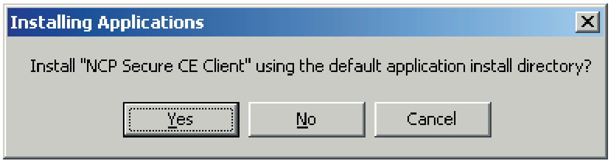
```
\programs\ncp\ceclient\bin\ncpphone.cfg
```

2.4 Installation of the PDA component

The installation of the PDA component will be triggered from the PC.

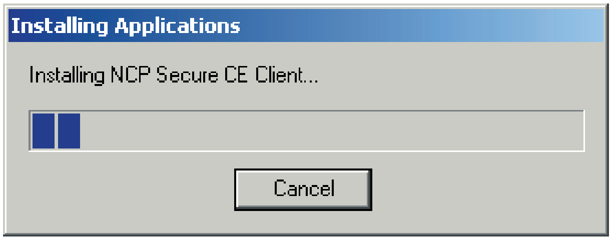
Activate the menu item “PDA installation” in the NCP Secure CE Client program group. Please insure that the “Software” dialog from ActiveSynch is not open when you execute the PDA installation program!

Now ActiveSynch has been requested to install the NCP Secure CE Client on the mobile device.



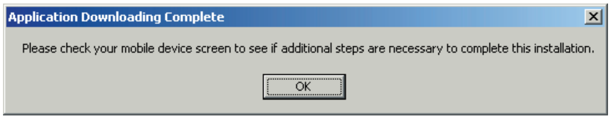
Install "NCP Secure CE Client" using the default application install directory?

Select the standard directory as the installation directory on the PDA. To do this click on “Yes” in the adjacent graphic.



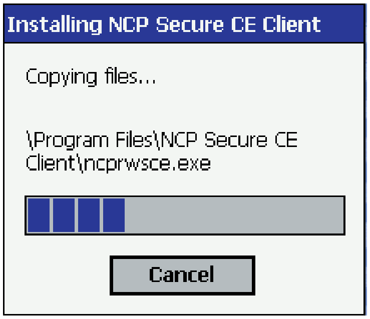
Installing NCP Secure CE Client...

Afterwards the data for the NCP Secure CE Client will be transmitted.



Please check your mobile device screen to see if additional steps are necessary to complete this installation.

After the data transmission has been concluded, check the screen of the mobile device:

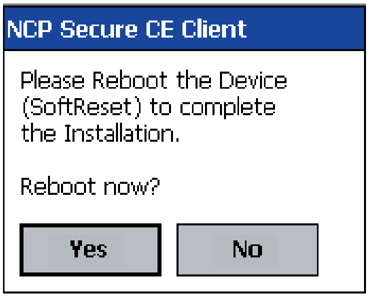


Copying files...

\Program Files\NCP Secure CE Client\ncprwsce.exe

On the PDA the installation is executed while unpacking the transferred data.

→ *next page*



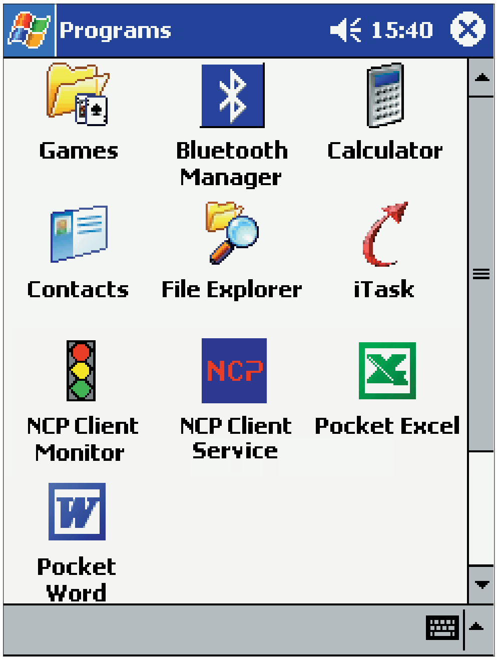
NCP Secure CE Client

Please Reboot the Device (SoftReset) to complete the Installation.

Reboot now?

After unpacking you will be requested by the PDA to do a soft reset.

This concludes the installation of the PDA component.



After the soft reset you will find the two icons in the programs file folder for

– NCP Client Monitor
– NCP Client Service

(Before starting the monitor the service must have been installed! See → “Establish a connection” and “PDA monitor”.)

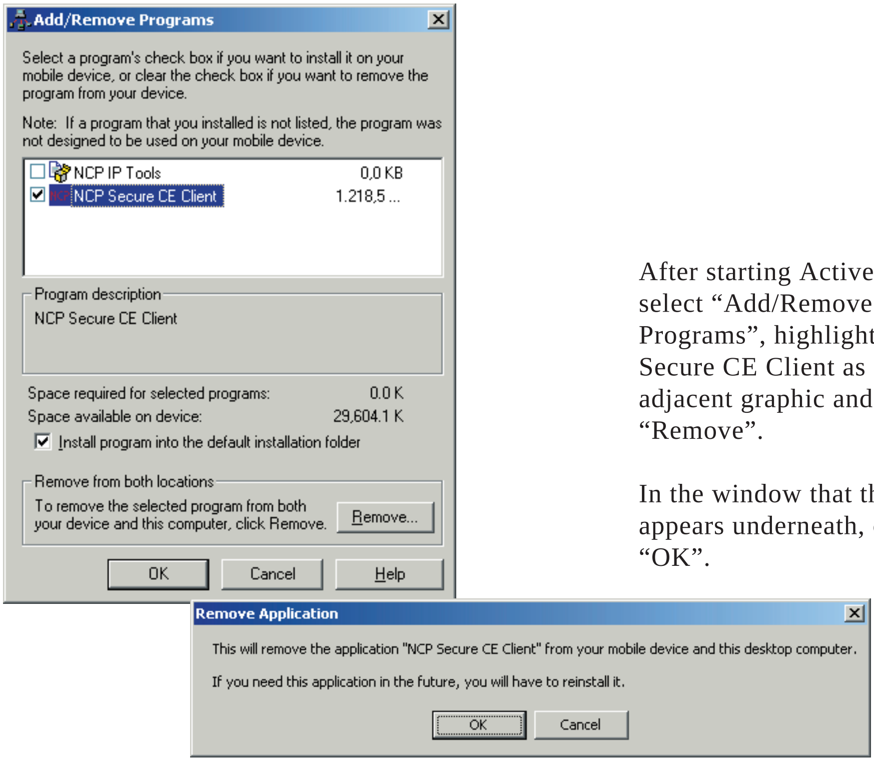
Before a connection can be established, the telephone book with the configured destination systems, and the certificate data, if required, must be transferred to the PDA!

→ *2.4 Transferring the Profiles and the Certificates*

2.5 Uninstalling the PDA Component

The PDA component can be removed from the PC side via ActiveSynch, and also directly on the PDA.

2.5.1 Uninstalling from PC



Add/Remove Programs

Select a program's check box if you want to install it on your mobile device, or clear the check box if you want to remove the program from your device.

Note: If a program that you installed is not listed, the program was not designed to be used on your mobile device.

□	NCP IP Tools	0,0 KB
☑	NCP Secure CE Client	1.218,5 ...

Program description

NCP Secure CE Client

Space required for selected programs: 0.0 K

Space available on device: 29,604.1 K

☑ Install program into the default installation folder

Remove from both locations

To remove the selected program from both your device and this computer, click Remove.

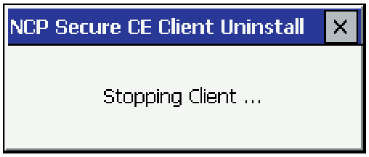
Remove Application

This will remove the application "NCP Secure CE Client" from your mobile device and this desktop computer.

If you need this application in the future, you will have to reinstall it.

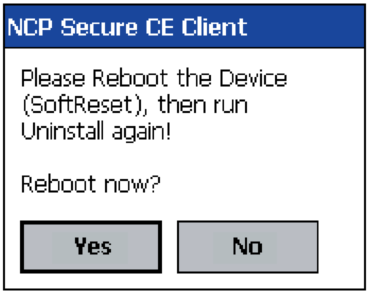
After starting ActiveSynch select “Add/Remove Programs”, highlight the NCP Secure CE Client as in the adjacent graphic and click on “Remove”.

In the window that then appears underneath, click on “OK”.



NCP Secure CE Client Uninstall

Stopping Client ...



NCP Secure CE Client

Please Reboot the Device (SoftReset), then run Uninstall again!

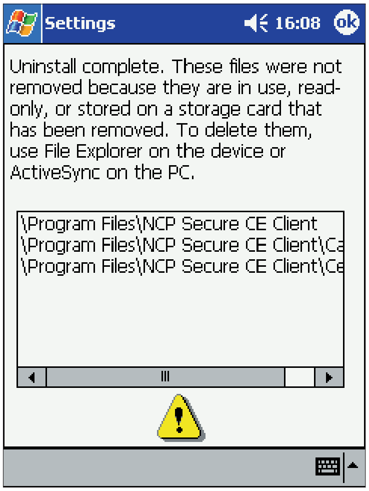
Reboot now?

On the PDA a message appears briefly next to it

... and then a request to do a soft reset appears.

Click OK, execute a soft reset, and then redo the Uninstall as described to this point!

→ *next page*



Uninstall complete. These files were not removed because they are in use, read-only, or stored on a storage card that has been removed. To delete them, use File Explorer on the device or ActiveSync on the PC.

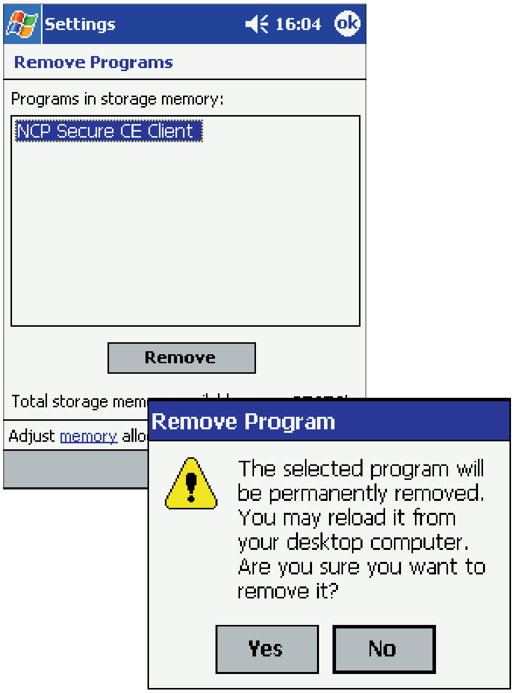
\Program Files\NCP Secure CE Client
\Program Files\NCP Secure CE Client\Ca
\Program Files\NCP Secure CE Client\Ce

After the renewed sequence the uninstall is concluded.

If certificates are still present on the PDA (see adjacent graphic), then these must be manually removed from the specified directories.

The profile settings will be deleted automatically.

2.8.2 Uninstalling the PDA component



Programs in storage memory:

NCP Secure CE Client

Total storage mem

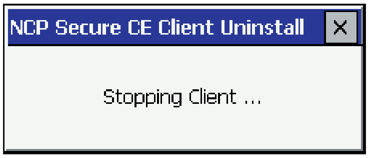
Adjust memory allo

Remove Program

The selected program will be permanently removed. You may reload it from your desktop computer. Are you sure you want to remove it?

Select “Settings – System – Remove Programs” in the start menu of the PDA, select the program NCP Secure CE Client and activate the remove button.

The system will ask you to confirm with “Yes”.

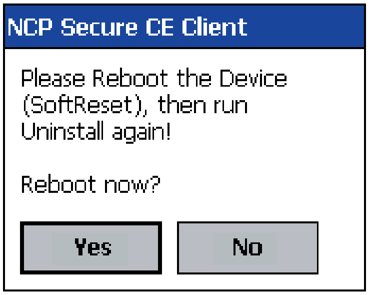


NCP Secure CE Client Uninstall

Stopping Client ...

The client will be stopped and...

→ *continue next page*



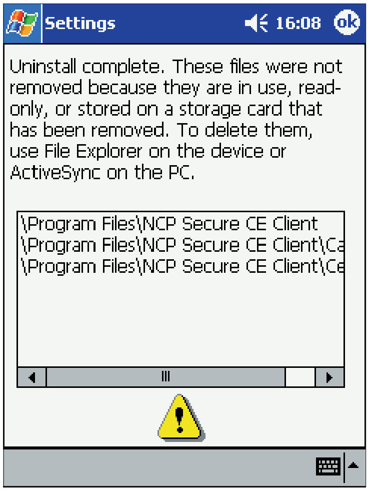
NCP Secure CE Client

Please Reboot the Device (SoftReset), then run Uninstall again!

Reboot now?

...then you will be requested to execute a soft reset.

Click OK here, execute a soft reset, and .then redo the uninstall as described to this point!



Uninstall complete. These files were not removed because they are in use, read-only, or stored on a storage card that has been removed. To delete them, use File Explorer on the device or ActiveSync on the PC.

\Program Files\NCP Secure CE Client
\Program Files\NCP Secure CE Client\Ca
\Program Files\NCP Secure CE Client\Ce

After the renewed sequence the uninstall is concluded.

If certificates are still present on the PDA (see adjacent graphic, (see adjacent graphic) then these must be manually removed from the specified directories.

The profile settings will be automatically deleted.

2.6 Extended Installation

An extended installation and modifications of the configuration can be done with the programs AUTOINSTALL.EXE on the PC and NCPCONFIG.EXE on the PDA.

2.6.1 Functions of AUTOINSTALL.EXE

In the installation directory of the PC component ther is the file AUTOINSTALL.RTF under \ncp\ceclient\bin\. This file describes how to use AUTOINSTALL.EXE which is located in the same directory.

Using this file you can execute following functions:

□ Installing

□ Uninstalling

□ Transferring the Phonebook

□ Changing the License

□ Changing the Settings

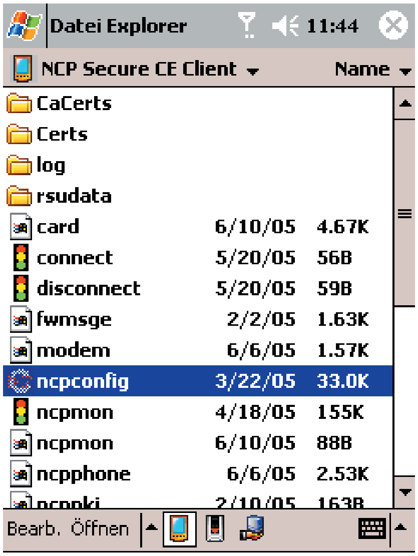
2.6.2 Autostarting the NCP Service on the PDA

The NCP Service does not have to be manually started from the program monitor after the installation, and after a soft reset. The service is started automatically if the ncprwscestart program has been copied from the installation directory on the PDA into the autostart directory under Windows CE. You can do this with AUTOINSTALL.EXE.

2.7 Configuration Programs on the PDA

The basis configuration is set in the profil settings by the configurator of the PC component. Further settings can be done on the PDA for adjustment to special devices. For this the configuration program NCPCONFIG.EXE with a pop up menu is available.

2.7.1 Functions of NCPCONFIG.EXE

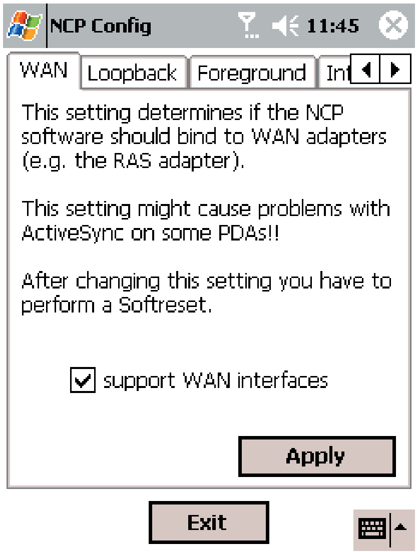


CaCerts		
Certs		
log		
rsudata		
card	6/10/05	4.67K
connect	5/20/05	56B
disconnect	5/20/05	59B
fwmsge	2/2/05	1.63K
modem	6/6/05	1.57K
ncpconfig	3/22/05	33.0K
ncpmon	4/18/05	155K
ncpmon	6/10/05	88B
ncpphone	6/6/05	2.53K
ncppki	2/10/05	163B

The program NCPCONFIG.EXE is stored in the installation directory (normally: \Programs\NCP Secure CE Client\) on the PDA and can be started manually.

After choosing the program five index cards will be displayed with informations for possible settings and device configurations.

■ **WAN Support**



This setting determines if the NCP software should bind to WAN adapters (e.g. the RAS adapter).

This setting might cause problems with ActiveSync on some PDAs!!

After changing this setting you have to perform a Softreset.

☑ support WAN interfaces

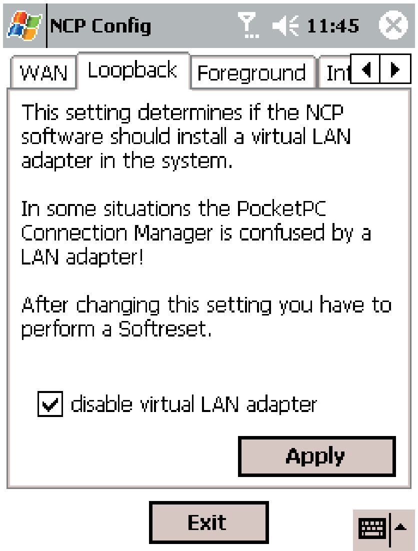
Support of WAN adapters can be configured on the PDA with the NCPCONFIG.EXE program. This program is in the installation directory on the PDA and can be started manually from the directory. The system is shipped with WAN support switched on.

Firewall functionality for the RAS adapter is also provided, but only with active WAN support. In addition, WAN support is also required in order to use IPSec tunneling via RAS connections. All other connection types via the RAS adapter do not require WAN support.

The prerequisite for WAN support is EUU3 on the PDA. After activation and subsequent soft reset, an ActiveSynch connection to the PC (via

USB or serial port) must still be possible. If this is not the case, then WAN support is not functioning and must be switched off with NCPCONFIG.EXE. After another soft reset ActiveSynch should be functioning again. NCP recommends deactivating WAN support only if problems occur.

Loopback (Operation Without Virtual Network Adapter)



This setting determines if the NCP software should install a virtual LAN adapter in the system.

In some situations the PocketPC Connection Manager is confused by a LAN adapter!

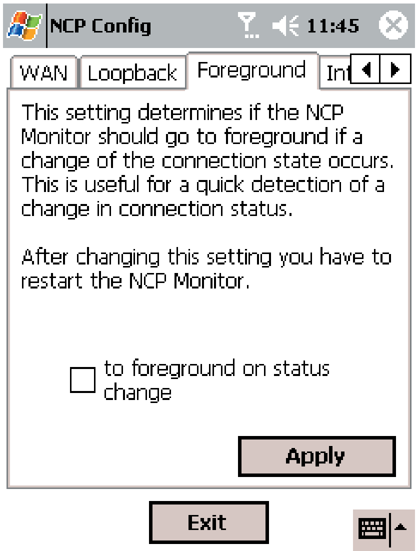
After changing this setting you have to perform a Softreset.

☑ disable virtual LAN adapter

On Windows CE devices of the PocketPC platform, the virtual network adapter “NCP Loopback” is deactivated with new installation (standard). This means that profile settings with NCP Dialer, and to some extent automatic mode as well, cannot be implemented. These profiles are automatically hidden on the PDA after an upload from the Configurator. In this case a text appears in the log window, stating that the profiles are not compatible with the current setting on the PDA.

Operation without virtual network adapter is recommended on devices with Pocket PC 2003 (Phone Edition).

Foreground



This setting determines if the NCP Monitor should go to foreground if a change of the connection state occurs. This is useful for a quick detection of a change in connection status.

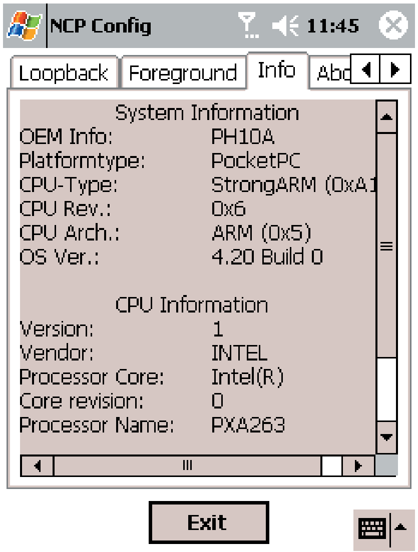
After changing this setting you have to restart the NCP Monitor.

□ to foreground on status change

When changing the connection status the Monitor appears in the foreground, if it has been switched on via the user interface in NCPCPNFIG.EXE on the PDA. This can be helpful when a quick reaction murst take place due to an unwanted disconnection.

The Monitor must be restarted after changing this setting.

Info



System Information

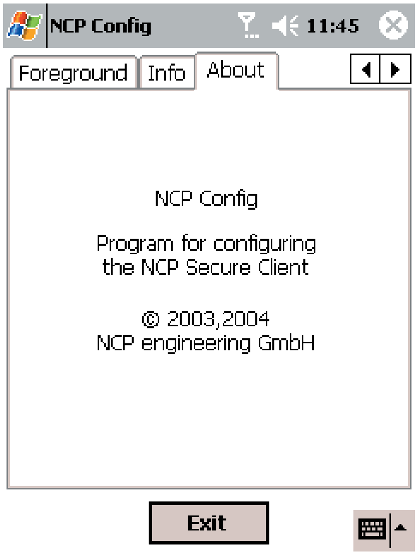
OEM Info: PH10A
Platformtype: PocketPC
CPU-Type: StrongARM (0xA1
CPU Rev.: 0x6
CPU Arch.: ARM (0x5)
OS Ver.: 4.20 Build 0

CPU Information

Version: 1
Vendor: INTEL
Processor Core: Intel(R)
Core revision: 0
Processor Name: PXA263

The Info folder shows quickly and clearly the most important informations concerning the system and the CPU.

About



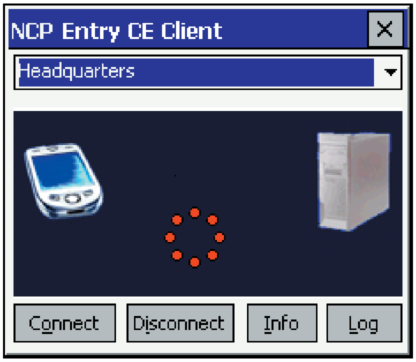
NCP Config

Program for configuring
the NCP Secure Client

© 2003,2004
NCP engineering GmbH

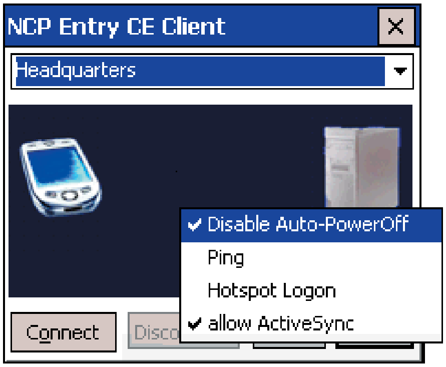
In this folder informations about the configuration program NCPCONFIG are displayed.

2.7.2 Popup Menu



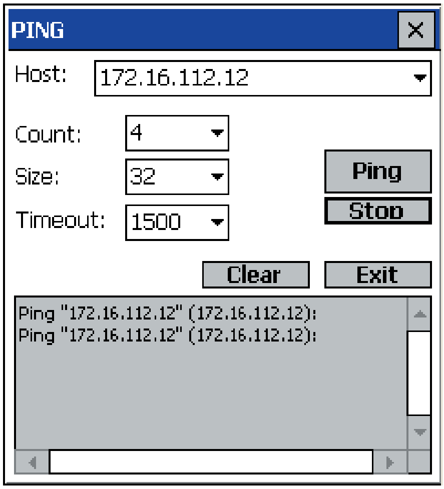
The popup menu is activated by doing a tab-and-hold with the pen on the grafic display of the monitor.

- **Auto-PowerOff**



The default setting of the auto-poweroff function is deactive, meaning that the PDA does not automatically switch to an electricity saving modus, when a connection has taken place and no data traffic is being done.

- **Ping**



Host: 172.16.112.12

Count: 4

Size: 32

Timeout: 1500

```
Ping "172.16.112.12" (172.16.112.12):
Ping "172.16.112.12" (172.16.112.12):
```

The CE Client has a program for sending ICMP echo_requests (ping). It is called via the Client’s popup menu. The program “Ping.exe” is in the installation directory of the Client software and can also be used stand-alone.

HotSpot Logon

To keep the remote Client invulnerable at all times when logging onto the WLAN, the firewall dynamically releases the ports for http or https for logon or logoff.

NCP has permanently integrated the Personal Firewall in the Secure Client software in order to protect the Remote Client against any kind of attack in every phase of the connection set-up in WLANs and hotspots, without the user having to do anything. It has intelligent automated processes for secure hotspot logon.

Requirements:

The user must be in the receiving range of a hotspot, with an activated WLAN card. There must be a connection to the hotspot and the wireless adapter must have an assigned IP-address.

The clients firewall makes sure that only the IP-address assignment is being done by DHCP without any further possibilities of access to or from the WLAN. The firewall has intelligent automated processes for clearing the ports of one or more https so as to make logins and -outs to the hotspot available. Durig this process only data traffic to the hotspot server is possible. In this way a public WLAN can only be used for connecting VPN to the central data network, direct internet access is excluded. For opening the homepage of a hotspot in the browser a possible existing proxy-configuration must be deactivated.

At present the clients hotspot access works only with those hotspots, that redirect inquiries with the help of browsers to the homepage of the public WLAN provider (for example T-Mobile or Eurospot).

Functional Description:

Under previously described conditions the user can select the option “HotSpot Logon” in the popup menu. The Client then searches the hotspot automatically and opens the website for the logon procedure in the standard browser. After successfully entering the access data and release by the operator, the VPN connection can be established to corporate headquarters, for instance, and the user can securely communicate, as he would on an office workstation.

In this process data traffic is only possible with the hotspot server of the operator. Non-requested data packets are rejected. Direct communication to the Internet bypassing the VPN tunnel is impossible due to the previously described dynamic firewall rules that are set automatically by the integrated Personal Firewall of the Client.

If hotspot logon has not been executed by the client the user gets the message “Hotspot could not be found”. In this case it must be checked if a general problem exists in conjunction with the mechanisms implemented by NCP engineering relative to the hotspot operator.

ActiveSync with Link Firewall

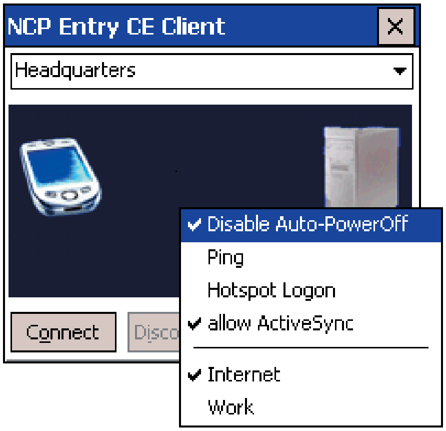
The (global) firewall must be released for ActiveSync in the case of a direct connection (via USB, serial or infrared). This is done in the firewall settings of the monitor under “Options - Permit ActiveSync connections (TCP 990, 999, 5678, 5679)”. This setting can also be made on the PDA via the popup menu, if the (global) firewall is active.

If ActiveSync is operated via network (LAN or WLAN) then in addition a separate firewall rule for name resolution (DNS/WINS) must be created.

ActiveSync connections are handled by the Link Firewall as normal TCP connections. Although ActiveSynch establishes the TCP connection in both directions (PC <—> PDA), with activated Stateful Inspection filter traffic is only allowed in the Link Firewall. The connection is blocked if “Only permit communication in the tunnel” is activated.

Also compressed connections of the RAS-Dialer can by monitored by the Client as normal IP traffic, because the compression (CCP), as well as the VanJacobson IP header compression (in the IPCP) can no longer be negotiated.

PocketPC Connection Manager



In the profile settings the connection medium “PocketPC Connection Manager” can be set for PocketPC platforms, in the “Basic settings” parameter folder. This connection medium is ideal for devices with integrated telephone (MDA). While a GPRS connection exists, you can telephone at the same time. The PocketPC Connection Manager automatically takes over the parking of GPRS connection. When configuring a profile for this application ensure that the selected timeout-period is large enough, or that timeout is deactivated, and Dead Peer Detection (DPD) is deactivated in the IPSec settings.

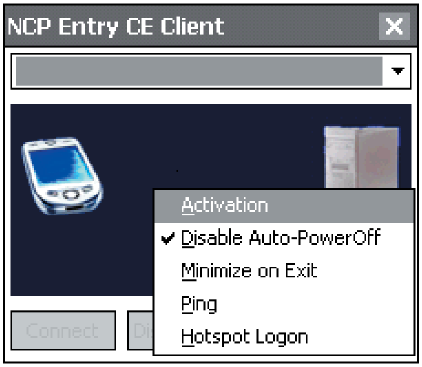
When using this connection medium, which is only practical for deactivated Loopback adapter, you can select the destination network: Internet or corporate network. This setting can also be changed retroactively on the PDA via the Popup menu.

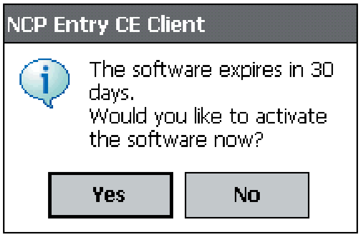
When using this media type, the PocketPC Connection Manager is forced to set-up a connection (in the Internet or corporate network). This means that the Connection Manager will automatically select a RAS connection and set it up, or it will detect an existing LAN card and will not setup any other connection.

Under “Start / Settings / Connections”, the system can configure appropriate Internet and company connections with its own onboard resources. If the virtual adapter is active then more precise project-specific knowledge of the environment is required for the effective use of the Connection Manager.

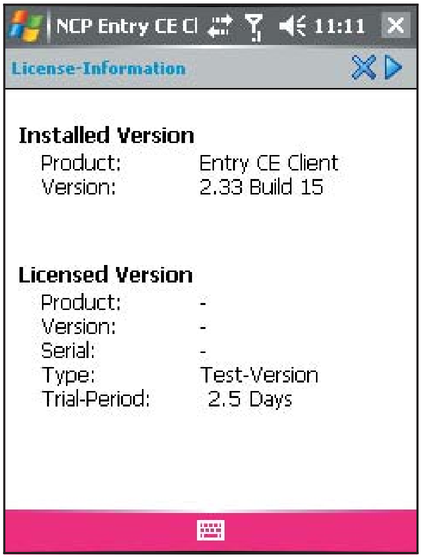
2.8 Licensing via Activation Dialog

The client software is always installed as a test version. After a new or pre-installation, the client needs to be activated. An older version which has been upgraded, will be during the upgrade process be reset to a test version and so too requires to be activated within 30 days.




NCP Entry CE Client

The software expires in 30 days.
Would you like to activate the software now?



License-Information

Installed Version

Product: Entry CE Client
Version: 2.33 Build 15

Licensed Version

Product: -
Version: -
Serial: -
Type: Test-Version
Trial-Period: 2.5 Days

The activation dialog is opend using the popup menu “Activiation” (see figure on the left) or by pressing on “Yes” when the message box is displayed after the start of the NCP client service.

The time remaining until software activation is required, i.e. the validity period of the test version, is displayed in the license information (figure left below). In order to use a full version with no time limitations, the software must be released version shown in the activation dialog with the license key and the serial number that you have received.

The activation dialog can be opened using the arrow button in the license information message (figure left below).

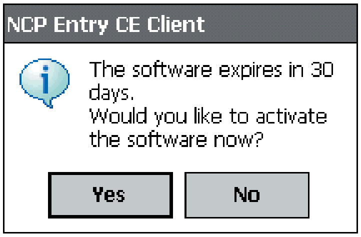
The license data can be entered either online or offline via a wizard.

In the offline variant, a file that is generated after entering the license key and serial number must be sent to the NCP aczivation server, and the activation key that is then displayed on the website must be noted. This activation key can be entered in the licensing window of the Monitor menu at a later point in time.

In the online variant, an assistant forwards the licensing data to the activation server immediately after entry and thus allowing the software to immediately be released.

2.8.1 Test Version Validity Period

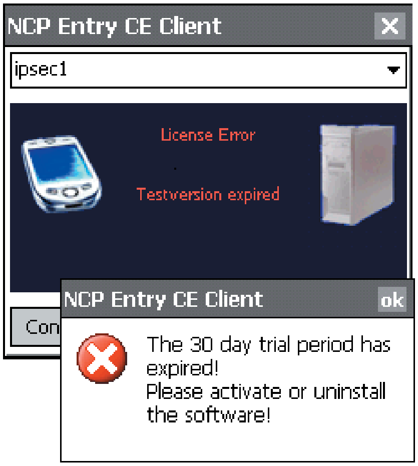
The test version is valid for 30 days. Without software activation or licensing it will no longer be possible to setup a connection after this 30-day period expires.


NCP Entry CE Client

The software expires in 30 days.
Would you like to activate the software now?

After installation, each time the software is started the validity period will be shown in the popup window once a day.

The software can be used during the trial period when clicking “No” in the activation dialog (shown on the left side).


NCP Entry CE Client

ipsec1

License Error

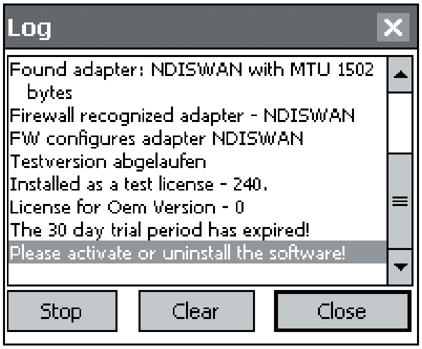
Testversion expired

NCP Entry CE Client

The 30 day trial period has expired!
Please activate or uninstall the software!

When the trial period has expired the software must be either activated or de-installed.

To activate, start the activation dialog by pressing the “ok”-button.

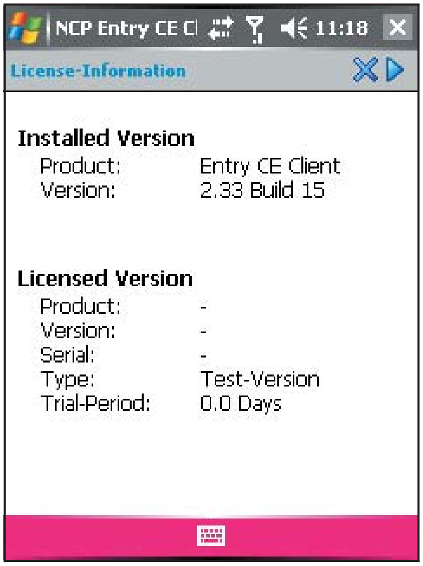

Log

```
Found adapter: NDISWAN with MTU 1502
   bytes
Firewall recognized adapter - NDISWAN
FW configures adapter NDISWAN
Testversion abgelaufen
Installed as a test license - 240.
License for Oem Version - 0
The 30 day trial period has expired!
Please activate or uninstall the software!
```

When the trial period has expired a message is also displayed in the log file.

2.8.2 Software Activation

When the test phase has expired, the software must be either activated or de-installed. To activate, select the menu option “Activation” in the popup menu.



Installed Version

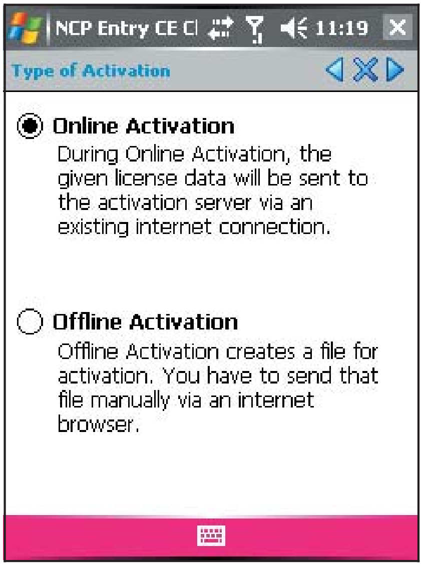
Product:	Entry CE Client
Version:	2.33 Build 15

Licensed Version

Product:	-
Version:	-
Serial:	-
Type:	Test-Version
Trial-Period:	0.0 Days

Here you can see which software version you have and how the software is licensed, i.e. you can see that the test version has expired and that the software has not yet been activated/licensed.

To activate click the arrow button right above.

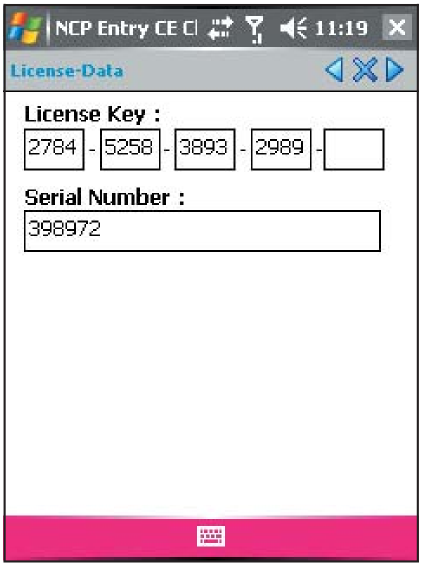


● **Online Activation**
During Online Activation, the given license data will be sent to the activation server via an existing internet connection.

○ **Offline Activation**
Offline Activation creates a file for activation. You have to send that file manually via an internet browser.

In the window that appears, select whether you wish activate the client online or offline by selecting either online activation or offline activation respectively.

In the offline variant, a file that is generated after entering the license key and serial number must be sent to the NCP activation server, and the activation key that is then displayed on the website must be noted. In the online variant, an assistant forwards the licensing data to the web server immediately after entry and thus the software is immediately released.


NCP Entry CE Cl 11:19

License-Data

License Key : 2784 - 5258 - 3893 - 2989 -

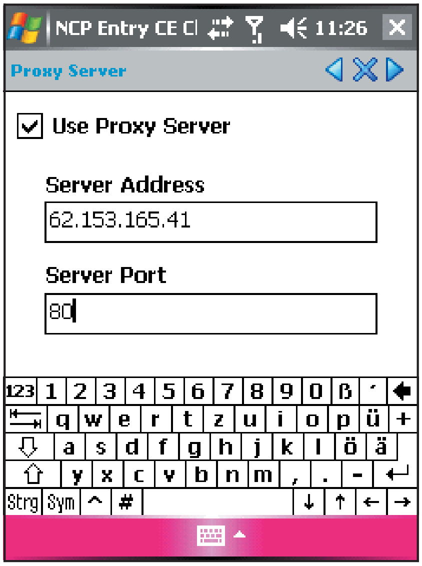
Serial Number : 398972

After selecting the type of activation the license data is to be entered in the appropriate fields.

Click on the arrow button on the right to continue.

Online Variant

With the online variant the license data will be transmitted to the NCP Activation Server via an Internet connection. This Internet connection can either be established via the Data Communications Dialer (via PocketPC Connection Manager or Modem/Mobile) or via the Entry Client.


NCP Entry CE Cl 11:26

Proxy Server

☑ Use Proxy Server

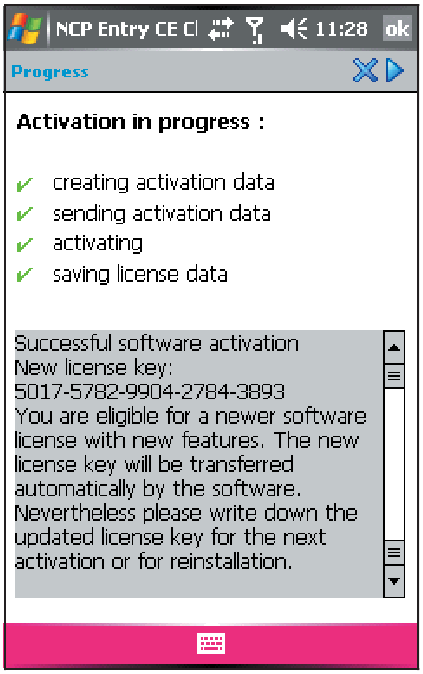
Server Address: 62.153.165.41

Server Port: 80

The activation assistent requiresa connection to already be established.

Ensure that port 80 is permitted (for HTTP) if the firewall is activated. (If a proxy server has been configured in the operating system enter the address data.)

Click on the arrow button on the right to continue.



Activation in progress :

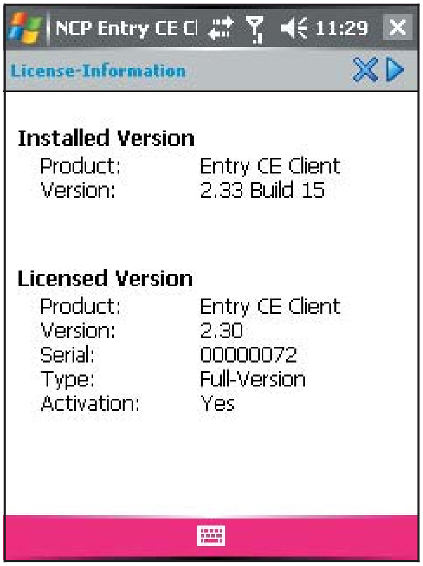
- ✓ creating activation data
- ✓ sending activation data
- ✓ activating
- ✓ saving license data

Successful software activation
New license key:
5017-5782-9904-2784-3893
You are eligible for a newer software license with new features. The new license key will be transferred automatically by the software.
Nevertheless please write down the updated license key for the next activation or for reinstallation.

The software is activated automatically in the specified sequence.

As soon as the Activation Server detects that you are entitled to a newer software license and that the license key agrees with the installed software, then with online activation the new license key will be transferred automatically (license update), and the new features of the software will be available to use.

Please write down the update key for the next activation or for reinstallation.



Installed Version

Product:	Entry CE Client
Version:	2.33 Build 15

Licensed Version

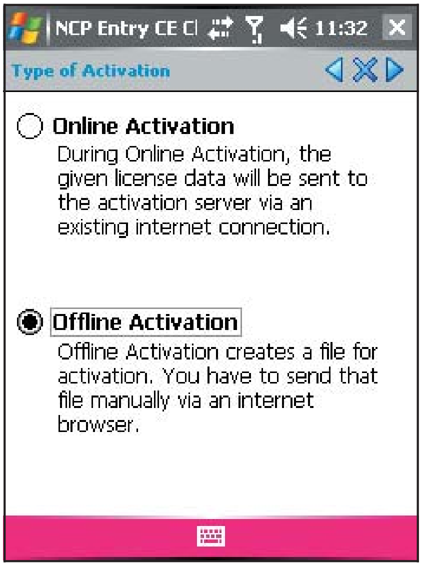
Product:	Entry CE Client
Version:	2.30
Serial:	00000072
Type:	Full-Version
Activation:	Yes

Upon completion of the activation process, the software version number may differ from the licensed version number if the license is valid only for an older version.

Offline Variant

The offline variant is executed in two steps. In the first step a file is generated after entering the license key and serial number, and is then sent to the NCP activation server. The URL is:
`http://www.ncp.de/english/services/license`

An activation key will be shown on the web site, and you must note this number in order to enter the license key in the licensing window of the activation dialog in a second step. (Which can also be executed at a later point in time.)

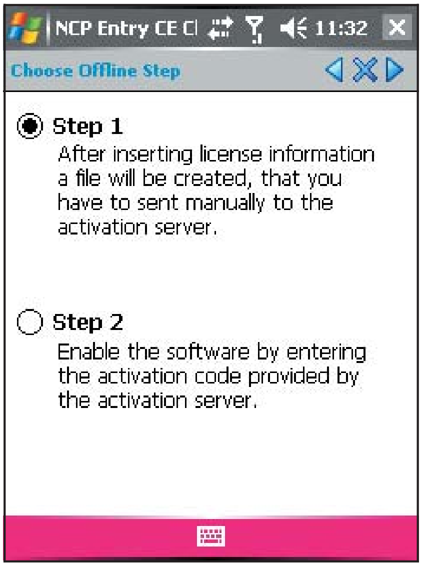


○ **Online Activation**
During Online Activation, the given license data will be sent to the activation server via an existing internet connection.

● **Offline Activation**
Offline Activation creates a file for activation. You have to send that file manually via an internet browser.

The offline variant can be initiated via the activation dialog and can be selected in the first window.

Click on the arrow button on the right.

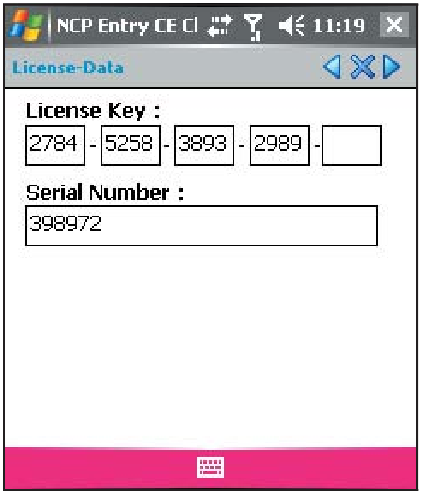


● **Step 1**
After inserting license information a file will be created, that you have to sent manually to the activation server.

○ **Step 2**
Enable the software by entering the activation code provided by the activation server.

In the second window of the activation assistant, the two steps of the offline activation process are explained. The first step, creation of the activation file, is selected automatically.

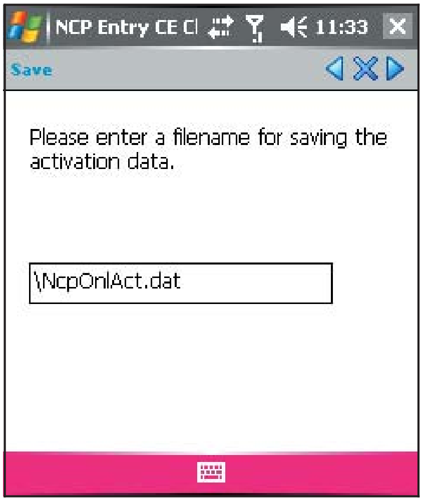
Click on the arrow button on the right to continue.



License Key :
2784 - 5258 - 3893 - 2989 -

Serial Number :
398972

In the following window enter the license data and click on the arrow button...

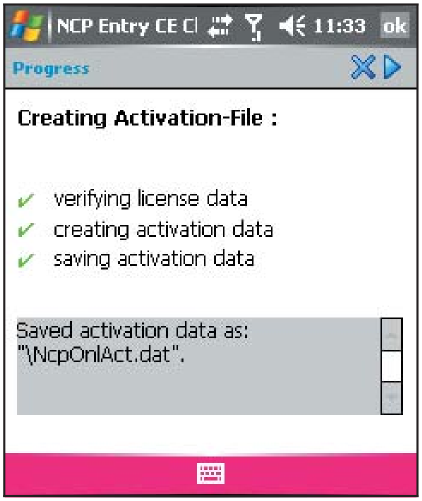


Please enter a filename for saving the activation data.

\NcpOnlAct.dat

Enter name and path for the activation file.

Click on the arrow button...



Creating Activation-File :

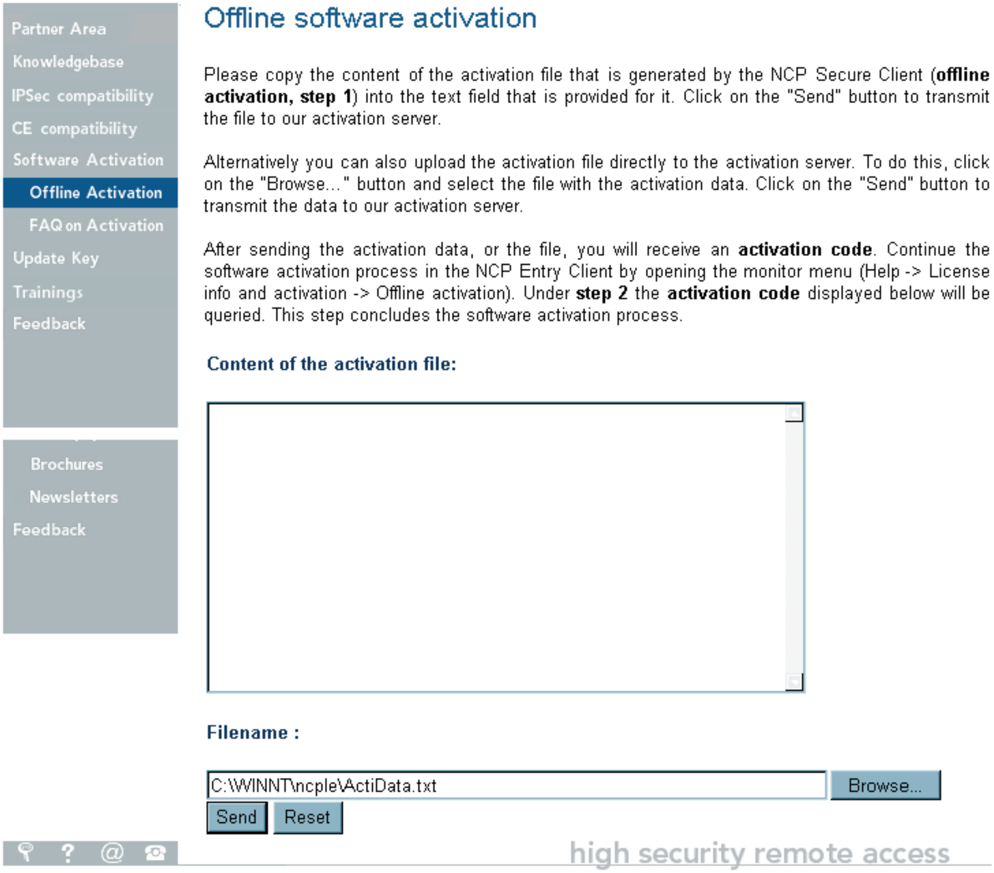
✓ verifying license data
✓ creating activation data
✓ saving activation data

Saved activation data as:
"\NcpOnlAct.dat".

Now an activation file is created and this file must be transferred to the Activation Server.

For this the NCP web site must be called:

http://www.ncp.de/english/services/license



Offline software activation

Please copy the content of the activation file that is generated by the NCP Secure Client (**offline activation, step 1**) into the text field that is provided for it. Click on the "Send" button to transmit the file to our activation server.

Alternatively you can also upload the activation file directly to the activation server. To do this, click on the "Browse..." button and select the file with the activation data. Click on the "Send" button to transmit the data to our activation server.

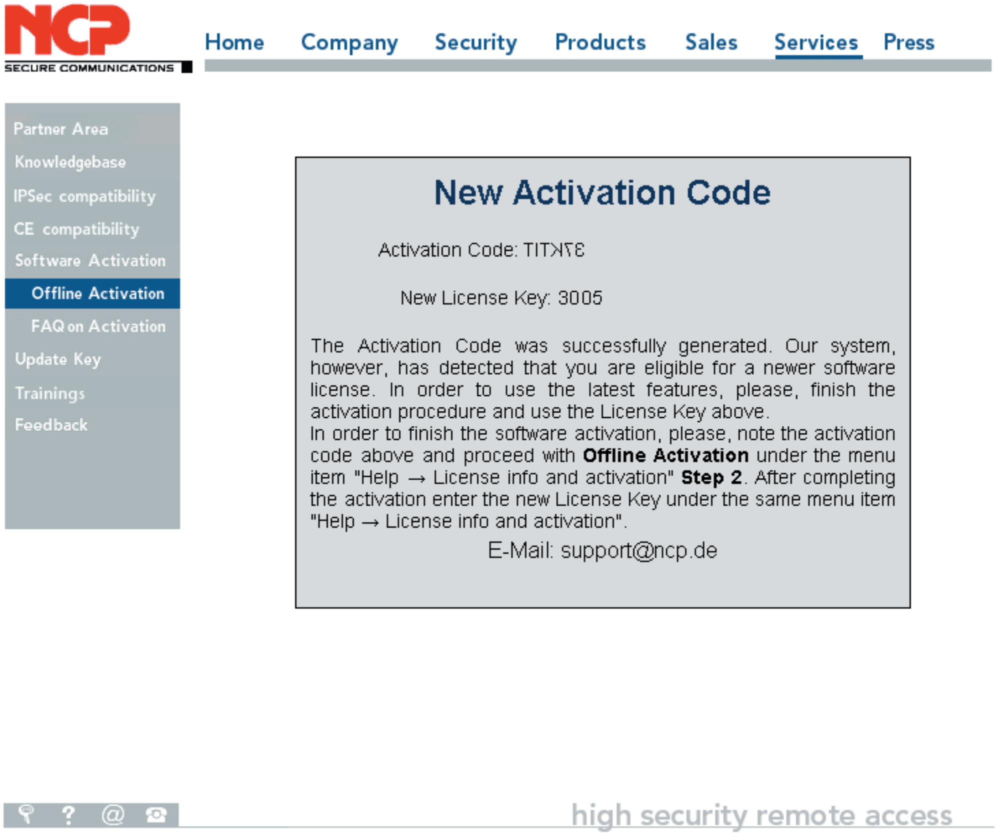
After sending the activation data, or the file, you will receive an **activation code**. Continue the software activation process in the NCP Entry Client by opening the monitor menu (Help -> License info and activation -> Offline activation). Under **step 2** the **activation code** displayed below will be queried. This step concludes the software activation process.

Content of the activation file:

Filename : C:\WINNT\ncple\ActiData.txt

There are two ways to transfer the activation file to the Activation Server. Either copy the content of the activation file with Copy & Paste, after you have opened the activation file with the Notepad (ASCII editor), into the window that is open on the web site, or click on the “Browse” button and select the activation file. Click on “Send”!

Then the activation code will be generated and displayed on the web site. Note the activation code and continue the activation process under the menu option “Help” / License data and activation", by executing the second step of the activation in the offline variant.



New Activation Code

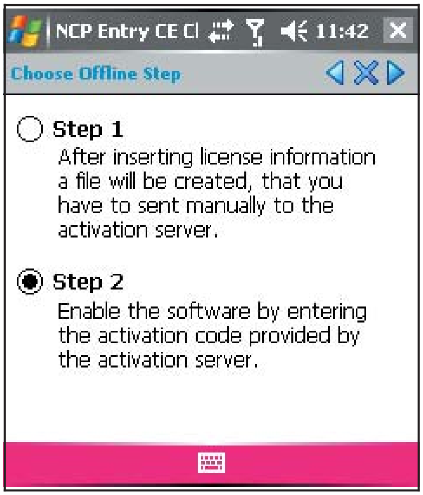
Activation Code: TITKΓƐ

New License Key: 3005

The Activation Code was successfully generated. Our system, however, has detected that you are eligible for a newer software license. In order to use the latest features, please, finish the activation procedure and use the License Key above.
In order to finish the software activation, please, note the activation code above and proceed with **Offline Activation** under the menu item "Help → License info and activation" **Step 2**. After completing the activation enter the new License Key under the same menu item "Help → License info and activation".

E-Mail: support@ncp.de

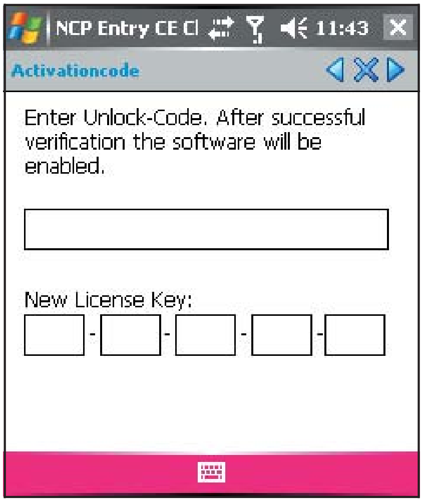
If the Activation Server detects that you are entitled to a newer software license and that the license key agrees with the installed software, then with the online activation the new license key will be displayed automatically. If you want to activate the new features then note the new license key, conclude the activation process, and then use the new license key.



○ Step 1
After inserting license information a file will be created, that you have to sent manually to the activation server.

● Step 2
Enable the software by entering the activation code provided by the activation server.

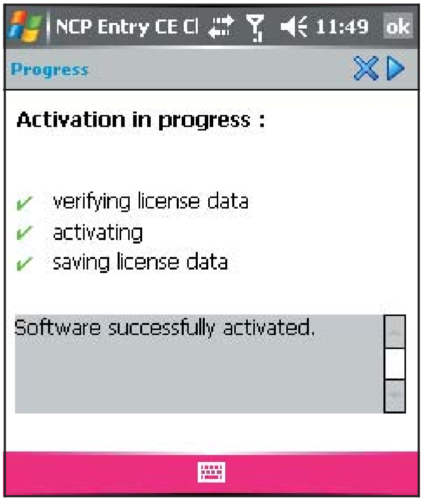
The second step of the offline variant is triggered via the Monitor menu “Help” “License data and activation”. After the offline variant has been selected, select the second step.



Enter Unlock-Code. After successful verification the software will be enabled.

New License Key:

A window will open where you can enter the activation code. After you have entered the activation code you can click on the arrow button.

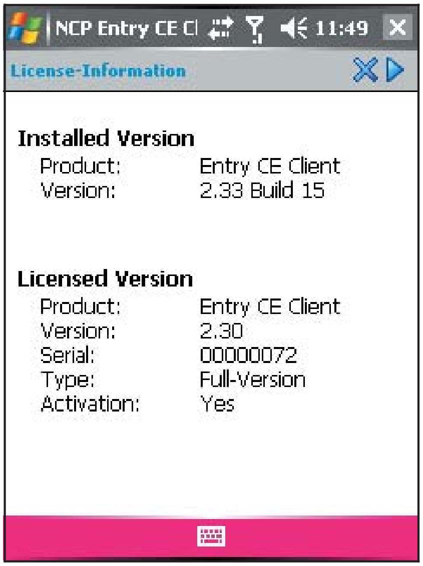


Activation in progress :

✓ verifying license data
✓ activating
✓ saving license data

Software successfully activated.

Offline activation is completed with the following window.



Installed Version

Product: Entry CE Client
Version: 2.33 Build 15

Licensed Version

Product: Entry CE Client
Version: 2.30
Serial: 00000072
Type: Full-Version
Activation: Yes

The license data is verified and then transferred.

Finish the activation dialog when the verification has been concluded.

Upon completion of the activation process, you will see that you now have correctly activated full version in the window for the license data.

The software version number may differ from the licensed version number if the license is valid only for an older version.

2.8.3 Operating System on the mobile device

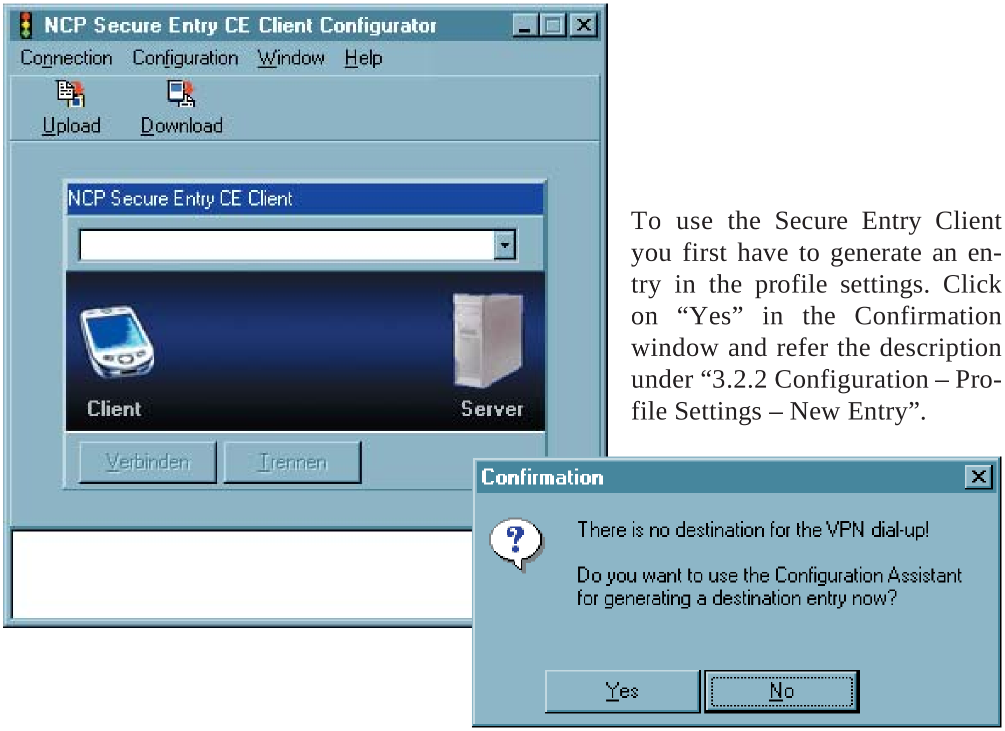
Windows Mobile 6, along with the other Windows Mobile / Win CE versions is supported by NCP Entry CE Client v. 2.33.

To install on Windows Mobile 6, it is required to have a licensed v. 2.33 (or higher).This software cannot be operated under an older license key.

It is a prerequisite to have at least a version 2.3 to activate the Client software under Windows Mobile 6. If a no-charge update to version 2.3 is available to you, then you will receive the respective license key when the software is activated. Otherwise, updates to version 2.3 may be purchased in the NCP E-store or purchased from your local NCP dealer.

3. Client Configurator

If the software has been installed according to the standard defaults, then the configurator can be activated via the start menu "Programs / NCP Secure Client / Secure Entry CE Client Configurator". This opens the configurator window on the screen if a destination system has been already configured (see above → 2.3 Before Starting).



There is no destination for the VPN dial-up!

Do you want to use the Configuration Assistant for generating a destination entry now?

To use the Secure Entry Client you first have to generate an entry in the profile settings. Click on "Yes" in the Confirmation window and refer the description under "3.2.2 Configuration – Profile Settings – New Entry".

Note: If the configurator has been reduced to an icon, then it appears as a stoplight in the task bar.

The Configurator has 4 important Functions:

☑ The definition and configuration of the destination systems with the creation of the profile settings.

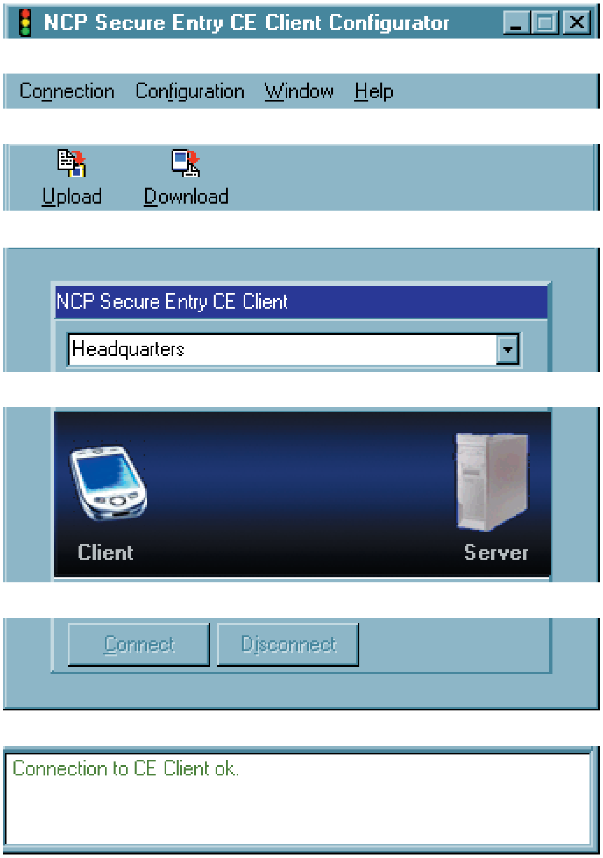
☑ Creating the IPSec and the certificate configuration.

☑ Copying the profile settings onto the PDA device.

☑ Downloading the profile settings from the PDA, in order to make modifications.

3.1 The Client Configurator user interface

The client configurator consists of:



Connection to CE Client ok.

- □ a title line with product designation,
- □ the main menu bar,
- □ a button bar for “Upload” and “Download” of the telephone book
- □ the destination selection for previously created destination systems,
- □ the graphic status field for display of the connection status (currently still without function),
- □ the button bar with “Connect” and “Disconnect” (currently still without function)
- □ and a log window for messages. The texts in this log window, (window size can be changed with the cursor), refer to the communication between PDA and PC component, or the compatibility of the profile settings of the Configurator relative to the current settings of the PDA. Thus, for example, the system checks whether the virtual adapter (Loopback Adapter) is switched off on the PDA, and when copying the profiles onto the PDA, the system indicates that in this case the NCP Dialer cannot be used. The corresponding profile will then not be displayed on the PDA.
  Red messages: Errors and unsuccessful connections
  Green messages: OK messages when uploading profile settings and certificate
  Blue messages: Instructions and warnings due to incompatible profiles WAN support, virtual adapter on the PDA - Upload to the PDA)

The user interface has been Windows conformant designed and adapted to the opera-tion of other Windows applications.

4. The Configurator Menu

The description follows the menu items in the menu bar.

The main menu items in the menu bar are from left to right:

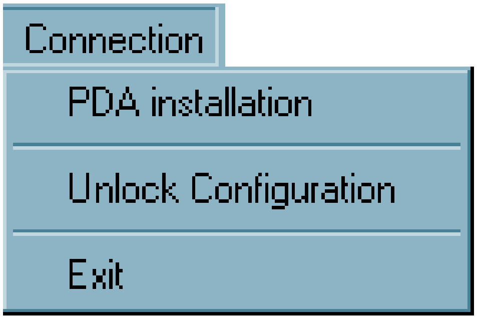
□ Connection |Menu

□ Configuration |Menu

□ Window |Menu

□ Help |Menu

4.1 Connection



This menu item initiates the installation of the PDA components (for more in this regard see 2.6 Installation of the PDA components), unlocks configuration locks and ends the Configurator.

PDA Installation

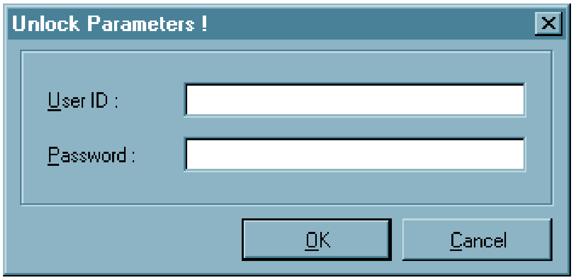
The installation of the PDA component will be triggered from this menu item. Insure taht the physical connection between PDA and PC is established and that ActiveSync is started.

Please insure that the dialog “Software” from ActiveSync is not open when executing the PDA installation program.

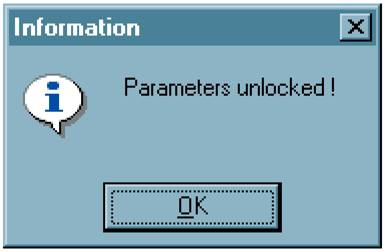
Unlock/Relock Configuration

This parameter will only be displayed when the configuration locks have been configured by your system administrator.

In accordance with the configuration your system administrator may have purposely hidden and locked various parameters in your phonebook/profile settings and respective destination(s). Such parameters are not visible and therefore cannot be modified under normal circumstances.



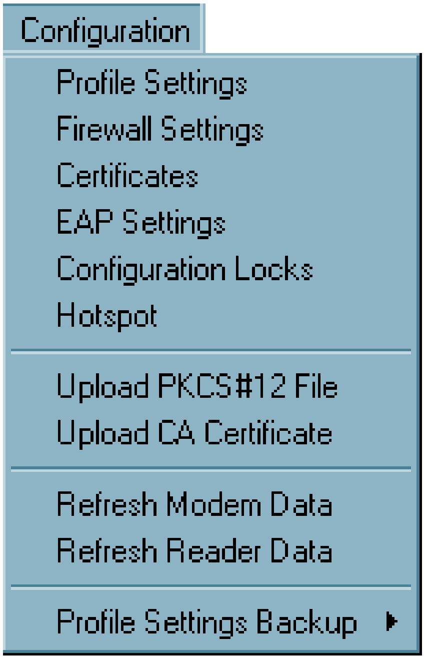
In order to make these parameters appear, select the unlock feature and then enter the user ID and password issued by your system administrator. Upon doing so the parameters will appear and be unlocked. Changes can now be made.



Parameters unlocked !

After this information window (on the left) the relock feature appears in the menu.

4.2 Configuration



Under this menu item the entries are created for the profile settings, this means the destination systems are created (the description of the individual parameters is located under “Configuration parameters / Profile Settings”).

In addition, you can autonomously configure how certificates are to be used, which IP pakets should be selected by the firewall and which configuration rights the user will obtain.

The menu item “Transfer PKCS#12-file to PDA” is for copying the soft certificate onto the PDA device.

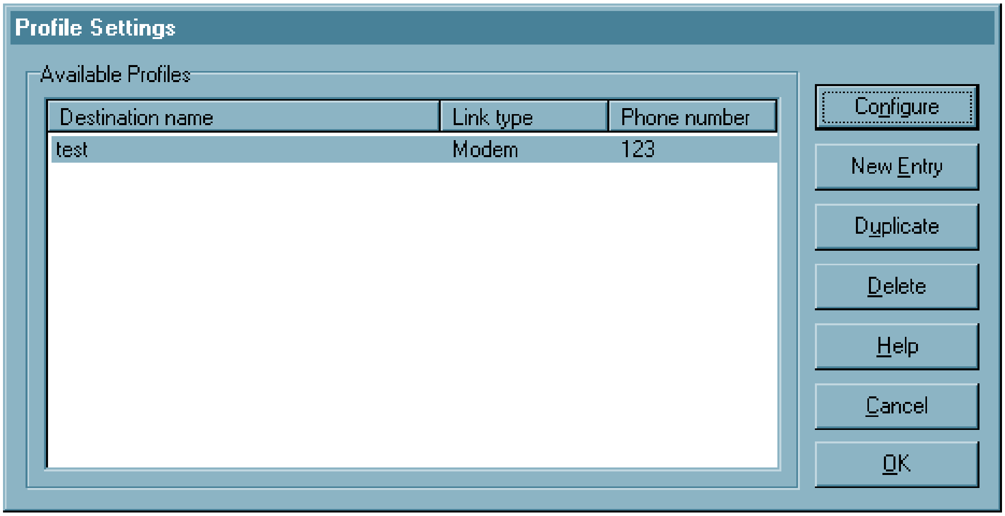
4.2.1 Profile Settings

■ Entries in the profile settings

After installing the Secure Client for the first time it will be necessary to define a profile for your requirements in the profile settings. For this purpose there is a “Configuration Assistant”, which will walk you through the configuration steps of a profile. In this way the first profile will be created.

The profile settings provide the basis for defining and configuring destinations (profiles) which can be modified or reconfigured at any time according to requirements.

Upon clicking “Profile Settings” in the Monitor menu “Configuration” the menu is opened and displays an overview of the defined profiles and their respective names and the telephone numbers of the according destinations.



Profile Settings

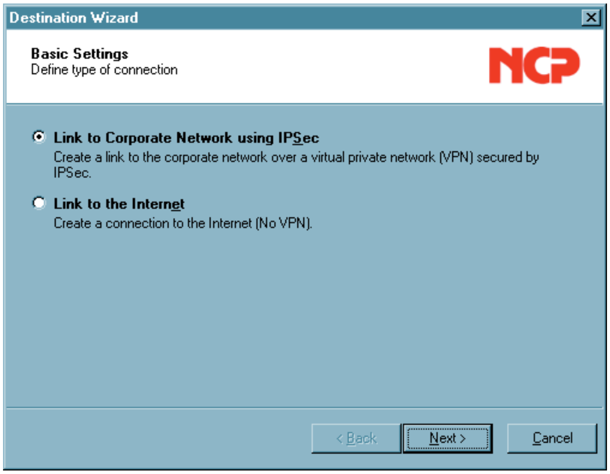
Available Profiles

Destination name	Link type	Phone number
test	Modem	123

There is also a toolbar with the following function buttons: Configure, New Entry, Duplicate, Delete, OK, Help and Cancel.

■ New Entry - Profile

In order to define a new Destination, click on “Profile Settings”. When the window opens click on “New Entry”. Upon doing so the “Configuration Assistant” opens and walks you through the configuration of a new Profile according to your requirements. Upon entering all items in the assistant the new profile is entered in the Profile Settings based on these parameters. All other parameters are assigned a default value.



Destination Wizard

Basic Settings
Define type of connection

● Link to Corporate Network using IPSec
Create a link to the corporate network over a virtual private network (VPN) secured by IPSec.

○ Link to the Internet
Create a connection to the Internet (No VPN).

Using the configuration assistant, connections can be quickly established with the Internet or to the corporate network. The profile is created after a few configuration questions, in accordance with the selection of the desired basic setting.

Below are the required data for the configuration:

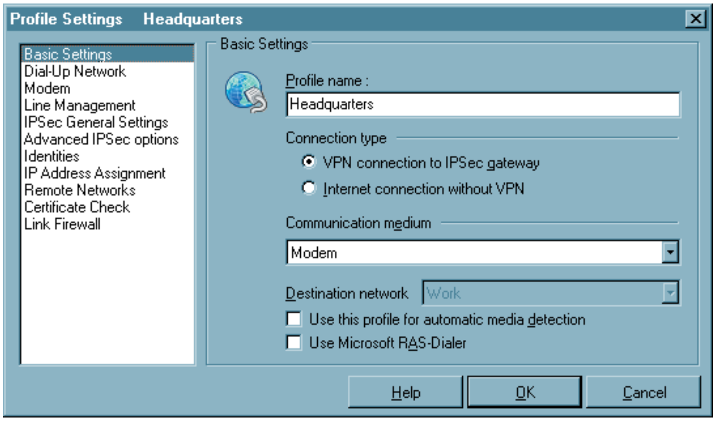
Link to Corporate Network using IPSec:
→ Profile Name
→ Communication Medium
→ Access data for Internet Service Provider (User ID, Password, Phone Number)
→ VPN-Gateway selection (Tunnel Endpoint IP address)
→ Access data for VPN Gateway (XAUTH, User ID, Password)
→ IPSec Configuration (Exch. Mode, PFS Group, Compression)
→ Static key (Preshared Key), without certificate (IKE ID Type, IKE ID)
→ IP Address Assignment (IP address of the client, DNS/WINS Server)
→ Firewall Settings

Link to the Internet:
→ Profile Name
→ Communication Medium
→ Access data for Internet Service Providers (User ID, Password, Phone Number)

The new profile is displayed now in a list of profiles with its assigned name. If no further parameter settings are necessary you can close the profile settings by clicking on “Ok”. The new profile is immediately available in the monitor. It can be selected in the monitor and via the menu “Connection → Connect” a connection to the relating destination can be established.

Configure - Profile

If you want to change any default profile data and parameters, start by selecting the appropriate profile and then click on the “Configure” button. Upon doing so a folder opens and displays a list of the following parameter folders on the left side:



Profile Settings Headquarters

Basic Settings

Profile name : Headquarters

Connection type

● VPN connection to IPSec gateway

○ Internet connection without VPN

Communication medium: Modem

Destination network: Work

☐ Use this profile for automatic media detection

☐ Use Microsoft RAS-Dialer

Basic Settings
Dial-Up Network
Modem
Line Management
IPSec General Settings
Advanced IPSec Options
Identity
IP Address Assignment
Remote Networks
Certificate Check
Firewall Settings

Upon selecting one of the folders the associated parameters will be displayed (see → 4. Configuration Parameters).

Ok – Profile

Upon clicking “OK” in the configuration window the configuration of a profile is concluded. The new or modified profile is available in the monitor. It can be selected in the monitor and via the menu “Connection → Connect” a connection to the relating destination can be established.

Duplicate – Profil

You may want to use an existing profile for the basis of a new profile, perhaps however with slight modifications. In order to do so first select the profile to be duplicated and then click on the “Duplicate” button. Upon doing so the “Basic Settings” parameter folder will open. You must now enter a new name for the profile and then click on “OK”. A new profile is now created with parameters identical to the profile that was duplicated except for the Proflie Name.

Important: It is not possible to have 2 or more profiles with identical names. Each profile must be assigned its own unique name.

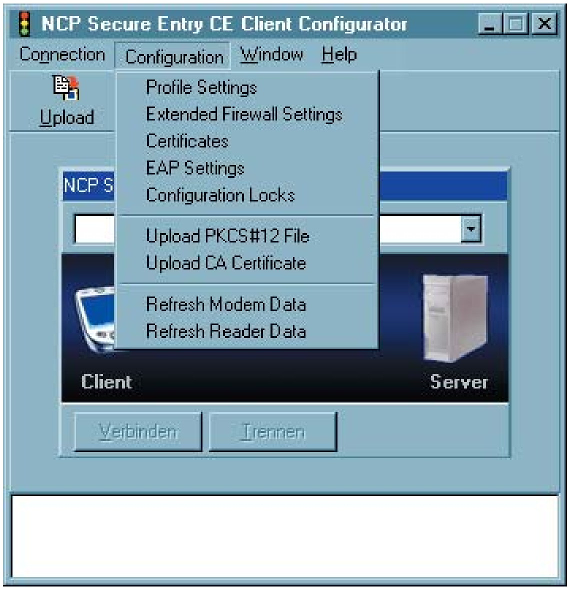
Delete – Profile

If you want to delete a profile select the appropriate profile and then click on the “Delete” button.

4.2.2 Firewall Settings

All firewall mechanisms are optimized for Remote Access applications and are activated when the computer is started. This means that in contrast to VPN solutions with autonomous firewall, the teleworkstation is already protected against attacks before actual VPN utilization.

The Personal Firewall also offers complete protection of the end device, even if the client software is deactivated. All firewall rules can be centrally specified by the administrator, and compliance with these rules can be forced. The prerequisite in this case is the central NCP Secure Enterprise Management system, which is used to configure the Client, which can be permanently specified as unchangeable for the user.



Please note that the firewall settings are globally valid, i.e. they apply for all destination systems in the telephone book.

On the other hand the Link Firewall Setting that is made in the telephone book can only be effective for the associated telephone book entry (destination system) and the connection to this destination system.

Firewall properties

The firewall works in accordance with the principle of packet filtering, in conjunction with Stateful Packet Inspection (SPI). The firewall checks all incoming and outgoing data packets and decides whether a packet will be forwarded or rejected on the basis of the configured rules.

Security is ensured in two ways. First unauthorized access to data and resources in the central data network is prevented. Secondly the respective status of existing connections is monitored via Stateful Inspection. Moreover the firewall can detect whether a connection has opened "Spawned connections" – as is the case with FTP or Netmeeting for example – whose packets likewise must be forwarded. If a rule is defined for an outgoing connection, which permits an access, then the rule automatically applies for the corresponding return packets. For the communication partner a Stateful Inspection connection is represented as a direct line, which can only be used for an exchange of data that corresponds to the agreed rules.

The firewall rules can be configured dynamically, i.e. it is not necessary to stop the software or restart the system.

The firewall settings in the configuration menu of the Client Monitor permit a more precise specification of firewall filtering rules. They have a global effect. This means that regardless of the currently selected destination system, the rules of the extended firewall settings are always worked through first, before the firewall rules from the telephone book are applied.

A combination of the global and link based firewall can be quite effective in certain scenarios. However generally, the global setting possibilities should be able to cover virtually all requirements.

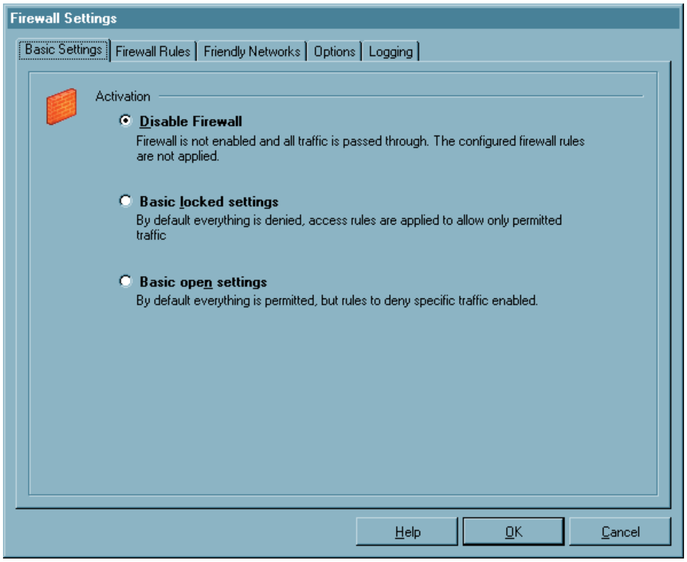
Please note that the link-based firewall settings take priority over the global firewall settings at activation. For instance if the Link Firewall is set to "Always" and "Only allow communication in the tunnel", then in spite of global configuration rules that may possibly be different, only one tunnel can be set-up for communication. All other traffic will be rejected by the Link Firewall.

Configuration of the firewall settings

The filter rules of the firewall can be defined application-based as well as (additionally) address-oriented, relative to friendly/unknown networks.

To avoid any conflict between the rules of the Link Firewall in the phonebook and the global firewall, we recommend to switch off the Link Firewall when using the advanced global firewall. The IP addresses of the respective links (to the VPN gateway) can be inserted in the filter rules of the global firewall.

Configurationfield Basic Settings



Activation

● **Disable Firewall**
Firewall is not enabled and all traffic is passed through. The configured firewall rules are not applied.

○ **Basic locked settings**
By default everything is denied, access rules are applied to allow only permitted traffic

○ **Basic open settings**
By default everything is permitted, but rules to deny specific traffic enabled.

In the basic settings you decide how the extended firewall settings will be used.

Disable Firewall

If the extended firewall is deactivated, then only the firewall configured in the telephone book will be used. This means that all data packets will only be worked through via the security mechanisms of this connection-oriented firewall, if they have been configured.

Basic locked settings (recommended)

If this setting is selected, then the security mechanisms of the firewall are always active. This means that without additionally configured rules all IP data traffic will be suppressed.

The exception are the data packets that are permitted (permitted through) by the separately created active firewall rules (Permit Filter). If a characteristic of a data packet meets the definition of a firewall rule, then at this point the work through of the filter rules is ended and the IP packet is forwarded.

In the blocked basic setting mode in a convenient manner an L2Sec/IPSec tunnel connection is released.

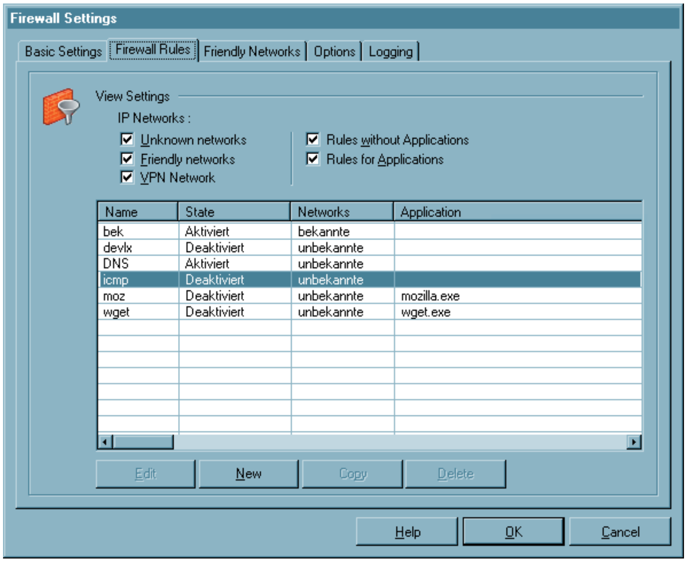
For this, the data traffic can be globally permitted in the configuration field “Options”, via VPN protocols (L2Sec, IPSec).

Basic open settings

In the open base setting all IP packets are first permitted. Without additional filter rules all IP packets are forwarded.

The exception are the data packets that are filtered out (not permitted through) by the separately created active firewall rules (Deny Filter). If one of the characteristics of an IP packet coming into the server/client meets the definition of a Deny Filter, then at this point the working through of filtering rules ends, and the IP packet will not be forwarded. Data packets that do not meet a suitable Deny Filter are forwarded.

Configurationfield Firewall Rules



View Settings

IP Networks :

☑ Unknown networks
☑ Friendly networks
☑ VPN Network
☑ Rules without Applications
☑ Rules for Applications

Name	State	Networks	Application
bek	Aktiviert	bekannte	
devlx	Deaktiviert	unbekannte	
DNS	Aktiviert	unbekannte	
icmp	Deaktiviert	unbekannte	
moz	Deaktiviert	unbekannte	mozilla.exe
wget	Deaktiviert	unbekannte	wget.exe

The rules for the extended firewall are brought together in this configuration field. The display options are all active by default and correspond to the selected networks, for which the respective rule can be defined, and whether this rule will be valid regardless of application:

– Unknown networks
– Friendly networks
– VPN networks
– Rules with applications
– without applications

These selection fields for the displays of rules are only for overview purposes and have no effect on the application of a filter rule. The most important characteristics are displayed for each defined rule:

– Name
– State
– Networks

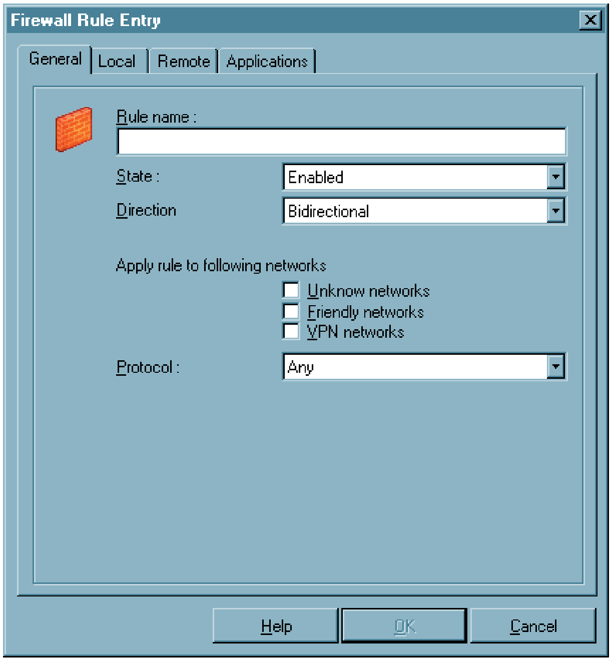
Clicking on these characteristic buttons sorts the displayed rules.

Creating a firewall rule

Use the buttons underneath the display line to generate or edit the rules. To create a firewall rule click on “New”. A filter rule is created via four configuration areas or tabs:

– General: In this configuration field you specify the network and the protocol for which the rule will apply.
– Local: Enter the values of the local ports and IP addresses in this configuration field.
– Remote: Enter the port and address values of the other side in the remote field.
– Applications: In this configuration field the rule can be assigned to one or more applications.

Firewall rule / General



Rule name :

State : Enabled

Direction Bidirectional

Apply rule to following networks

□ Unknow networks
□ Friendly networks
□ VPN networks

Protocol : Any

The created rule is always executed as an exception to the basic setting (see → Basic Settings).

Rule name

The rule appears under this name in the display list.

State

The rule will only be applied to data packets, if the status is “active”.

Direction

With the direction you specify whether this rule will apply for incoming or outgoing data packets. According to the Stateful Inspection principle, data packets are received that come in from a destination, to which data packets may be sent and vice versa. However Stateful Inspection is only used for TCP/IP protocols (UDP, TCP).

You can switch to “incoming” for instance if a connection will be set-up from the remote side (e.g. for “incoming calls” or administrator accesses).

The “bi-directional” setting is only practical if Stateful Inspection is not available, e.g. for the ICMP protocol (for a ping).

Apply rule to following networks

When creating a rule, at first do not assign it to any network. A rule can only be saved if the desired allocation has been made and if a name has been assigned.
Unknown networks
– are all networks (IP network interfaces), that can neither be allocated to a known nor VPN. These include for example connections via the Microsoft remote data transmission network or also direct or unencrypted connections with the integrated dialer of the client, as well as Hotspot WLAN connections. If a rule will apply for unknown networks then this option must be activated.

Known networks
– are defined in the tab of the same name in the “Firewall settings” window. If a rule will apply for known networks then this option must be activated.
VPN networks
– are all L2Sec or IPSec connections in the set-up condition. Moreover under this group there are also all encrypted direct dial-in connections via the client’s integrated dialer. If a rule will apply for VPN networks then this option must be activated.

Protocol

Select the appropriate protocol depending on the application:

TCP, UDP, ICMP, GRE, ESP, AH, IGRP, RSVP, IPv6 or IPv4, all

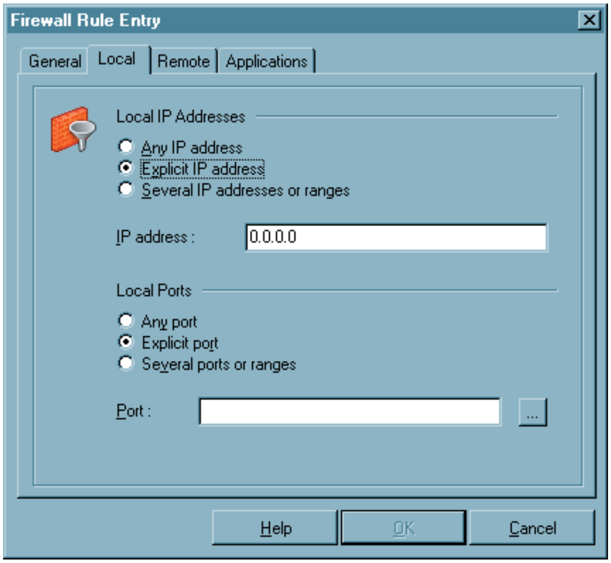
Line management

Use this parameter to influence the type of connection.

For example, you select the option that the rule configured here “is only valid at inactive VPN connection”, if you an Internet connection with concurrently present VPN connection to be excluded, otherwise the Internet connections to unknown networks should be allowed. For this, this rule for “unknown networks” must be used, i.e. this rule must permit access to unknown networks.

The option, “no automatic connect” is only practical if in the telephone book the connection set-up has been set to “automatic” in the “Line Management” parameter field. For the data packets defined via this rule, automatic connection set-up does not take place when activating this function, it does for other data packets.

Firewall rule / Local



Firewall Rule Entry

Local IP Addresses

○ Any IP address
● Explicit IP address
○ Several IP addresses or ranges

IP address : 0.0.0.0

Local Ports

○ Any port
● Explicit port
○ Several ports or ranges

Port :

On this tab the filter are set for the local IP addresses and IP ports.

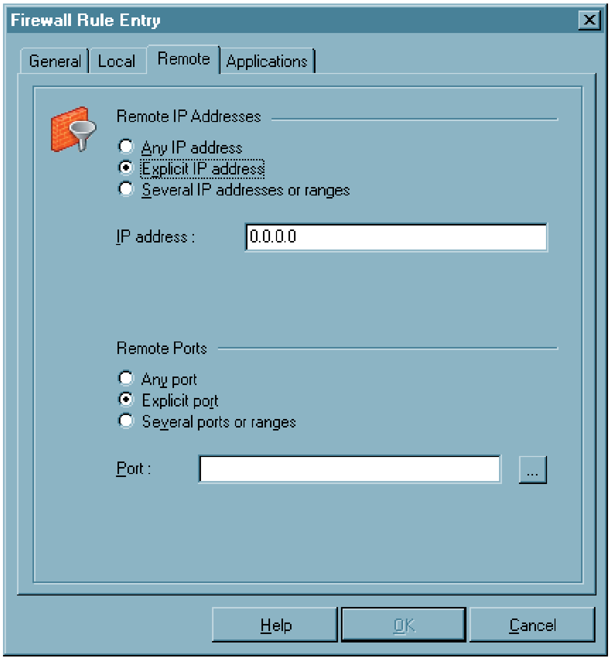
If the basic setting is blocked then those data packets will be let through to the outside by the firewall whose source address agrees with the address under “Local IP address” or is within the range of validity. Of the incoming data packets those are let through whose destination address agrees with the address under “Local IP addresses” or is within the validity area.

The same is true for blocked basic setting with the IP ports. Those data packets are permitted outside by the firewall whose source port falls under the definition of the local port. Of the incoming data packets those are let through whose destination port falls under the definition of the local port.

All IP addresses
– includes all source IP addresses of outgoing packets or destination IP addresses of incoming packets, regardless of the local network adapter.
Unique IP address
– is the IP address defined for the local network adapter. It can be assigned to the address of the Ethernet card, the WLAN card, or it can also be assigned to the VPN adapter.
Multiple IP addresses
– designates an address range or pool. For example this can be the IP address pool, from which the address assigned by the DHCP server to the client originates.

All ports
– allows communication via all source ports for outgoing packets and destination ports for incoming ports.
Unique port
– This setting should only be used if this system makes a server service available (e.g. remote desktop on port 3389).
Multiple ports
– This setting should only be used if the local ports can be combined in a range, that is required by a services that will be made available on this system (e.g. FTP ports 20/21).

Firewall rule / Remote



Remote IP Addresses

○ Any IP address
● Explicit IP address
○ Several IP addresses or ranges

IP address : 0.0.0.0

Remote Ports

○ Any port
● Explicit port
○ Several ports or ranges

Port :

On this tab the filters are set for the remote IP addresses and IP ports.

If the basic setting is blocked then those data packets will be let through to the outside by the firewall whose destination address agrees with the address under “Local IP address” or is within the range of validity. Of the incoming data packets those are let through whose source address agrees with the address under “Local IP addresses” or is within the validity area.

The same is true for blocked basic setting with the IP ports. Those data packets are permitted outside by the firewall whose destination port falls under the definition of the local port. Of the incoming data packets those are let through whose source port falls under the definition of the local port.

With the settings under remote IP address you can specify the remote IP addresses with which the system may communicate.

All IP addresses
– permits communication with any IP address of the other side, without limitation.
Unique IP address
– only allows communication with the IP address on the other side specified here.
Multiple IP addresses / IP ranges
– permits communication with different IP address on the other side according to the entries.

With the settings under remote ports, you can specify the ports via communication with remote systems is permitted.

All ports
– sets no limitations whatsoever relative to destination port for outgoing packets or source port for incoming packets.

Unique port
– only allow communication via the specified port, if this port if it is present al destination port in the outgoing data packet, or if it is present a source port in the incoming packet. If for example a rule only permits Telnet to a different system, then port 23 must be entered here.
Multiple ports / ranges
– can be used if multiple ports will be used for a rule (e.g. FTP port 20/21).

Configurationsfield Friendly Networks

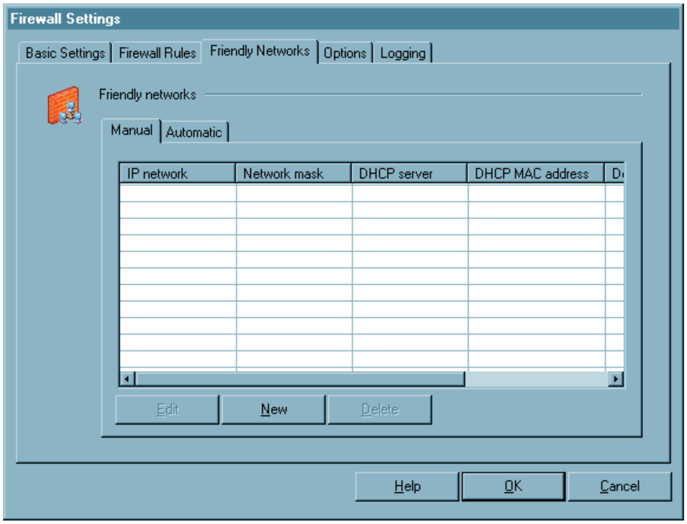
If in “Firewall rules” you have defined in the configuration field, that a rule will be applied to connections with known network, then this rule is always used, if a network can be identified as known network according to the criteria that is entered here, e.g. the LAN adapter is in a known network.

The administrator centrally specifies what constitutes a Friendly Net. A Friendly Net is indicated in the monitor by the Firewall icon, which is green as soon as the Client has dialed-in to a Friendly Net.

The manual definition of a known network by the administrator and the automatic detection of a known network via Friendly Net Detection are not mutually exclusive, rather they can be used concurrently and they can be configured via the “Manual” and Automatic" tabs.

The signal on the tray icon and on the application icon indicates an active firewall in red, with Friendly Net it is indicated in green.

Manual



If in “Firewall rules” you have defined in the configuration field, that a rule will be applied to connections with known network, then this rule is always used, if a network can be identified as known network according to the criteria that is entered here, e.g. the LAN adapter is in a known network.

The LAN adapter of the client is considered to be in a known network if:

[IP network and Network mask]

– the IP address of the LAN adapter originates from the specified network range. If for example the IP network 192.168.254.0 is specified with the mask 255.255.255.0, then the address 192.168.254.10 would effect an allocation to the known network.

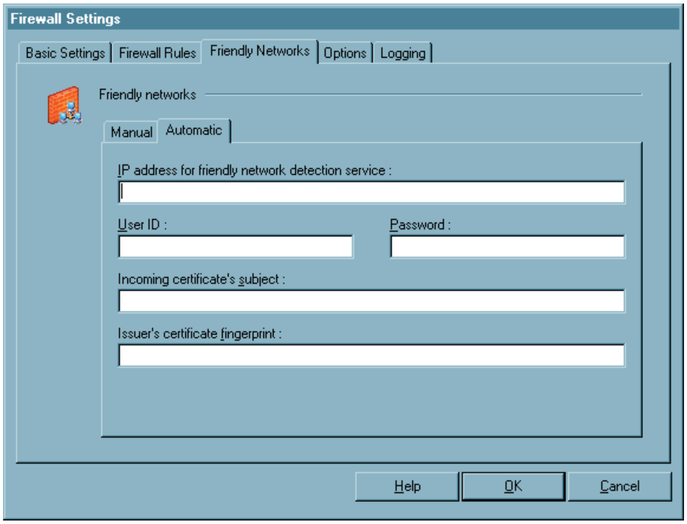
[DHCP server]

– the IP address has been assigned by the DHCP server that has the IP address specified here;

[DHCP MAC address]

– if this DHCP server has the MAC address specified here. This option can only be used if the DHCP server is located in the same IP subnet as the DHCP client.
The more of these conditions that are fulfilled the more precise the verification that a known network is involved.
The allocation of an adapter to unknown or known network is automatically logged in the log window of the Client Monitor and in the log file of the firewall (see → Logging).

Automatic


Firewall Settings

The administrator centrally specifies what constitutes a Friendly Net. A Friendly Net is indicated in the monitor by the Firewall icon, which is green as soon as the Client has dialed-in to a Friendly Net.

IP address of the friendly net detection service

A Friendly Net Detection Server (FNDS) is required; this is an NCP software component that must be installed in a network that is defined as “Friendly Net”. This Friendly Net Detection Server must be reachable via IP, and its IP address must be entered here.

User ID, Password (FNDS)

The Friendly Net Detection Server is authenticated via MD5 or TLS. The user ID and password entered here must agree with those that have been stored on the FNDS.

Incoming Certificate’s Subject (User)

The incoming certificate of the FNDS is checked for this string. It a Friendly Net only if there is agreement.

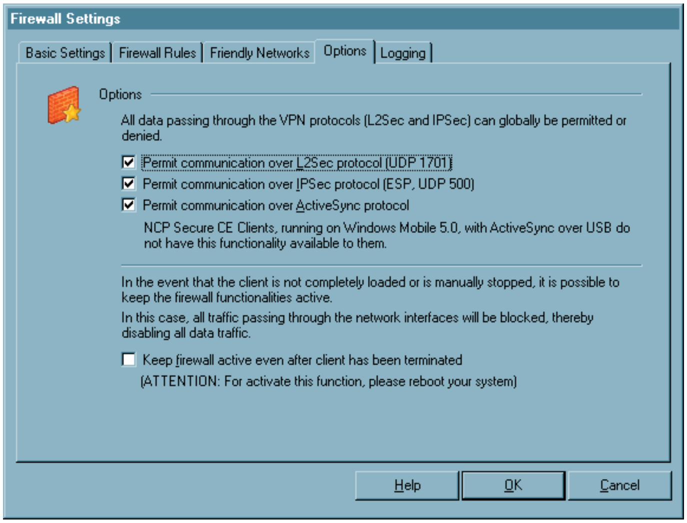
Issuer’s Certificate Fingerprint

In order to offer maximum security against counterfeiting, the fingerprint of the issuer certificate must be capable of verification. It must agree with the hash value entered here.

Friendly Net Detection via TLS

If the Friendly Net will be detected via TLS, (including authentication via the issuer certificate fingerprint), then this issuer certificate must be located in the “CaCerts” program directory, and its fingerprint must agree with the fingerprint configured here.

Configurationsfield Options



Options

All data passing through the VPN protocols (L2Sec and IPSec) can globally be permitted or denied.

☑ Permit communication over L2Sec protocol (UDP 1701)

☑ Permit communication over IPSec protocol (ESP, UDP 500)

☑ Permit communication over ActiveSync protocol

NCP Secure CE Clients, running on Windows Mobile 5.0, with ActiveSync over USB do not have this functionality available to them.

In the event that the client is not completely loaded or is manually stopped, it is possible to keep the firewall functionalities active.

In this case, all traffic passing through the network interfaces will be blocked, thereby disabling all data traffic.

☐ Keep firewall active even after client has been terminated

(ATTENTION: For activate this function, please reboot your system)

With blocked basic setting the set-up of VPN connections via the “Options” tab can be globally permitted.

The following protocols and ports required for the tunnel set-up are released per generated filter:

For L2Sec: UDP 1701 (L2TP), UDP 67 (DHCPS), UDP 68 (DHCPC)
For IPSec: UDP 500 (IKE ISAKMP), IP-protocol 50 (ESP), UDP 4500 (NAT-T), UDP 67 (DHCPS), UDP 68 (DHCPC)
For ActiveSync: TCP 990, 999, 5678, 5679

The (global) firewall must be released for ActiveSync in the case of a direct connection (via USB, serial or infrared). This is done in the firewall settings of the monitor under “Options - Permit ActiveSync connections (TCP 990, 999, 5678, 5679, 26675, 5721)”. This setting can also be made on the PDA via the popup menu, if the (global) firewall is active. If ActiveSync is operated via network (LAN or WLAN) then in addition a separate firewall rule for name resolution (DNS/WINS) must be created.

This global definition saves you the set-up of dedicated single rules for the respective VPN variants.

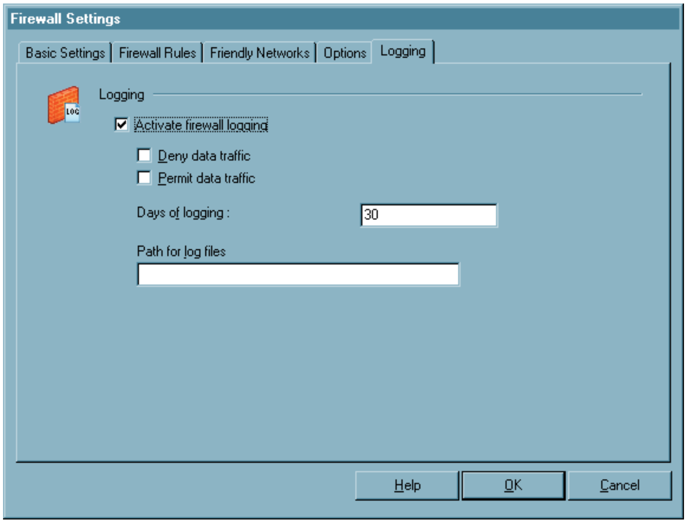
Please note that only the tunnel set-up is enabled with this. If no additional rules exist for VPN networks, that permit a communication in the tunnel, then no data transfer can occur via the VPN connection.

Continue to activate firewall with stopped client

The firewall can also be active if the client is stopped, if this function is selected. In this state however each incoming and outgoing communication is suppressed, so that no data traffic at all is possible, as long as the client is deactivated.

If the above mentioned function is not used and the client is stopped, then the firewall will also be deactivated.

Configurationsfield Logging



Logging

☑ Activate firewall logging

☐ Deny data traffic

☐ Permit data traffic

Days of logging : 30

Path for log files

The activities of the firewall are written to log file depending on the setting. The default location of the “Output directory for log files” is in the installation directory under \log.

The log files for the firewall are written in pure text format and are named Firewallyymmdd.log. They contain a description of “rejected data traffic” and or “Permitted data traffic”. If neither of these options has been selected then only status information on the firewall will be logged.

The log files are written at each start of the firewall. The maximum number is maintained in the log directory, as has been entered as number of the “Days for logging”.

Note: Activating the Logging will decrease the performance. For each packet corresponding to this setting, an according log text has to be written.

4.2.3 Certificate Configuration

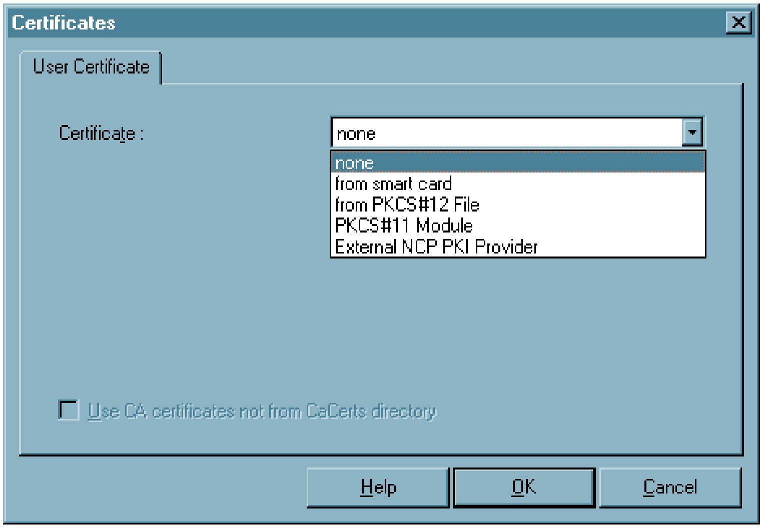
By clicking on the menu item "Configuration – Certificates" you can first determine whether you want to use the certificates, and thus the "Extended Authentication", and where you want to store the user certificates. The PIN entry policies and the interval of validity are specified in a second parameter field.

Certificates are normally created by a CA (Certification Authority) utilizing some sort of PKI-based architecture and they may be implemented on a Smart Card in addition to a digital signature(s). Such Smart Cards represent an individual "personal identity card". You can use certificates with the length of the private key up to 2048 Bits.

The system monitors whether the PKCS#12 file is present. If, for example, this file is stored on USB stick or an SD card, then after pulling out the SD card the PIN is reset and an existing connection is disconnected. This process corresponds to the "Connection disconnect when smart card is removed", which can be set when using a smart card, under "Configuration, Certificates" in the monitor menu. If the SD card is later re-inserted, then the connection can be restored, after another PIN entry.

The environment variables (users) of the operating system can be inserted in the certificate configuration. The variables are changed when closing the dialog, and when copying the telephone book, and they are written back into the configuration. If an environment variable does not exist, then it is removed from the path when converted, and a log entry is written into the logbook. If a % sign (syntax), is missing then the variable remains, and a log entry is written, as above.

User Certificate



Certificates

User Certificate

Certificate : none

none
from smart card
from PKCS#12 File
PKCS#11 Module
External NCP PKI Provider
□ Use CA certificates not from CaCerts directory
Help
OK
Cancel

Certificate

By choosing "Certificate" from the submenu you can determine whether or not you want to use the certificate and thus use the "Extended Authentication".

None: The default value is "None", indicating that no certificates will be used

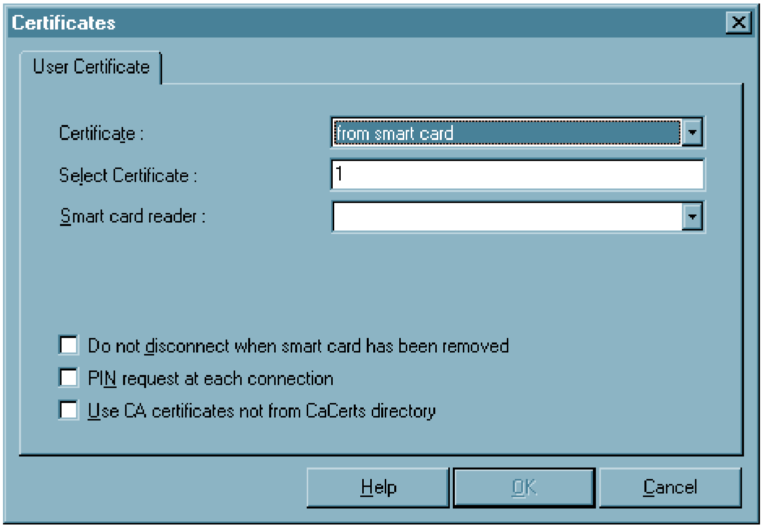
from Smart Card: Select "from Smart Card Reader" in the list in conjunction with "Extended Authentication" in order for the respective Certificate of your Smart Card to be read by the Smart Card Reader.

from PKCS#12 File: Select "from PKCS#12 File" in the list in conjunction with "Extended Authentication" in order for the respective Certificate of your Smart Card to be read from a file on the harddisc of your PC.

from PKCS#11 Module: Select "from PKCS#11 Module" from the list in conjunction with "Extended Authentication" in order select a Certificate to be read via the defined cryptographic interface.

External NCP PKI provider: An external NCP PKI provider designates an NCP-specific interface for special requirements.

Smart Card Reader



Certificate : from smart card

Select Certificate : 1

Smart card reader :

□ Do not disconnect when smart card has been removed

□ PIN request at each connection

□ Use CA certificates not from CaCerts directory

The software automatically supports all chip card readers that are PC/SC conformant. If you want to use certificates from the Smart Card with your reading device, then select your Smart Card Reader from the list box.

Please note that the chip card reader can only be selected if it has been installed on the PDA and the NCP Client Service on the PDA has been started at least once. (see → Prerequisites for the Strong Security Version)

The name of a smart card reader is specified in the configuration. If you subsequently use a different reader then the name is different and the reader will not be found. For two readers that only differ in firmware, (and which consequently have a different name), this may not be desired. For instance:
SpringCard GCR-R1.44-GI slot A
SpringCard GCR-R1.44-GI slot A
→ for the above example the following reader name can be entered with an asterisk (*) as wildcard: SpringCard*

Certificate Selection

1. Certificate... (default = 1) Up to three different certificates that are on the Smart Card can be selected from the list box. The number of certificates on the Smart Card depends on the Registration Authority. For further information please consult your system administrator.

Example:

On the Smart Cards of Signtrust and NetKey 2000 there are located three certificates:
(1) for signification
(2) for encryption and decryption
(3) for authentication (NetKey 2000 option)

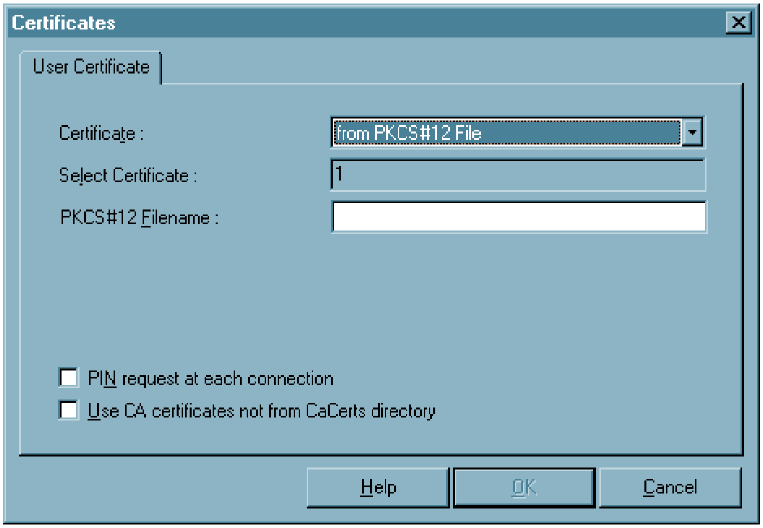
- ### Do not disconnect when Smart Card is removed

The connection is not necessarily broken off when the Smart Card is removed. Whether “Do not disconnect when Smart Card is removed” occurs is set via the main menu of the monitor under this menu item.

- ### PIN request at each connection

You can specify that the PIN must be entered correctly, not only after each initial connection establishment after booting the PC, but rather before any connection establishment. This functionality can be used for all connection modes (manual, automatic, alternating).

PKCS#12 File



Certificate : from PKCS#12 File

Select Certificate : 1

PKCS#12 Filename :

□ PIN request at each connection

□ Use CA certificates not from CaCerts directory

If you use the PKCS#12 format, then you will receive a file from your system administrator that must be copied onto the PDA (see → transfer PKCS#12 file onto the PDA). In this case path and Filenames of the PKCS#12 file must be entered.

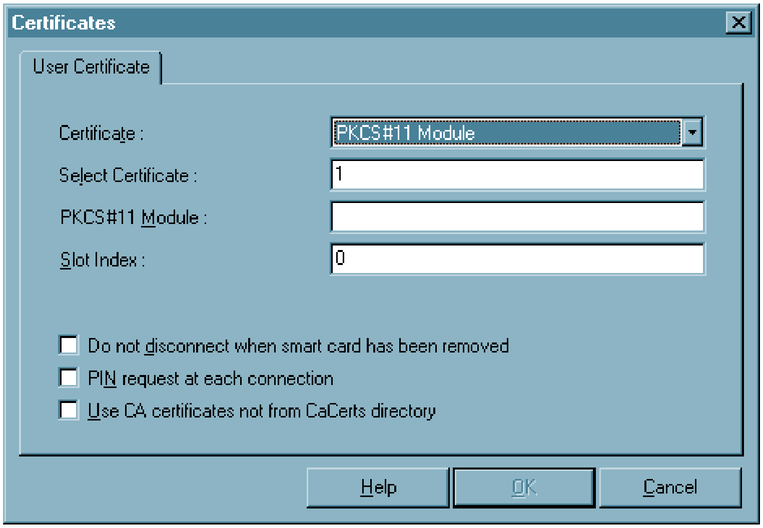
PKCS#12 Filename

Please note: Path and name for the PKCS#12 file required for the configuration must agree with the location of the file on the PDA!

The menu item “Configuration – Transfer PKCS#12-file to the PDA” in the configurator of the PC component can be used for transferring the PKCS#12 file. If this function is used, then the path can be specified as follows:

```
%INSTALLDIR%\certs\<PKCS#12-file name>
```

PKCS#11 Module



Certificates

User Certificate

Certificate : PKCS#11 Module

Select Certificate : 1

PKCS#11 Module :

Slot Index : 0

□ Do not disconnect when smart card has been removed

□ PIN request at each connection

□ Use CA certificates not from CaCerts directory

A driver is supplied along with the smart card or the token in the form of a PKCS#11 library (DLL). This driver software must first be installed on the PDA. This means that the DLL will be stored in a directory on the PDA depending on the manufacturer. This directory is usually the Windows directory. If the DLL is stored there, then it suffices to enter the name of the DLL in the PKCS#11 module field (see the example in the above Fig. “aetpkss1.dll”. If the DLL is stored in a different directory when it is installed, then the complete path name must be specified.

Alternatively the NCPPKI.CONF file can be edited. It is located in the installation directory on the PDA (\programs\ncp secure ce client). For editing, the file must be copied onto the PC manually. Under “Interfaces” set “PKCS11=1", as module name, enter an ID for the connected reader, and enter the name of the associated driver file as PKCS11-DLL (”aetpkss1.dll" in the example below).

```
[General]
LogLevel=
LogFile=

[Interfaces]
CTAPI=0
PCSC=1
PKCS11=1

[PKCS11 1]
ModulName       = A.E.T. SafeSign (PKCS11)
PKCS11-DLL      = aetpkss1.dll

Slotindex       = 1
```

After editing, the NCPPKI.CONF file must be copied back onto the PDA. Then you must execute a soft reboot of the PDA and restart the NCP Client Service. Once the card reader data have been refreshed (see below) the PKCS#11 module is available in the configurator as “smart card reader” (see above).

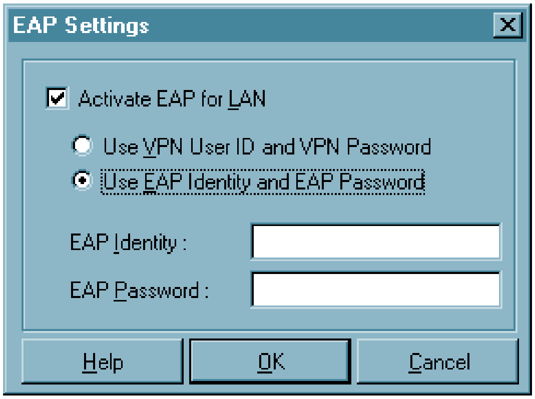
Slotindex

Usually the slotindex is “0". If this value deviates in the associated description, then it can only be changed via the NCPPKI.CONF file.

Use CA Certificates not from CACerts directory

When activating this function, an alternate CA Certificate e.g. from chipcard is to be used, not the CA Certificate of the local directory on the PDA. This cerificate must be the one which is used for verifying against the incoming server certificate.

4.2.4 EAP Settings



EAP Settings

☑ Activate EAP for LAN

○ Use VPN User ID and VPN Password
● Use EAP Identity and EAP Password

EAP Identity :
EAP Password :

Use of the Extended Authentication Protocol Message Digest5 (EAP MP5) can be specified via the main menu of the configurator under “Configuration - EAP Settings”. This protocol can then be used if a switch, a hub, or if an access point is used, which support 802.1x and the according Authentication Mode for the access to the wireless LAN.

You can prevent unauthorized users from getting into the LAN via the hardware interface with the Extended Authentication Protocol (EAP MP5).

You can use either “VPN User ID” with “VPN Password” or your own “EAP Identity” with an “EAP Password”.

Certificate content can be automatically transferred if in the Phonebook under “Tunnel Parameters” VPN User ID and VPN Password are transferred from the certificate, and if “Use VPN User ID and VPN Password” is activated in the EAP options.

For EAP-TLS (with certificate) now the EAP user name can be directly referenced from the certificate configuration. The following content of the configured certificate can be used by entering the appropriate placeholders in the EAP configuration:

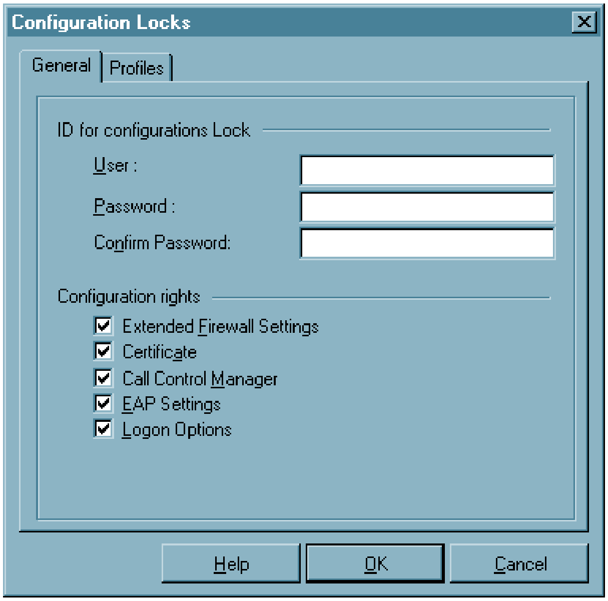
```
Commonname : %CERT_CN%
E-mail : %CERT_EMAIL%
```

4.2.5 Configuration Locks

Use configuration locks to modify the configuration main menu in the monitor in such a way that the user can no longer modify the pre-set configurations, or so that selected parameter fields are no longer visible for the user.

The configuration locks are enabled after applying the defined settings with “OK”. Clicking the cancel button the default settings will be used.

■ General | Configuration Locks



ID for configurations Lock

User :

Password :

Confirm Password:

Configuration rights

☑ Extended Firewall Settings
☑ Certificate
☑ Call Control Manager
☑ EAP Settings
☑ Logon Options

In order to effectively specify the configuration blocks, identification must be entered, which consists of “User ID” and “Password”. The password must be confirmed thereafter.

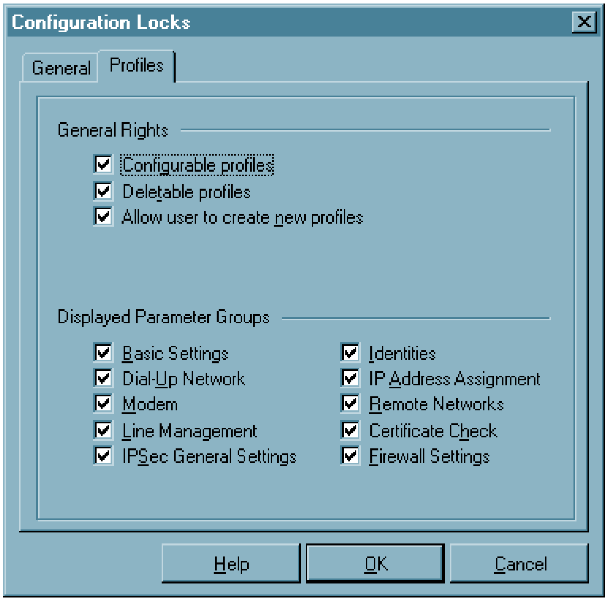
Please note that identification is absolutely necessary for the configuration block, in order to activate the blocks, or to cancel the configuration blocks. If the identification is forgotten there is no other possibility to cancel the blocks!

Now authorization to open menu items under the main menu item, “Configuration”, can be limited for the user. As standard, the user can open all menu items and edit the configurations. If the check mark is removed from the respective menu item with a mouse click, then the user can no longer open this menu item.

Profiles | Configuration Locks

The editing rights for the parameters in the profile settings are divided into two groups:

– General rights
– Visible profile parameter fields



General Rights

☑ Configurable profiles
☑ Deletable profiles
☑ Allow user to create new profiles

Displayed Parameter Groups

☑ Basic Settings
☑ Dial-Up Network
☑ Modem
☑ Line Management
☑ IPSec General Settings
☑ Identities
☑ IP Address Assignment
☑ Remote Networks
☑ Certificate Check
☑ Firewall Settings

General rights

The general rights refer only to (configuration of) the profiles. If you specify “Profiles may be created”, then “Profiles may be configured”, however remains excluded, thus while new profiles can indeed be defined with the assistant, subsequent modification of individual parameters will then no longer be possible.

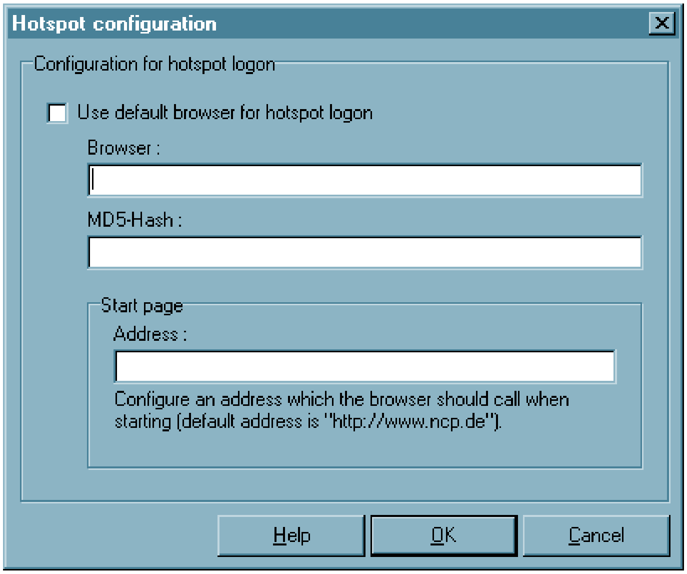
Visible profile parameter fields

The parameter fields of the profile settings can be suppressed for the user.

Please note as well that parameters of a non-visible field cannot be configured.

4.2.6 Hotspot

The following settings for HotSpot Logon are possible:



Hotspot configuration

Configuration for hotspot logon

□ Use default browser for hotspot logon

Browser :

MD5-Hash :

Start page

Address :

Configure an address which the browser should call when starting (default address is "http://www.ncp.de").

- ### Use default browser for hotspot logon

(Default setting). If the check mark is removed from the checkbox then a different browser can be specified by entering of its path on the PDA.

The alternative browser can be especially configured for the requirements at hotspots. Specifically no proxy server will be installed and all active elements (Java, JavaScript, ActiveX) will be deactivated. (The alternative browser is not part of the Client software!)

- ### MD5-Hash

In addition the MD5 hash value of the browser exe file can be determined and entered in the “MD5 Hash” field. In this manner the system ensures that a hotspot connection is only realized with this browser.

- ### Start Page / Address

Under “Start Page / Address” the start page described above is entered in the form: http://www.mycompagnie.de/error.html.

4.2.7 Transfer PKCS#12 File

After clicking on this menu item, the PKCS#12-file can be transferred from the PC onto the PDA device.

For this, first a selection window opens in which the desired PKCS#12 file must be selected.

Insure that the physical connection between PDA and PC is established and that ActiveSynch is started.

4.2.8 Transfer CA Certificate

Use this menu item in the user interface of the PC component to copy CA certificates into the “cacert” directory on the PDA.

Insure that the physical connection between PDA and PC is established and that ActiveSynch is started.

4.2.9 Refresh Modem Data

Use this menu item in the user interface of the PC component to generate the file for modem data (MODEM.INI) and to copy it from the PC to the PDA.

Insure that the physical connection between PDA and PC is established and that ActiveSynch is started.

4.2.10 Refresh Reader Data

Use this menu item in the user interface of the PC component to copy the file for the Smart Card reader (READER.INI) from the PC to the PDA.

Insure that the physical connection between PDA and PC is established and that ActiveSynch is started.

4.2.11 Profile Settings Backup

If a secure profile setting has not yet been generated, for instance in the case of a first installation, then a first profile setting (NCPPHONE.SAV) will automatically be created.

- **Create [Profile Settings Backup]**

A profile setting backup will be created after each click on the "Create" menu item, and after a confirmation question, that contains the configuration up to this point.

- **Restore [Profile Settings Backup]**

The last profile setting backup will be read in after each click on "Restore". Thus, changes in the configuration that have been made since the last profile setting backup will be lost.

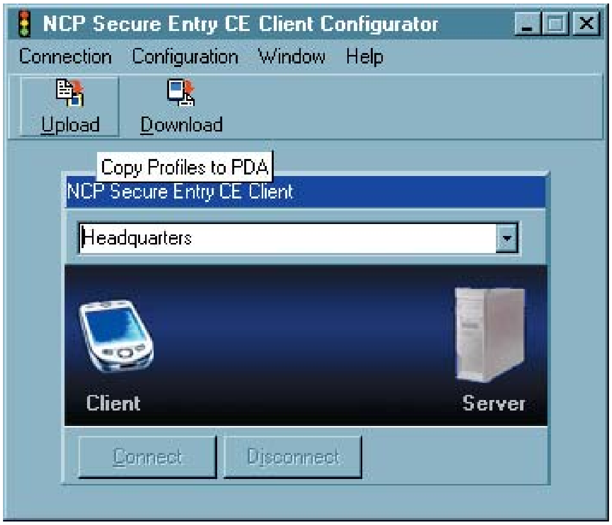
4.3 Window – Language

Under the menu item “Window” you can switch back and forth between German and English by clicking on Language. We ship the system with German as the default language setting.

4.4 Help – Info

Under the menu item help, you can find the version number of your implemented software by clicking on “Info”.

4.5 Uploading the Profile Settings



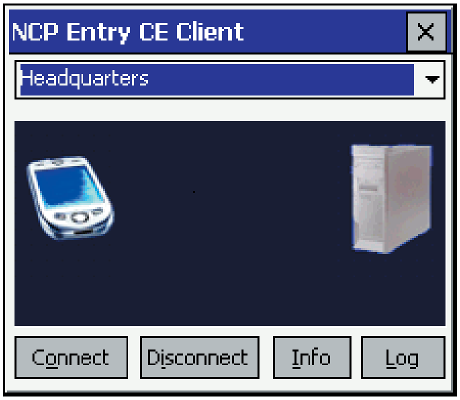
After the configuration of a destination system has been concluded and the profile settings have been completed, then the profiles must be copied onto the PDA.

Activate the upload button to do this.

Please insure that ActiveSynch correctly establishes the connection to the PDA.

The NCP Client Service and the NCP Client Configurator on the PDA must not be started.

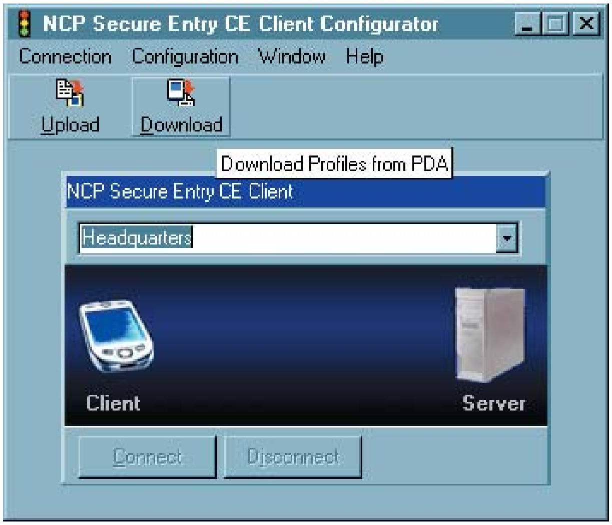
Please be aware however that a possibly existing VPN connection can be disconnected by the upload without warning.



After the upload has been successfully executed the same name must be in the destination selection in the PDA monitor as is found in the PC configurator.

Please note that a possible, previously existing profile setting can be overwritten on the PDA without warning.

4.6 Downloading the Profile Settings


NCP Secure Entry CE Client Configurator
Connection
Configuration
Window
Help
Upload
Download
Download Profiles from PDA
NCP Secure Entry CE Client
Headquarters
Client
Server
Connect
Disconnect

A download of the profile settings from PDA onto the PC is always required when changes must be made in the configuration of a destination system.

Activate the download button for this.

Please insure that ActiveSynch correctly establishes the connection to the PDA.

The profile settings on the PC will be overwritten when the profiles are downloaded from the PDA.

In order to keep the existing profile setting on the PC, it must have been saved separately. It is located in the directory:

```
\Programs\ncp\ceclient\bin\ncpphone.cfg
```

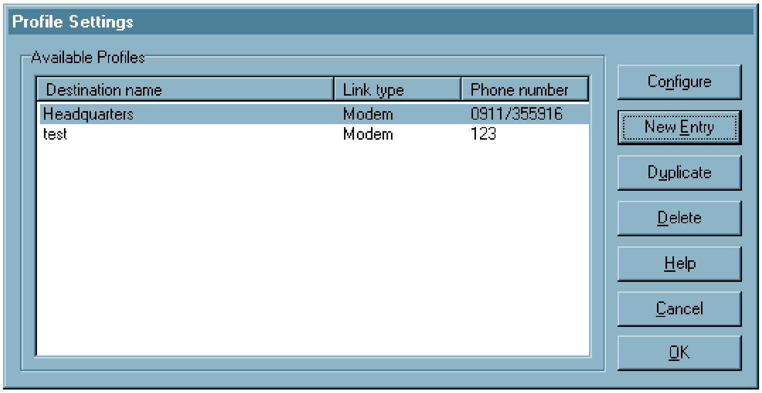
5. Configuration Parameters

With the IPSec client you can define and configure numerous individual profiles for corresponding destinations, in accordance with your communication requirements.

In this section all parameter descriptions are listed and they are arranged in the same sequential order as displayed in the monitor.

5.1 Profile Settings

Upon clicking “Profile Settings” in the monitor menu, the menu is opened with an overview of the definied profiles and the phonenumbers of the assigned destinations.



Destination name	Link type	Phone number
Headquarters	Modem	0911/355916
test	Modem	123

The buttons located to the right can be used to add, remove, copy and modify the entries of the profiles.

In order to define a new profile click on “Profile Settings” in the monitor menu under “Configuration”. Upon doing so the menu opens displaying any defined profiles. Click on “New Entry”. Enabeling the “Configuration Assistant”, which assists in the creation of a new profile definition. All other parameters will be assigned default values.

To edit these default values, in order to fulfill the requirements of the profile, select the desired profile and then “Configure” to gain access to the individual parameters. (See → Profile Settings, Configure)

In order to duplicate a profile click on “Duplicate”

In order to delete a profile click on “Delete”.

Parameterfolders:

Parameters which specify the connection via the profile to the destinations, are found in the configuration folders. The name of the profile appears in the titel bar (see → Profile Settings, Configure). Within the configuration folder the connection parameters pretaining to this profile can be configured.

1 ***Basic Settings***

2 ***Dial-Up Network***

3 ***Modem***

4 ***Line Management***

5 ***IPSec General Settings***

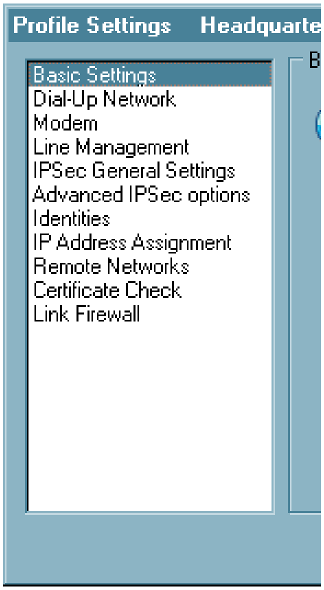
6 ***Identities***

7 ***IP Address Assignment***

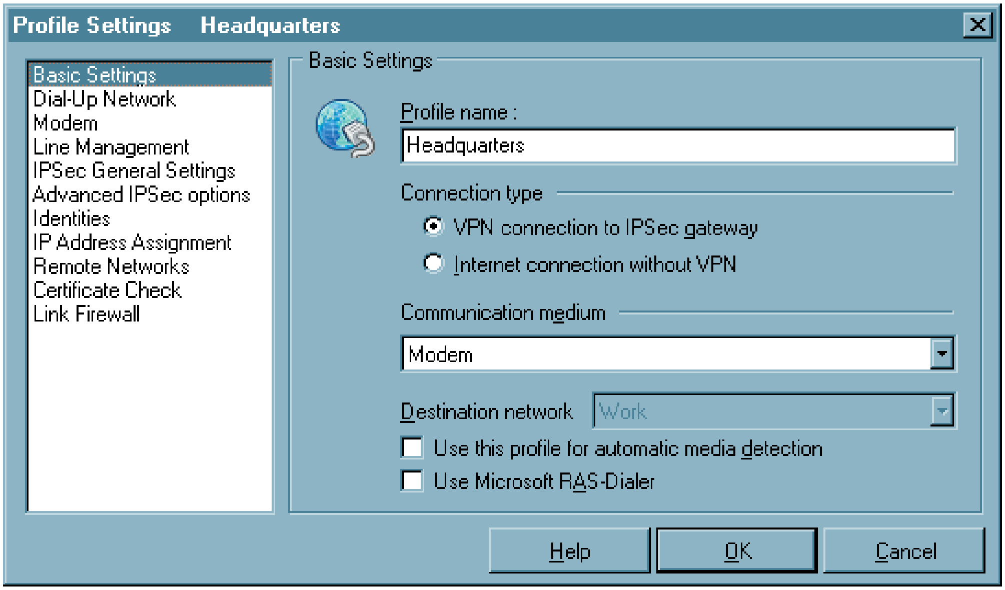
8 ***Remote Networks***

9 ***Certificate Check***

10 ***Link Firewall***



5.1.1 Basic Settings



Basic Settings

Profile name : Headquarters

Connection type

● VPN connection to IPSec gateway

○ Internet connection without VPN

Communication medium: Modem

Destination network: Work

□ Use this profile for automatic media detection

□ Use Microsoft RAS-Dialer

In the folder "General" enter "Profile name", the "Communication type" and the "Communication medium" you wish to use and is available to Windows.

Parameters:

□ Profil name

□ Connection type

□ Communication medium

□ Destination network

□ Use this profile for automatic media detection

□ Use Microsoft RAS-Dialer

■ Profile name

When entering new profiles you should enter a unique name for each profile. The profile name may include any character or number as desired up to a maximum of 39 characters (including spaces).

■ Connection type

Alternatively there are two connection types available with the IPSec client:

VPN to IPSec correspondent:

In this case you dial into the corporate network (or into the gateway) with the IPSec client. A VPN tunnel is set up for this.

Internet connection without VPN:

In this case only use the IPSec client for dialing into the Internet. Here the Network Address Translation (IPNAT) continues to be used in background so that only those data packets are accepted that have been requested.

■ Communication medium

You can select the communication medium for each profile, provided that you have the required device installed on your PC and recognized by Windows.

Modem:

Hardware: Asynchronous modem (PCMCIA modem, GSM adapter)
with COM Port support;
Network: PSTN (also GSM);
Remote destination: Modem or ISDN device with digital modem;

LAN (over IP):

Hardware: LAN adapter;
Networks: Ethernet or Token Ring based LAN;

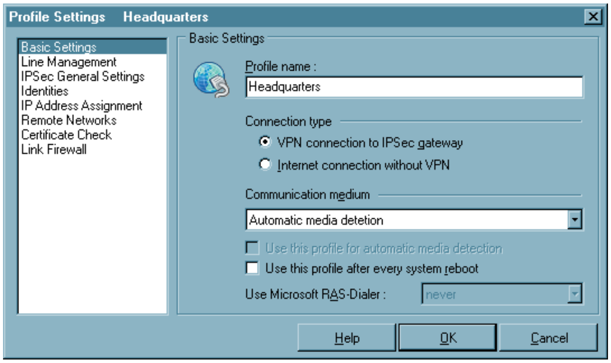
PocketPC Connection Manager:

This connection medium can be set for PocketPC platforms. It is ideal for devices with integrated telephone (MDA). While a GPRS connection exists, you can telephone at the same time. The PocketPC Connection Manager automatically takes over the parking of GPRS connection. When configuring a profile for this application ensure that the timeout-span selected is large enough, or that timeout is deactivated, and Dead Peer Detection (DPD) is deactivated in the IPSec settings.

When using this media type, the PocketPC Connection Manager is forced to set-up a connection (in the Internet or corporate network). This means that the Connection Manager will automatically select an RAS connection and set it up, or it will detect an existing LAN card and will not setup any other connection. Under “Start -> Settings -> Connections”, the system can configure appropriate Internet and company connection with its own onboard resources. If the virtual adapter is active then more precise project-specific knowledge of the environment is required for effective use of the Connection Manager.

Automatic media detection

If different connection types are used in alternation, such as modem and ISDN, then manual selection of the destination system with the respectively available connection medium is not necessary, if a destination system has been configured for “Automatic media detection”, and in each case a destination system with the alternatively available connection types, such as modem and LAN has been selected.



Profile Settings Headquarters

Basic Settings

Profile name : Headquarters

Connection type

● VPN connection to IPSec gateway

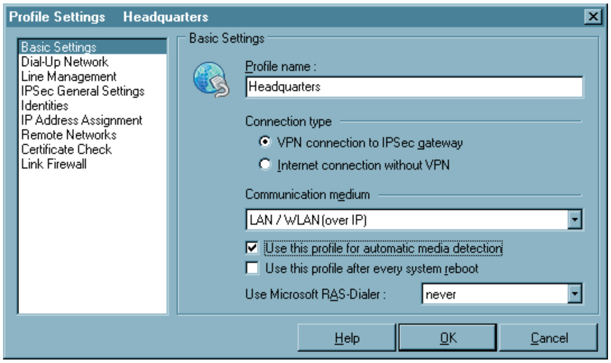
○ Internet connection without VPN

Communication medium: Automatic media detetion

□ Use this profile for automatic media detection

□ Use this profile after every system reboot

Use Microsoft RAS-Dialer : never



Profile Settings Headquarters

Basic Settings

Profile name : Headquarters

Connection type

● VPN connection to IPSec gateway

○ Internet connection without VPN

Communication medium: LAN / WLAN (over IP)

☑ Use this profile for automatic media detection

□ Use this profile after every system reboot

Use Microsoft RAS-Dialer : never

In this regard ensure that the destination system with automatic media detection is configured with all parameters necessary for the connection to the VPN Gateway (particularly the IP address of the VPN gateway), on the other hand the destination systems with the alternative connection types must be configured in such a manner that each desired connection type (possibly the modem parameters as well) is set and the function “Entry for automatic media detection” is activated.

In addition for the respective connection medium the input data to the ISP must be set in the “Network dial-in parameter field.

For connection setup the Client automatically detects which connection types are currently available and selects the fastest of these, and if there are multiple alternative transmission paths it automatically selects the fastest. The connection type priority is specified in the following sequence in a search routine: 1. LAN, 2. MODEM. The incoming data for the connection for the ISP are transferred from the phonebook entries that have been configured for automatic media detection.

Use this profile for automatic media detection

Activating this function this destination system is assigned to the phonebook entry for automatic media detection. If the according media type is currently available, this destination system is to be used automatically. Please note the description under “Link Type”.

If this function is switched off (the check mark is removed), then this destination system can also be selected manually in order to setup a connection, if the tunnel parameters for access to the VPN Gateway have been entered correctly.

Destination network

When using the connection medium “PocketPC Connection Manager”, which is only practical for deactivated Loopback adapter, you can select the destination network: Internet or corporate network. This setting can also be changed retroactively on the PDA via the Popup menu.

Use Microsoft RAS-Dialer

Microsoft’s RAS Dial-Up Networking can be used for dialing in to an ISP. This is necessary when then access point requires a dial-up script. The RAS Dial-Up Networking supports this script. The RAS Script file including its path and name can be entered in the parameter folder “Dial-Up Network” (see → RAS Script file).

NCP Dialer and Microsoft RAS Dialer

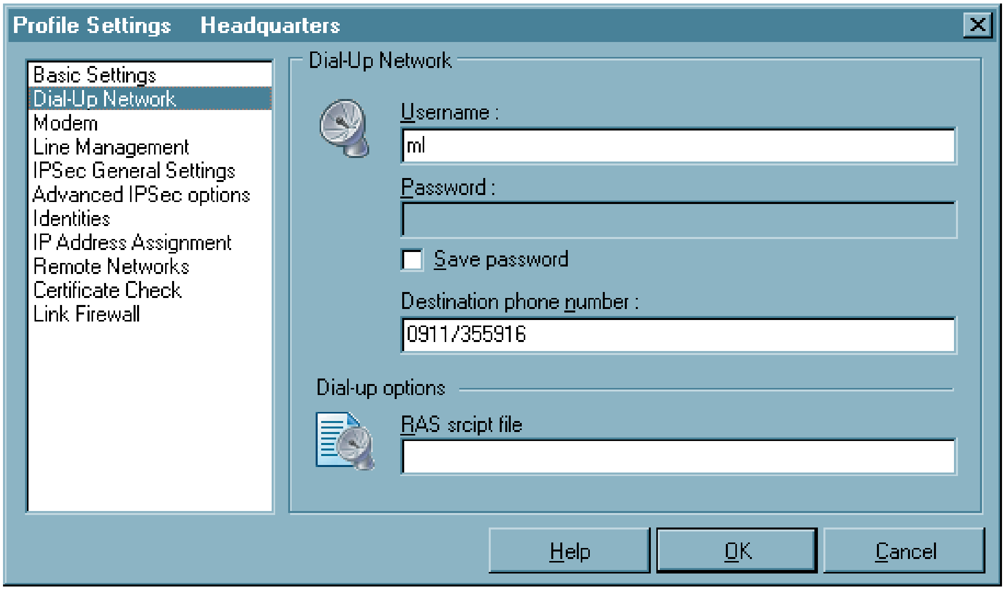
The CE Client can use the Microsoft RAS dialer as well as the NCP Dialer. With the NCP Dialer, initialization strings can be sent to mobile phones (modems) so that GPRS connections can be established with any suitable mobile phone (v.110 connections also).

The NCP Dialer is preset as default and does not have to be set separately in the profile under “Destination system”. If the connection type “Modem” is selected for the destination system, then the “Use Microsoft RAS dialer” option can be activated. If this option is not selected, then the NCP Dialer is active.

The question of which dialer to use depends on the hardware components or which mobile phone or modem is implemented for establishing the connection, and whether the dial-in point (ISP) requires a dial-in script.

For communication via modem (or mobile phone), the modem must have been correctly recognized by Windows CE. Drivers for modems that support the Hayes command set are integrated in Windows CE. Likewise Windows CE supports most mobile phones with IR interface and built-in modem that do not require an init string. Data connections requiring an initialization string for their establishment (mostly GPRS) are also possible.

5.1.2 Dial-Up Network



Username : ml

Password :

□ Save password

Destination phone number : 0911/355916

Dial-up options

RAS sricpt file

This folder contains the parameters Username and Password, which are needed to properly identify you when accessing the destination. From a technical standpoint these two items are included as part of the PPP negotiation to the ISP (Internet Service Provider). If the Communication media "LAN over IP" has been selected, then this folder will not appear since these parameters are not relevant for LAN operation.

Parameters:

□ Username

□ Password

□ Save password

□ Destination phone number

□ Alternate destination phone numbers

□ RAS script file

Username

This parameter is used to identify yourself to the remote Network Access System (NAS) when establishing a connection to your destination, or alternatively to your Internet Service Provider (ISP) if you are communicating across the Internet. The username may consist of up to 254 characters. Normally the username will be assigned to you by your destination (e.g. your company Headquarters, User Help Desk, Internet Service Provider, etc.), because it must be supported and accepted by the NAS, Radius or LDAP server for authentication purposes.

Password

This parameter is used for identifying yourself to your Internet Service Provider (ISP) if the Internet is used. The password can include up to 128 characters. Normally the password will be assigned to you by your destination (e.g. your company Headquarters, User Help Desk, Internet Service Provider, etc.), because it must be supported and accepted by the NAS, RADIUS or LDAP Server for authentication purposes.

Upon entering your password all characters will be displayed as an asterisk (*) in order to keep them from being detected by someone else. Therefore it is necessary to be very careful that you enter your password exactly with regards to the use of upper case and lower case characters.

If the user chooses not to enter and save the password he will be prompted to manually enter it with every connection attempt.

Save password

This parameter should be activated when it is desired that the Password (if entered) is to be stored. Otherwise it will be removed from memory when (re)booting the PC or changing the profile. Default is the activated function.

Important: For security purposes you must be aware that should some unauthorized person use your PC, they will be able to use your password.

Destination phone number

You must define a phone number for all destinations. The phone number must be entered exactly in the same manner as if you were dialing the number from a telephone. You must enter any required prefixes, country codes, area codes, extensions, etc. etc.
Example: Making a connection from Germany to UK:
00 (gets you an international line when dialing from Germany)
44 (this is the country code for United Kingdom)
171 (prefix for London)
1234567 (the number you want to reach)

The following number will be used by the Client for dialing purposes and it will be displayed in the profile as follows: 00441711234567.
The destination phonenumber may include up to 128 characters.

Obtaining an outside line (pre-digits)

Pre-digits for obtaining an outside line, if required, must be preset in the profile under “Network dial-in” when using the NCP Dialer of the “Destination number”. This must be executed with the PC component when creating the profile and cannot be retroactively changed on the PDA.

If the RAS Dialer is used, then the pre-digits for obtaining an outside line can be modified retroactively on the PDA. Please refer to the section “Adapting the dial parameters”.

■ Alternate destination phone numbers

It could be that the destination you want to communicate with uses a Network Access System (NAS) that is equipped with multiple phone numbers. If this is the case, then it may be useful to enter more than one phone number for the destination if for example the primary Destination Phone Number is occupied. The alternate destination phone number(s) can be entered following the primary destination phone number and separated by a colon (:).

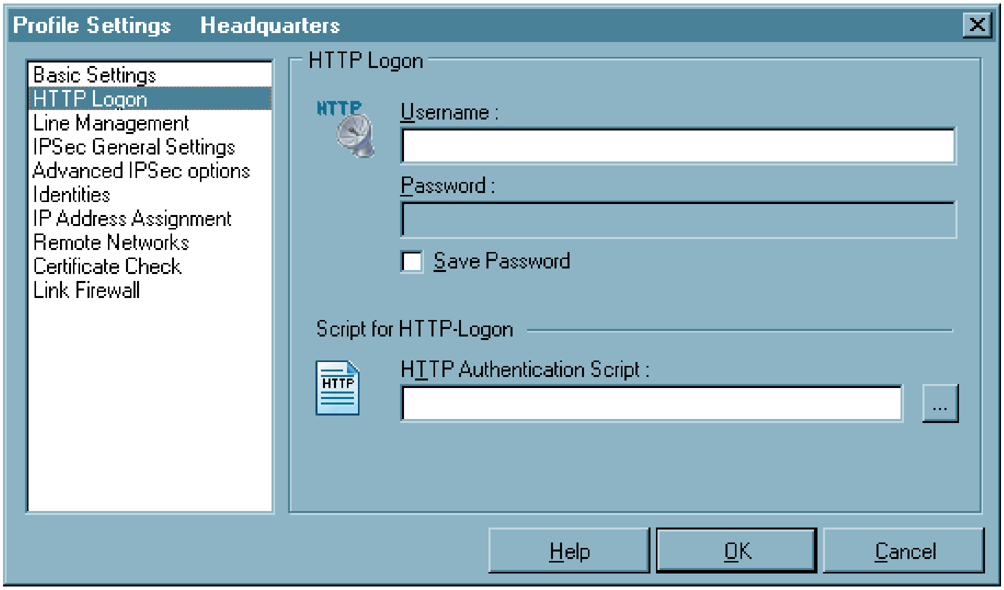
A maximum of 30 digits can be entered in the Destination phone number field. The IP-Sec client supports a maximum of 8 alternate phone numbers.
Example: 00441711234567:00441719876543
The first number is the primary Destination Phone Number and will always be dialed first. The second number is the Alternate Destination phone number and will be dialed when a connection to the primary number is not possible.

Important: This will only work if the protocol settings associated with alternate Destination phone number are the same as the primary Destination phone number.

■ RAS script file

If Microsoft’s RAS Dial-Up networking is to be used, the RAS script file including its path and name must be entered. (See → Basic Settings, Use Micosoft RAS-Dialer)

5.1.3 HTTP Logon



The automatic HTTP logon can be executed automatically with the settings in this parameter field. Centrally created logon scripts and the stored logon data can be transferred from the access point hotspot without opening a browser window.

Please note that there are charges associated with the connection via a HotSpot operator. You must agree to the terms and conditions of the HotSpot operator in order to set up the connection.

Parameters:

□ User name | HTTP Logon

□ Password | HTTP Logon

□ Save Password | HTTP Logon

□ HTTP Authentication Script | HTTP Logon

The logon at the HotSpot is automated with these data. This is executed as follows; for a connection setup to the Access Point an HTTP redirect to the Client with a website for logon is executed from the Access Point. Instead of a browser start for HTTP authentication, the authentication occurs automatically in background, with the entries made here.

For script driven logon you can use a script from the installation directory
`<install>\scripts\samples`
and you can modify it for other HotSpots

For the WLAN connection type the authentication data for the HotSpot are transferred from the WLAN settings.

Username | HTTP Logon

This is the user name that you have obtained from your HotSpot operator.

Password | HTTP Logon

This is the password that you have obtained from your HotSpot operator. The password is concealed with asterisks (*) when entered.

Save Password | HTTP Logon

After the password has been entered it can be saved

HTTP Authentication Script | HTTP Logon

Click on the Browse button [...] to select the saved logon script.

Incoming certificates can be verified with HTTP authentication. For this the variable CACERTDIR must have been set in the script. In addition WEB server certificate content can also be verified. Additional variables are available in this regard:

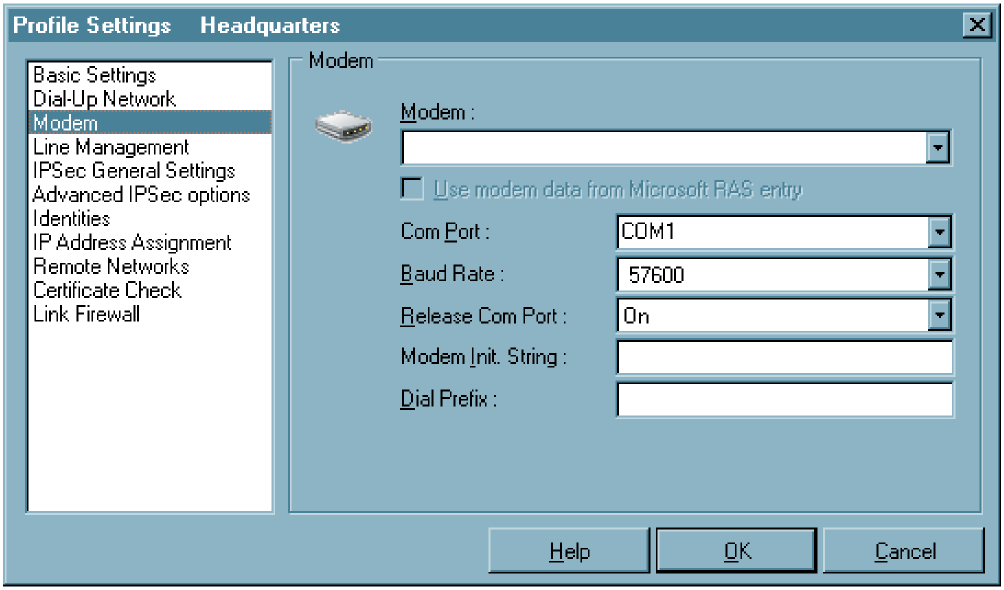
`CACERTVERIFY_SUBJECT`
Checks the content of the subject (e.g. cn=WEB Server 1)

`CACERTVERIFY_ISSUER`
Checks the content of the issuer

`CACERTVERIFY_FINGERPRINT`
Checks the MD5 fingerprint of the issuer certificate

If the content of the variable does not agree with the entered certificate, then the SSL connection will not be established and a log message will be output in the Monitor.

5.1.4 Modem



Modem :

□ Use modem data from Microsoft RAS entry

Com Port : COM1

Baud Rate : 57600

Release Com Port : On

Modem Init. String :

Dial Prefix :

This parameter field is only displayed if your selected communication medium is "Modem". All necessary parameters for this link type are listed here.

When using an MDA with integrated modem, the link type "PocketPC Connection Manager" should be selected. Under certain circumstances with the link type "Modem" the PocketPC Connection Manager will be started additionally, which causes errors and a disconnect of the UMTS/GPRS connection of the client. (See -> Link Type, PocketPC Connection Manager)

Parameters:

□ Modem

□ COM Port

□ Baud Rate

□ Release COM Port

□ Modem Init. String

□ Dial Prefix

□ Use modem data from Microsoft RAS entry

Modem

This field will view the modem(s) installed on your PC. Select the required modem.

Selecting a Modem causes the corresponding COM Port and Modem Init. String for this Modem to be automatically entered in the appropriate Link Definition parameter fields.

All other parameters for this communication media can be configured in the control panel of your PC.

Note: We recommend that you install your Modem prior to installing and configuring the Secure Client. In this case the Secure Client will automatically use the driver and values installed with the Modem.

COM Port

In this field you can define the COM Port to be used by your Modem. Normally when you install a Modem under Windows the COM Port will be defined during the installation of the Modem. If you then select Modem under the Link Definition field, the COM Port already assigned to the Modem will be automatically enter in the COM Port field.

Note: We recommend that you first select the appropriate modem in the field “Modem”. Thereafter the Secure Client will automatically import and use the pre-defined COM Port.

Baud Rate

Baud Rate refers to the transmission rate between the PC’s Com Port and the Modem. If for example your Modem is able to transmit data at 14.4 Kbits, then the Baud Rate should be set to 19200 (factory default setting).

The following rates may be selected:
1200, 2400, 4800, 9600, 19200, 38400, 57600 und 115200

Release Com Port

If you are using an analog modem for communications in conjunction with the IPSec client, it may be desirable upon conclusion of each communications session to release the Com Port for other communication applications (e.g. Fax, Answering Machine). As long as this parameter is set to “OFF” (factory default setting), the Com Port will be assigned exclusively to the Secure Client, and no other application will be able to use it.

Modem Init. String

AT commands can be required, depending on the mobile (cellular) phone or modem and the link mode. For these commands, refer to the respective user manual or obtain the information from your telco or provider. Complete each command with <cr> (Carriage Return).

Dial Prefix

This field is optional. Normally it will not be necessary to enter anything in this field, provided that your modem has been properly installed and is available to the client as a standard communications driver. However, if it is desirable to enter a “Dial Prefix”, refer to your Modem manual for more detailed information.

Following are some examples of Dial Prefixes:

ATDT
ATDP
ATDI
ATDX

Use modem data from Microsoft RAS entry

This parameter is only available if the “Use Microsoft RAS Dialer” has been activated in the “Basic Settings” parameter window. If the modem data are accepted from the Microsoft RAS entry, then all existing RAS entries will be displayed in the “Modem” field. The modem configuration (including init string and all device specific settings) will be accepted from each selected RAS entry.

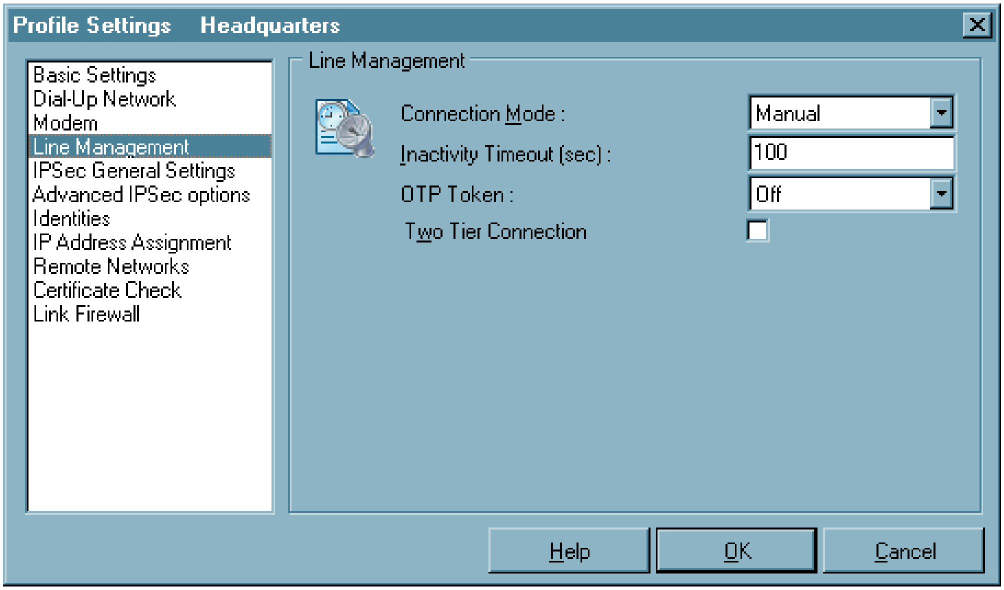
Please note that the telephone number and the access data will not be accepted from the RAS configuration, rather they must be entered as described under “Network dial-in”.

New phonebook entry with modem connection

If a new phonebook entry is generated with modem connection by pressing the “New entry” button in the phonebook, then the configuration assistant starts. This distinguishs between NCP Dialer, Microsoft RAS Dialer or modem data from Microsoft RAS entry. According to the selected type of dial-in, all drivers available on the PDA will be displayed in the “modem” parameter window.

Use the menu item “Refresh Modem Data” in the menu “Configuration” of the configurator.

5.1.5 Line Management



Connection Mode : Manual

Inactivity Timeout (sec) : 100

OTP Token : Off

Two Tier Connection □

In the "Line Management" you can define the Connection Mode as well as Timeout values used for automatically disconnecting the link.

The required authentication before VPN connect is assigned by the network of the hotspot operator.

Parameters:

- □ Connection Mode
- □ Inactivity Timeout
- □ Two Tier Connection
- □ EAP-Authentisierung
- □ HTTP-Authentisierung

Connection Mode

You can define how the client builds a link via the profile to the destination:

automatic: (default) Means that the Secure Client will automatically activate a connection in accordance with your application program requirements to the profile setting. A disconnect also occurs automatically, provided that the Inactivity Timeout parameter is set to any value other then zero.

manual: Means that you must manually activate a connection. Disconnect will be activated by the Inactivity Timeout provided that this parameter has been set to any value other the zero (0).

variable: When this mode is selected, the connection must be established “manually”. Subsequently, the mode adapts according to the manner in which the connection was terminated:
– If the connection was terminated as a result of a timeout, then the following connection will be automatically initiated as required.
– If the connection was terminated manually, then the following connection must also be established manually.

Important: When setting the Connection Mode to “Manual” you should also set the Inactivity Timeout parameter to any value other than zero (0) in order for an automatic disconnect to be made. Otherwise you may incur unnecessary communication costs if a Disconnect is not executed.

Inactivity Timeout

This parameter is for setting the time delay to be used following the last transmission of data before automatically executing disconnect. Time is expressed in seconds. Possible settings are from 1 to 65356 seconds. The default value is “100". If your communications connection (regardless of link type) receives a Charge/Unit impulse from the network provider, this will be used by the Secure Client Timeout feature for achieving an optimal disconnect time with regard to the value set in the Inactivity Timeout. This optimized timeout feature will further help to reduce communication costs.

Note: In order for the Inactivity Timeout to be activated it is necessary to enter any value from 1 to 65356. The value “0" (zero) means that no automatic timeout (disconnect) will be executed. When the Inactivity Timeout is set to ”0" (zero) you must manually execute Disconnect.

Important: The Inactivity Timer only begins counting down after the last data transmission and after any communications handshaking has stopped.

Two Tier Connection

With this function, a dial-in to the Internet first occurs, so that authentication on a website is possible. Re-clicking on the connect button in the graphic interface of the CE client establishes the VPN tunnel connection.

EAP authentication

If the Client must authenticate itself at the Access Point (HotSpot) with EAP (Extensible Authentication Protocol), then this function must be activated. It means that for this destination system the EAP configuration in the Monitor menu under “EAP options” will be used.

Please note that the EAP configuration in the monitor menu is valid for all destination systems and must be switched active if this link-specific setting will be effective.

EAP is used if an Access Point is used for the wireless LAN that is 802.1x capable, and it demands a corresponding authentication. This can prevent unauthorized users from plugging into the LAN via the hardware interface.

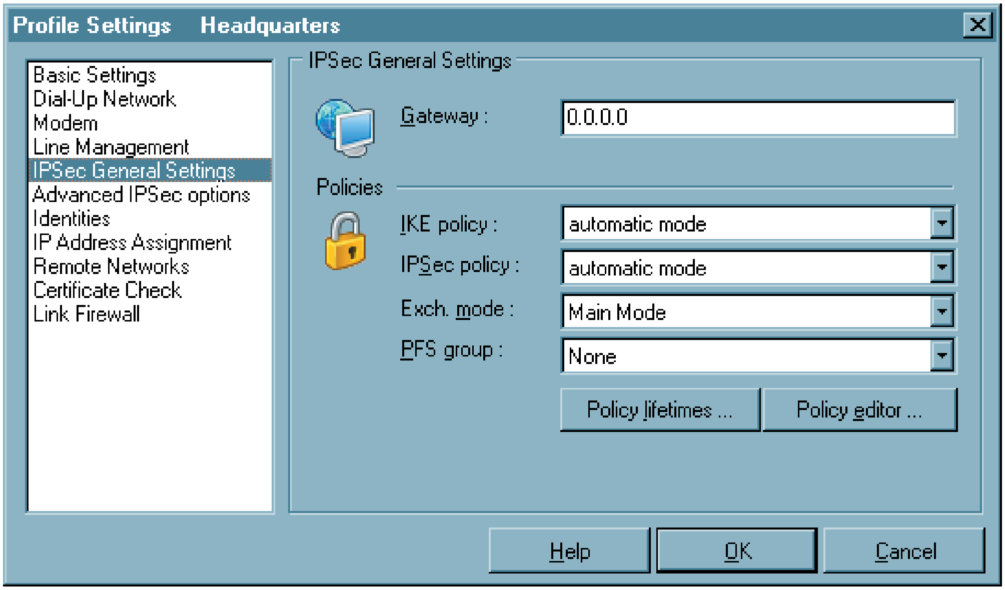
After configuration of the EAP a status display must appear in the graphic field of the Monitor. If this is not the case then the EAP configuration must be switched active in the Monitor menu. Double click on the EAP icon to reset the EAP. Then the EAP is re-negotiated.

HTTP authentication

This function must be activated for automatic HTTP authentication at the access point (HotSpot).

For this an additional parameter field “HTTP Logon” must be switched on in the phonebook, where the authentication data can be entered thereafter (see -> Next parameter field).

5.1.6 IPSec General Settings



Gateway : 0.0.0.0

IKE policy : automatic mode

IPSec policy : automatic mode

Exch. mode : Main Mode

PFS group : None

In this parameter folder you enter the IP address of the gateway. Furthermore you determine the policies to be used for the IPSec connection in the negotiation of phase 1 and 2. Using the automatic mode, the client accepts the policies assigned by the gateway. Should the client use its own policies as the initiator of the connection, you have to configure them with the policy editor. The advanced options could be used according to the requirements of the gateway.

Parameters:

- □ Gateway
- □ IKE Policy
- □ IPSec Policy
- □ Policy lifetimes
- □ Policy editor
- □ Exch. mode
- □ PFS group
- □ Use IP compression (LZS)
- □ Disable DPD (Dead Peer Detection)

Gateway

This is the IP address of the IPSec gateway. You receive the address from your administrator as an IP number, if the gateway has a permanent official IP address - or as a string “hostname” that is mapped to a dynamic IP address from the Internet Service Provider.

IP address: The address is 32 bits long and consists of four numbers separated by periods.

Name (String): Enter the name which you have received from your administrator. This is the DNS Name of this gateway which is stored by the DynDNS service provider.

IKE Policy

The IKE policy is selected from the list box. All IKE policies that you set up with the policy editor are listed under IKE policy. The policies appear in the box with the name that you specified in the configuration.

You will find two pre-configured policies in the policy editor under IKE policy as “Pre-shared Key” and “RSA Signature”. Contents and name of these policies can be changed at any time, i.e. new policies can be added. Every policy lists at least one proposal for authentication and encryption algorithms (see → IKE Policy (editing)). This means that a policy consists of different proposals. There are functional differences between these two IKE policies by using a static key or an RSA signature (see → Examples and Explanations, IPSec, IKE Modes).

The same policies with their affiliated proposals should be valid for all users. This means that on the client side, as well as on the server side, the same proposals for the policies should be available.

Automatic mode: In this case it is not necessary to configure the IKE policy in the “IPSec Configuration”. It will be assigned by the remote site.

Pre-shared Key: This preconfigured policy can be used without PKI support. The same “Static Key” is used on both sides (see → Pre-shared key, Shared secret in the parameter folder “Identity”).

RSA Signature: This preconfigured policy can only be set with PKI support. Implementation of the RSA signature as additional strong authentication only makes sense when using a Smart Card or a soft certificate.

- ### IPSec Policy

The IPSec policy is selected from the List box. All IPSec policies that you set up with the policy editor are listed under IPSec policy. The policies appear in the box with the name that you specified in the configuration.

Two IPSec policies differ according to the IPSec security protocol AH (Authentication Header) or ESP (Encapsulating Security payload. Because the IPSec mode with AH security is totally unsuitable for flexible remote access, only an IPSec policy with ESP protocol, “ESP - 3DES - MD5", is preconfigured and comes standard with the software (see → Examples and Explanations, IPSec, AH and ESP).

Every policy lists at least one proposal for authentication and encryption algorithms (see → IPSec Policy (editing)). This means that a policy consists of different proposals.

☞ The same policies with their affiliated proposals should be valid for all users. This means that on the client side, as well as on the server side, the same proposals for the policies should be available.

Automatic mode: In this case it is not necessary to configure the IPSec policy with the policy editor. It will be assigned by the destination.

ESP - 3DES - MD5 (or other policy name): When selecting the name of the pre-configured IPSec policy the same policies with their affiliated proposals should be valid for all users. This means that on the client side, as well as on the server side, the same proposals for the policies should be available.

- ### Exch. mode

The Exchange Mode determines how the “Internet Key Exchange” should proceed. Two different modes are available; Main Mode also referred to as Identity Protection Mode and the Aggressive Mode. These modes are differentiated by the number of messages and by their encryption.

Main Mode: In Main Mode (standard setting) six messages are sent over the Control Channel and the last two messages are encrypted. The last two messages contain the username, the signature or a hash value. This is why it is also known as Identity Protection Mode.

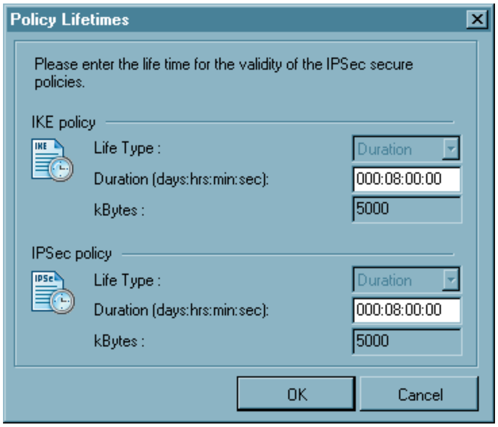
Aggressive Mode: In Aggressive Mode only three messages are sent over the Control Channel and nothing is encrypted.

- ### PFS group

With the selection of one of the offered Diffie Hellman groups it is determined whether a complete Diffie Hellman, (DH Group), key exchange (PFS, Perfect Forward Secrecy) should occur in Phase 2 in addition to the SA negotiation. The Standard is “none”.

Policy lifetimes

The lifetime of the policies defined here are applicable to all the policies.



Policy Lifetimes

Please enter the life time for the validity of the IPSec secure policies.

IKE policy

Life Type : Duration

Duration (days:hrs:min:sec): 000:08:00:00

kBytes : 5000

IPSec policy

Life Type : Duration

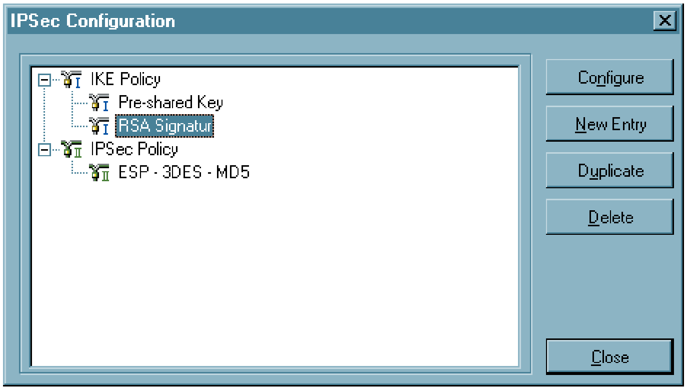
Duration (days:hrs:min:sec): 000:08:00:00

kBytes : 5000

Duration

The number of Kbytes or the size of the time interval can be adjusted.

Policy editor



IPSec Configuration

- IKE Policy
  - Pre-shared Key
  - RSA Signatur
- IPSec Policy
  - ESP - 3DES - MD5

This menu item is clicked for configuring policies and, if necessary, a static Secure Policy Database. A configuration window will open displaying the branch with the policies and the Secure Policy Database as well as buttons for operation in the right-hand part of the configuration window.

Use the mouse to select the policy whose values are to be modified. The buttons will then be active.

The (default) values of the policies can be edited, i.e. the parameters can be set or modified according to the requirements for the link to the defined destination

Configure
If you want to change any Policy or SPD data and parameters, start by selecting the appropriate name and then click on the “Configure” button. Upon doing so a folder opens and displays the IPSec parameters.

New Entry
In order to define a new Policy or SPD, select one of the Policies or the SPD and click on “New Entry”. The new Policy/SPD is entered. All parameters are assigned a default value except the Name.

Duplicate

You may want to use an existing Policy or SPD for the basis of a new one, however with some slight modifications. In order to do so first select the Policy or SPD to be duplicated and then click on the “Duplicate” button. Upon doing so a parameter folder will open. You must now enter a new name for this group and then click on “OK”. A new Policy or SPD is now created with parameters identical to those that were duplicated except for the Name.

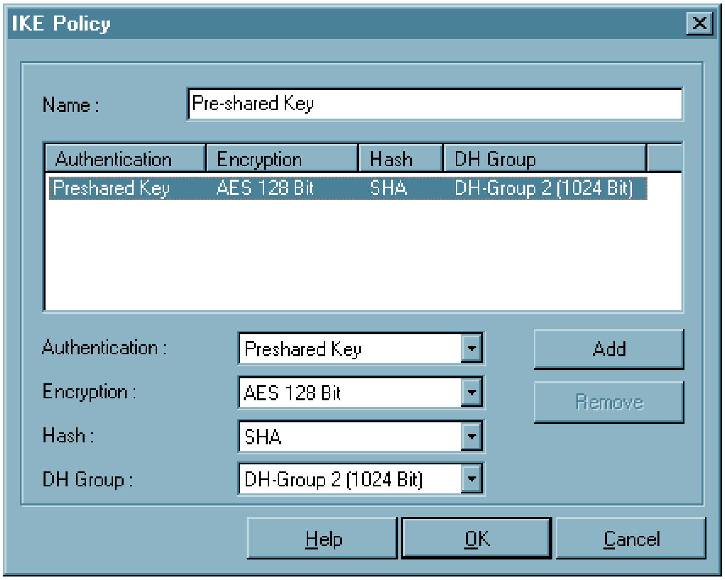
Delete

If you want to delete a Policy or SPD from the IPSec configuration tree select the appropriate group and then click on the “Delete” button. Upon executing “Delete” the Policy or SPD will be permanently deleted.

Close

When you click on “Close” the IPSec folder closes and returns to the Monitor.

IKE Policy (edit)



IKE Policy

Name : Pre-shared Key

Authentication	Encryption	Hash	DH Group
Preshared Key	AES 128 Bit	SHA	DH-Group 2 (1024 Bit)

Authentication : Preshared Key

Encryption : AES 128 Bit

Hash : SHA

DH Group : DH-Group 2 (1024 Bit)

The parameters in this field relate to phase 1 of the Internet Key Exchange (IKE) with which the control channel for the SA negotiation was established. You determine the IKE mode (Exchange Mode), main mode or aggressive mode under “IPSec General Settings”. The IKE policies that you configure here will be listed for the policy selection.

Contents and name of these policies can be changed at any time, i.e. new policies can be added. Every policy lists at least one proposal for authentication and encryption algorithms. This means that any policy can consist of several proposals.

The same policies with their affiliated proposals should be valid for all users. This means that on the client side, as well as on the server side, the same proposals for the policies should be available.

You can extend the list of proposals or delete a proposal from the proposal list by using the buttons “Add” and “Remove”.

Policy Name | IKE Policy

Give this policy a name over which later an SPD can be allocated.

Authentication | IKE Policy

Both sides must have been successfully authenticated in order to establish a control channel for phase 1 (IKE Security Association).

The authentication mode is limited to the use of pre-shared keys. This means for mutual authentication a static key is used. You define this key in the parameter folder “Identity”.

Encryption | IKE Policy

Symmetrical encryption of messages 5 and 6 in the control channel occurs according to one of the optional encryption algorithms if Main Mode (“Identity Protection Mode”) is used. Choices are DES, 3DES, Blowfish, AES 128, AES 192, and AES 256.

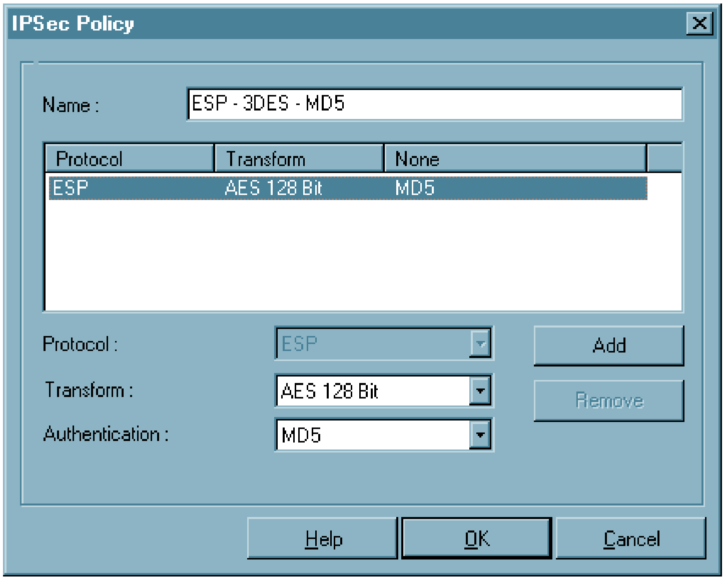
Hash | IKE Policy

This is mode that determines how the hash value over the ID is formed, or in other words this determines which hash algorithm is used in the IKE negotiation. Choices are: MD5 (Message Digest, version 5) and SHA (Secure Hash Algorithm).

DH Group | IKE Policy

The selection of one of the offered Diffie Hellman groups determines the level of security for the key exchange in the control channel. Later a symmetrical key will be generated according to this selection. The higher the DH group the more secure the key exchange will be.

IPSec Policy (edit)



IPSec Policy

Name : ESP - 3DES - MD5

Protocol	Transform	None
ESP	AES 128 Bit	MD5

Protocol : ESP

Transform : AES 128 Bit

Authentication : MD5

The IPSec policies (Phase 2 parameters) that you configure here will be listed for the policy selection.

The same policies with their affiliated proposals should be valid for all users. This means that on the client side, as well as on the server side, the same proposals for the policies should be available.

You can extend the list of proposals or delete a proposal from the Proposal List by using the buttons “Add” and “Remove”.

- **Policy Name | IPSec Policy**

Give this policy a name over which an SPD can later be allocated.

- **Protocol | IPSec Policy**

The fixed default value is ESP.

- **Transform | IPSec Policy**

One can specify which encryption algorithms (DES, Triple DES, Blowfish, AES 128, AES 192, and AES 256) are to be used within the ESP (Encrypted Security Payload). Multiple IPSec proposals with different security combinations can be defined.

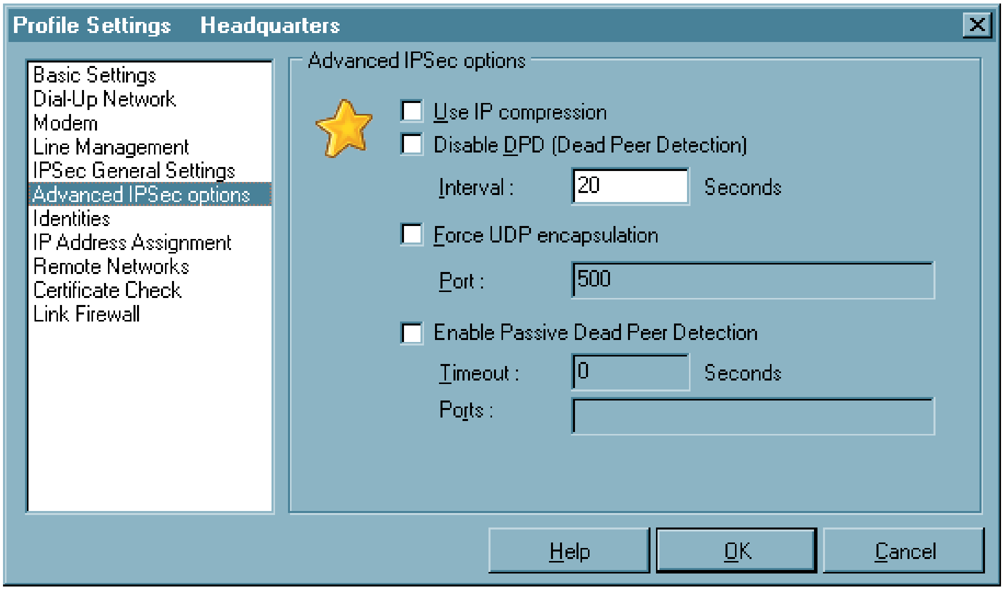
- **Transformation (Comp) | IPSec Policy**

IPSec compression. The data transmission with IPSec can also be compressed as in transfer without IPSec. This enables a maximum threefold increase in throughput. After selecting the “Comp” (compression) protocol you can select between LZS and deflate compression.

- **Authentication | IPSec Policy**

The authentication mode can be specifically set here for the security protocol ESP. Choices are: MD5 and SHA

5.1.7 Advanced IPSec Options



□ Use IP compression

□ Disable DPD (Dead Peer Detection)

Interval : 20 Seconds

□ Force UDP encapsulation

Port : 500

□ Enable Passive Dead Peer Detection

Timeout : 0 Seconds

Ports :

In this filed you can enter further IPSec settings.

Parameters:

□ Use IP compression (LZS)

□ Disable DPD (Dead Peer Detection)

□ Force UDP Encapsulation

□ Enable Passive Dead Peer Detection

Use IP compression (LZS)

The data can be compressed in order to increase transmission rates. By enabeling compression the throughput can be increased to up 3 times that the regular transmissions without compression.

Disable DPD (Dead Peer Detection)

DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background if supported by the destination gateway. The IPSec client uses DPD to check, in regular intervals, whether the other side is still active. If the other side is inactive, then an automatic connection-disconnect occurs.

With this function you can disable DPD.

With DPD (Dead Peer Detection) the VPN Gateway active (according to the defined Time Interval) will be “pinged” and the Tunnel deactivated (independent of the actual data transfer) if no reply is received from the Gateway or a Timeout occurs.

Therefore, when using a GPRS/UMTS connection, DPD could create additional Data transfer and thus extra costs.

Activate Passive Dead Peer Detection

If Applications are active in the background using a GPRS/UMTS connection without a Flatrate, then the use of PPD makes more sense.

With PPD the Timeout will be activated when the Application sends data to the Gateway. Incoming data will stop the timer. If a Timeout occurs, the Tunnel will be deactivated.

The value of timeout can be entered in seconds.

PPD is a feature in the Client software, whereby the Gateway need not support any additional features. Each application for which PPD should be used will be identified by the TCP target port. This may be entered in the phonebook of the PC components to activate PPD.

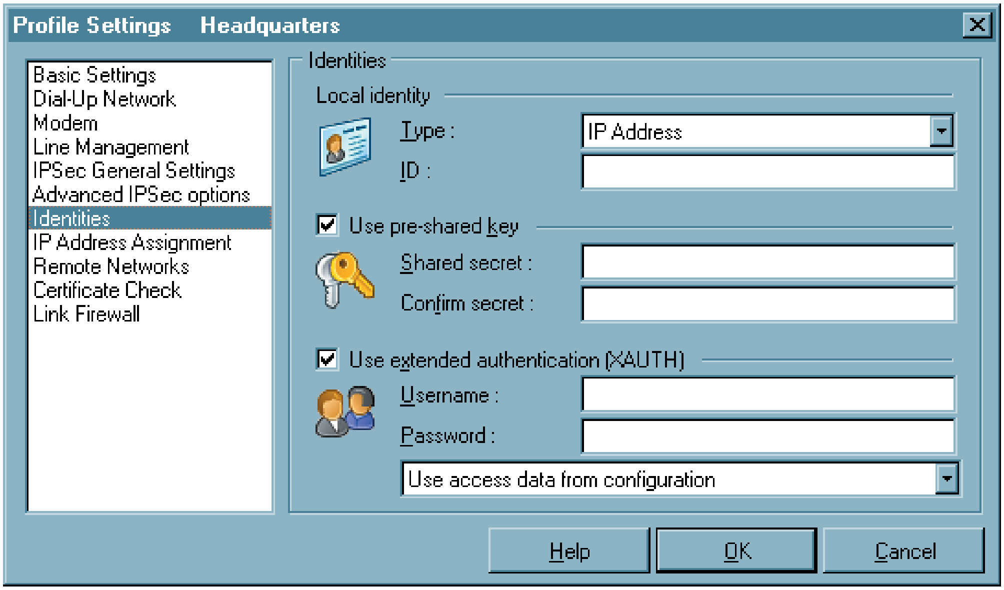
Force UDP Encapsulation

With UDP encapsulation only port 4500 should be released on the external firewall, (this is different than the situation with NAT Traversal or UDP 500 with ESP).

Standard for IPSec with UPD is port 4500, for IPSec without UDP it is port 500.

The NCP Gateway detects UDP encapsulation automatically.

5.1.8 Identities



Identities

Local identity

Type : IP Address

ID :

☑ Use pre-shared key

Shared secret :

Confirm secret :

☑ Use extended authentication (XAUTH)

Username :

Password :

Use access data from configuration

According to the security mode setting IPSec a more detailed parameter setting can take place.

Parameters:

☐ Type | Identity

☐ ID | Identity

☐ Use pre-shared key

☐ Use extended authentication (XAUTH)

☐ Username | Identity

☐ Password | Identity

☐ Use access data from configuration

Type | Identity

For IPSec there is a differentiation of incoming and outgoing connections. The value that the initiator selected as ID for outgoing connection must also be selected by the recipient as the ID for incoming connection.

The following ID Types are available:
– IP Address
– Fully Qualified Domain Name
– Fully Qualified Username
(entspricht der E-Mail-Adresse des Benutzers)
– IP Subnet Address
– ASN1 Distinguished Name
– ASN1 Group Name
– Free String used to identify Groups

ID | Identity

For IPSec there is a differentiation of incoming and outgoing connections. The value that the initiator selected as ID for outgoing connection must also be selected by the recipient as the ID for incoming connection.

According to the selected ID type the character string i.e. the address range (with minus “-”) must be entered in this field.

Use pre-shared key

The pre-shared key is a string of the max. length of 255 characters. Any (alpha)numeric characters can be used. If the other side expects a pre-shared key during the IKE negotiation, then this key must be entered in the field “Shared secret”.

Please confirm the shared secret in the field below. The same pre-shared (static) key must be used at both end points of the communication.

Use extended authentication (XAUTH)

The authentication for “IPSec Tunneling” can be dealt with utilizing extended authentication (XAUTH protocol, Draft 6). If “XAUTH” is to be used, and supported by the gateway, enable “Use extended authentication (XAUTH)”. In addition to pre-shared key, username and password can be defined:

Username = Username of the IPSec user

Password = Password of the IPSec user

Username | Identity

Contact your System Administrator for your “Username”. The name can be up to 256 characters long.

Note: This parameter pertains only to accessing the gateway at the remote site.

Password | Identity

Contact your System Administrator for your “Password” for XAUTH. The password can be up to 256 characters long.

Note: This parameter pertains only to accessing the gateway at the remote site.

Use access data from configuration

You can select one of the following methods for authenticating the VPN tunnel against the gateway:

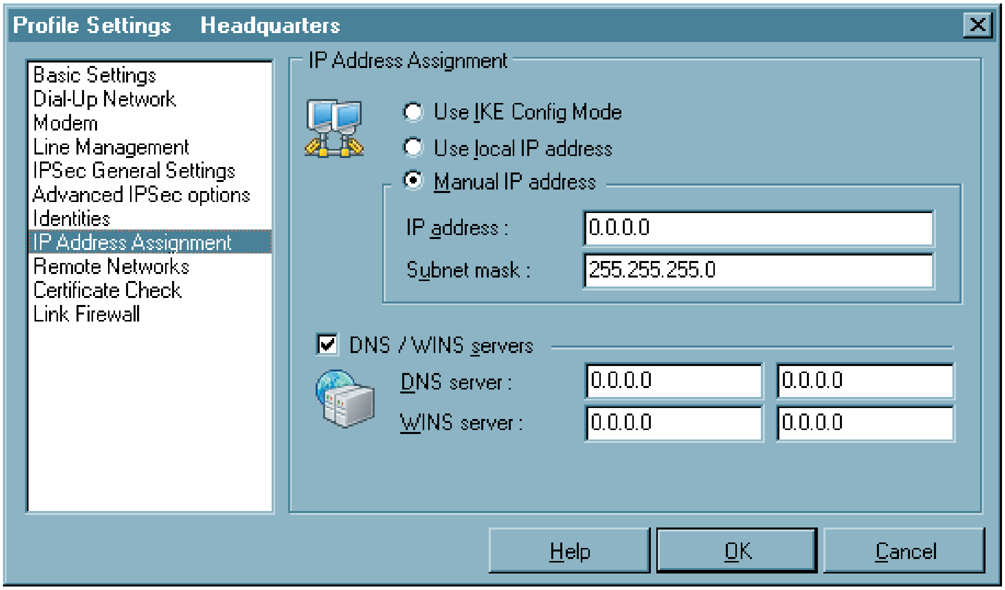
Use access data from configuration:
The VPN tunnel will be authenticated based on the User ID and Password entered in the respective fields above.

Use access data from certificate field “e-mail”:
The VPN tunnel will be authenticated based on the contents of E-Mail field of the selected certificate.

Use access data from certificate field “cn”:
The VPN tunnel will be authenticated based on the contents of “Customer” field of the selected certificate.

Use access data from certificate field “serial no.”:
The VPN tunnel will be authenticated based on the contents of “Serial No.” field of the selected certificate.

5.1.9 IP Address Assignment



IP Address Assignment

○ Use IKE Config Mode

○ Use local IP address

● Manual IP address

IP address : 0.0.0.0

Subnet mask : 255.255.255.0

☑ DNS / WINS servers

DNS server : 0.0.0.0 0.0.0.0

WINS server : 0.0.0.0 0.0.0.0

In this parameterfield you can determine how to assign IP addresses. Moreover the server, assigned automatically by the PPP negotiation, can be changed with an alternativ server. Therefore the network settigs of the operation system must be switched to DNS mode.

Parameters:

☐ Use IKE Config Mode

☐ Use local IP address

☐ Manual IP address

☐ DNS/WINS

☐ DNS server

☐ WINS server

■ Use IKE Config Mode

IP addresses and DNS servers are assigned via the IKE Config Mode protocol (Draft 2). All WAN interfaces can be used for the NAS dial-in.

DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background for “IPSec Tunneling” if supported by the destination gateway. The IPSec client uses DPD to check, in regular intervals, whether the other side is still active. If the other side is inactive, then an automatic connection-disconnect occurs. Using NAT Traversal is automatic with the IPSec client and is always necessary if network address translation is used on the side of the destination system device.

■ Use local IP address

In this case the currently configured IP address (DHCP as well) of the PC is used for the IPSec client.

■ Manual IP address

This is the IP address and the subnet mask; these can be freely entered here. In this case the address entered here is used, regardless of the configuration in the network settings.

■ DNS/WINS

IKE Config Mode, if configured and available, enables dynamic assignment of client IP addresses, DNS / WINS server addresses and domain name.

Activating this function you can define an alternative DNS Server as opposed to using the one that is automatically assigned during the PPP negotiation to the NAS/ISP.

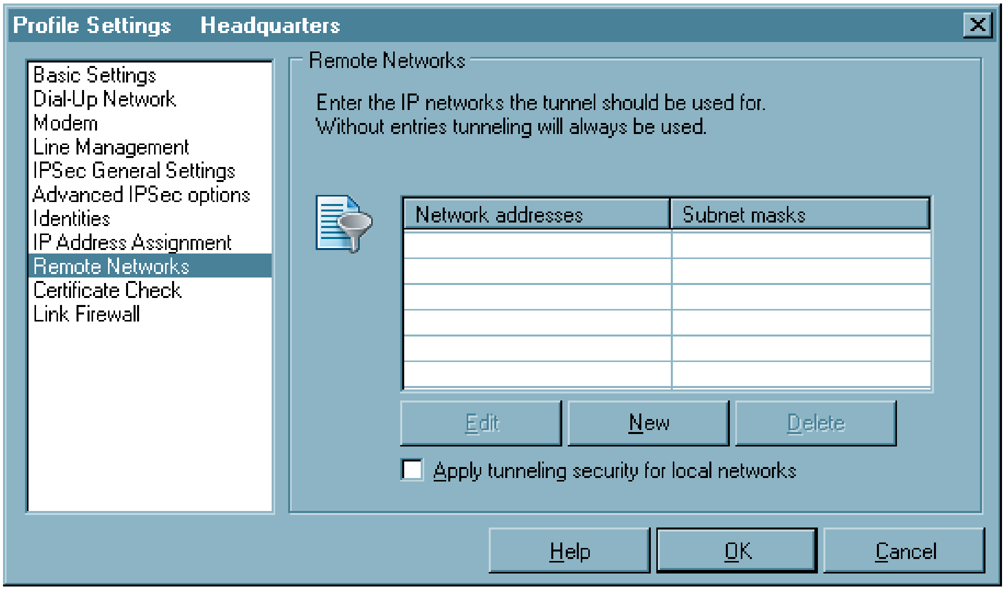
■ DNS server

The IP address of the DNS server entered will be the one used instead of the DNS server assigned during the PPP negotiation.

■ WINS server

The IP address of the WINS server entered will be the one used instead of the WINS Server assigned during the PPP negotiation.

5.1.10 Remote Networks



Remote Networks

Enter the IP networks the tunnel should be used for.
Without entries tunneling will always be used.

Network addresses	Subnet masks

☐ Apply tunneling security for local networks

In this folder you can precisely define the IP Network(s) to which the Client can communicate with via VPN tunnels. If you are using tunneling and you have made no entries in this folder, then your communications will always be established only to the tunnel end-point (VPN gateway). However if you would like to alternatively communicate with your central site using tunneling as well as the Internet, then you must define the IP Networks in your company that you wish to communicate with. Then you can toggle between the Internet and your company's VPN gateway. This is also referred to as "Split Tunneling".

Parameters:

□ Network addresses | Remote Networks

□ Subnet masks

□ Apply tunneling security for local networks

Network addresses | Remote Networks

In this window enter the address of the IP Network(s) that you want to reach via the gateway. These addresses are available from your administrator.

Note: Be sure that IP addresses entered in this field are not the same subnet as the gateway.

Subnet masks

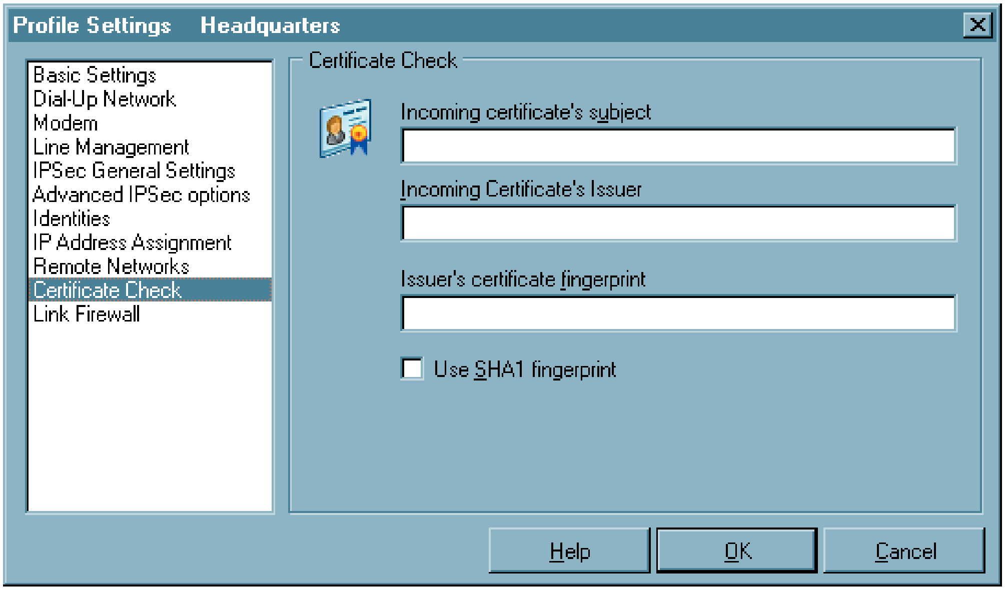
In this window enter the address(es) and netmask(s) of IP Network(s) that you want to reach via the gateway. These addresses are available from your administrator.

Note: Be sure that IP addresses entered in this field are not the same subnet as the gateway.

Apply tunneling security for local networks

If you wish to encrypt the local LAN traffic by means of VPN tunneling enable this function.

5.1.11 Certificate Check



You can specify in the "Certificate Check" parameter field, per destination system, which entries must be present in a certificate from the other side (Secure Server) (see → Display Incoming Certificate, General). See also → Further Certificate Checks.

See also:

- □ Incoming certificate's subject
- □ Incoming certificate's Issuer
- □ Issuer's certificate fingerprint
- □ Use SHA1 fingerprint
- □ Further certificate checks

Incoming certificate’s subject

All attributes of the user, to the extent known - even with wildcards -, can be used as user certificate entries of the other side (server). In this regard compare the entries that are always listed under users for “Display Incoming Certificates”.

Use the attribute name abbreviations for this. The attribute type abbreviations for certificate entries have the following meaning:

```
cn    = Common Name / Name
s     = Surname / Nachname
g     = Givenname / Vorname
t     = Title / Titel
o     = Organisation / Firma
ou    = Organization Unit / Abteilung
c     = Country / Land
st    = State / Bundesland, Provinz
l     = Location / Stadt, Ort
email = E-mail
```

Example:
`cn=VPNGW*, o=ABC, c=de`
The common name of the security server is verified here only until the wildcard “*”. All following positions can be as desired, like 1 - 5 as numbering. The organizational unit must always be ABC in this case and Germany must be the country.

Incoming certificate’s Issuer

All attributes of the user, to the extent known - even with wildcards -, can be used as user certificate entries of the other side (server). In this regard compare the entries that are always listed under users for “Display Incoming Certificates”.

Use the attribute name abbreviations for this. The attribute type abbreviations for certificate entries have the following meaning:

```
cn    = Common Name / Name
s     = Surname / Nachname
g     = Givenname / Vorname
t     = Title / Titel
o     = Organisation / Firma
ou    = Organization Unit / Abteilung
c     = Country / Land
st    = State / Bundesland, Provinz
l     = Location / Stadt, Ort
email = E-mail
```

Example:
`cn=ABC GmbH`
Only the common name of the issuer is verified here.

- **Issuer's certificate fingerprint**

To prevent an unauthorized person that imitates a trusted CA, from using a counterfeited issuer certificate, the issuer's fingerprint can also be entered if it is known.

- **Use SHA1 fingerprint**

The algorithm for fingerprint generation can be either MD5 (Message Digest version 5) or SHA1 (Secure Hash Algorithm 1).

Further certificate checks

In addition to the certificate verification according to content a certificate check is executed on the Secure Client in many respects.

1. Selection of the CA Certificates

The corporate network administrator specifies which issuers of certificates can be trusted. This is done by copying the CA certificates of his choice into the \ncple\cacerts\ Windows directory. The copying over can be automated with diskettes in a software distribution, if the issuer certificates are located in the root directory of the first diskette at the installation. Afterwards issuer certificates can be automatically distributed via the Secure Update Server (see → Update Server Manual), or if the user has the requisite write authorizations in the designated directory - they can be set by the user himself (see → Display CA Certificates.

The formats *.pem and *.crt are supported for issuer certificates. They can be viewed in the monitor under the menu item "Connection - Certificates - Display CA Certificates".

If the issuer certificate of another side is received, then the client determines the issuer, then searches the issuer certificate, first on Smart Card or in the PKCS#12 file, and then in the NCPLE\CACERTS\ directory. If the issuer certificate cannot be located, then the connection cannot be established.

If no issuer certificates are present, then no connection will be permitted.

2. Check of Certificate Extensions

Certificates can contain extensions. These serve for the linking of additional attributes with users or public keys, that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written in the certificate by the issuing certification authority.

Three extensions are significant for the Secure Client and the Secure Server:
– extendedKeyUsage
– subjectKeyIdentifier
– authorityKeyIdentifier

extendedKeyUsage:

If the extendedKeyUsage extension is present in an incoming user certificate, then the Secure Client checks whether the defined extended application intent is “SSL Server Authentication”. If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Please note that the SSL server authentication is direction dependent. This means that the initiator of the tunnel establishment checks the incoming certificate of the other side, if the extendedKeyUsage extension is present, then the intended purpose must contain “SSL Server Authentication”. This applies as well for callback to the Client via VPN.

subjectKeyIdentifier / authorityKeyIdentifier:

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer’s public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA certificate is found then the connection is rejected.

The keyidentifier designates the public key of the certification authority and thus not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determining a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

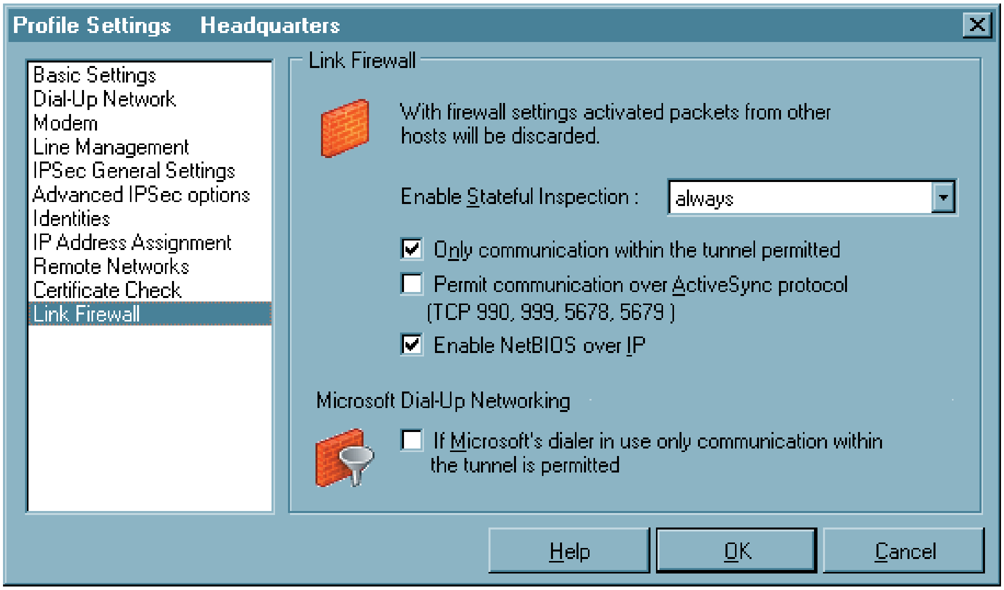
3. Checking Revocation Lists

The Secure Server can be provided with the associated CRL (Certificate Revocation List) for each issuer certificate. It will be copied into the \ncple\crls\ Windows directory. If a CRL is present, then the Secure Client checks the incoming certificates to see if they are listed in the CRL. The same applies for an ARL (Authority Revocation List) that must be copied into the \ncple\arls\ Windows directory.

If incoming certificates are contained in the CRL or ARL lists, then the connection is not permitted.

If CRLs or ARLs are not present, then no check takes place in this regard.

5.1.12 Link Firewall



Link Firewall

With firewall settings activated packets from other hosts will be discarded.

Enable Stateful Inspection : always

☑ Only communication within the tunnel permitted

□ Permit communication over ActiveSync protocol (TCP 990, 999, 5678, 5679)

☑ Enable NetBIOS over IP

Microsoft Dial-Up Networking

□ If Microsoft's dialer in use only communication within the tunnel is permitted

The "Link Firewall" configuration field with extended configuration possibilities is included in this client. The firewall settings can also be used to protect the RAS connections. The activated firewall is displayed on the monitor as a symbol (wall with arrow). A firewall's fundamental task is to prevent hazards from the Internet from spreading within the corporate network. This is why a firewall is also installed at the junction between corporate network and the Internet. It checks all incoming and outgoing data packets and decides whether a data packet will be permitted through or not, on the basis of previously specified configurations. The implemented technology is Stateful Inspection. Stateful Inspection is a very recent firewall technology and offers the high-est security available today for Internet connections and thus the corporate network. Security is insured from two perspectives. On one hand, this functionality prevents unauthorized access to data and resources in the central data network. On the other hand it monitors the respective status of all existing Internet connections as a control instance. Additionally, the Stateful Inspection firewall recognizes whether a connection has opened; "spawned connections" - such as is the case with FTP or Netmeeting - whose packets likewise must be forwarded. The Stateful Inspection connection presents itself as a direct line to the communication partner that may only be used for a data exchange that corresponds to one of the agreed upon rules.

Parameters:

□ Enable Stateful Inspection

□ Only communication within the tunnel permitted

□ Permit communication over ActiveSync protocol

□ Enable NetBios over IP

□ If Microsoft's dialer in use only communication within the tunnel is permitted

- **Enable Stateful Inspection**

off: The firewall’s security mechanisms will not be used.

always: The firewall’s security mechanisms will always be used, this means the PC is protected from unauthorized accesses even if no connection is established.

when connected: The PC is not vulnerable if a connection exists.

ActiveSync connections are handled by the Link Firewall as normal TCP connections. Although ActiveSynch establishes the TCP connection in both directions (PC ⟷ PDA), with activated Stateful Inspection filter traffic is only allowed in the Link Firewall. The connection is blocked if “Only permit communication in the tunnel” is activated.

Also compressed connections of the RAS-Dialer can by monitored by the Client as normal IP traffic, because the compression (CCP), as well as the VanJacobson IP header compression (in the IPCP) can no longer be negotiated.

- **Only communication within the tunnel permitted**

Only communication within the tunnel permitted: This function can also be switched on with activated firewall to additionally filter IP packets so that only VPN connections are possible.

- **Permit communication over ActiveSync protocol**

ActiveSync connections are handled by the Link Firewall as normal TCP connections. Although ActiveSync establishes the TCP connection in both directions (PC <—> PDA), with activated Stateful Inspection filter ActiveSync traffic is allowed in the Link Firewall.

The connection is blocked if “Only permit communication in the tunnel” is activated. To permit an ActiveSync connection with this setting the function “Permit communication over ActiveSync protocol” must be enabled.

The (global) firewall must be released for ActiveSync in the case of a direct connection (via USB, serial or infrared). This is done in the firewall settings of the monitor under “Options - Permit ActiveSync connections (TCP 990, 999, 5678, 5679, 26675, 5721)”. This setting can also be made on the PDA via the popup menu, if the (global) firewall is active.

Under Windows Mobile 5.0 an ActiveSync connection via the USB interface of the PC does not depend on the firewall rules. Using elder operating systems or alternate interfaces like Bluetooth, the connection must be switched on with the parameter “Permit communication over ActiveSync protocol”.

If ActiveSync is operated via network (LAN or WLAN) then in addition a separate firewall rule for name resolution (DNS/WINS) must be created.

- **Enable NetBios over IP**

This parameter switches off a filter, which prevents NetBios frames from being transmitted over IP links.

The default setting is “Off”, meaning that NetBios frames are filtered will be filtered out of the data stream.

When this parameter is activated, NetBios frames will be included in the data stream over IP. This may be desirable when using Microsoft Networking in conjunction with the Secure Client.

- **If Microsoft’s dialer in use only communication within the tunnel is permitted**

When using the Client Monitor this function prevents communication to the Internet via the RAS Dialer.

6. Establishing a connection

Please note that different settings must be made before establishing a connection. The type of connection establishment to the destination system is specified during the configuration with the PC component, the settings of the optional parameters are defined on the PDA.

If a connection setup is faulty then error codes are displayed as red text in the graphic field of the monitor. These error codes have been extended in such a manner that when a connection setup fails, a text is always displayed when the Client detects the failed attempt. For example no error can be displayed if the connection has been disconnected by the server.

6.1 The type of connection establishment to the destination system

The client software allows the definition of the most widely varying destination systems that can be named as required and that can be configured with the PC in advance.

As soon as the software is installed and the telephone book has been transferred to the PDA, the dial-in to a destination system can take place. In this regard the dial-in type is a component of the destination system configuration. You can select from among three dial-in modes for the connection establishment: automatic, manual and alternating. You define the mode of the connection establishment for a destination system in the telephone book under “Connection control / Connection establishment”.

Automatic connection establishment:

The connection will be automatically established according to the target system parameters. Even if you have selected the connection establishment mode “Automatic”, you must establish the connection manually the first time.

Manual connection establishment:

It is also possible to establish the connection to a destination manually by activating the “Connect” button in the button bar of the PDA monitor.

Variable connection establishment:

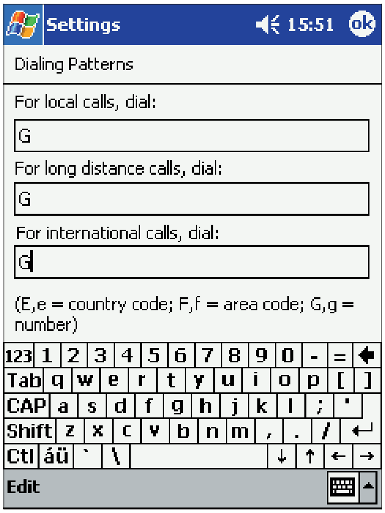
If this mode is selected, then first the connection must be established “manually”. Thereafter the mode changes according to connection establishment as follows:
– if the connection ends with time out, then the connection will be “automatically” established at the next request
– if the connection was disconnected “manually” then it must be reestablished “manually”.

6.2 Adapting the optional parameters

Before the dial-in with the PDA monitor you must configure or create the dial parameters or the dial sample on the PDA. To do this, activate the menu to the system settings under Pocket 2002 as follows:

From the start menus select →
Settings, then →
Connections, then →
Connections again, then →
Dialing Locations and finally →
Dialing Patterns (see graphic to the right).

Here you change the settings for local calls, long distance calls, and international calls, by entering a "G" respectively (see graphic) and confirming this with OK.



Settings 15:51 ok

Dialing Patterns

For local calls, dial: G

For long distance calls, dial: G

For international calls, dial: G

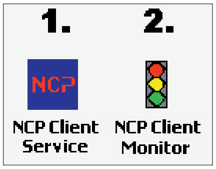
(E,e = country code; F,f = area code; G,g = number)

123 1 2 3 4 5 6 7 8 9 0 - =
Tab q w e r t y u i o p [ ]
CAP a s d f g h j k l ; '
Shift z x c v b n m , . /
Ctl áü ` \ ↓ ↑ ← →
Edit

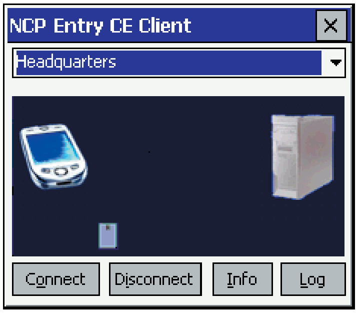
Only in this way do you insure that the CE client dials the number entered in its telephone book. If another code is required at a later time, to get an outside line in a hotel for example, then the appropriate entry can be supplemented.

6.3 Starting

First the service and then the monitor must be started before a connection can be established. Select the respective icons from the program group for this.

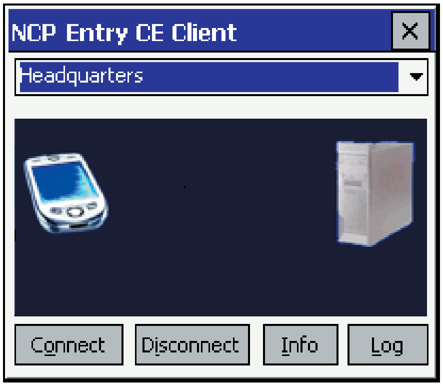


Do not forget to insert the Smart Card or to initialize the reader when you use PKI with Smart Card! In this case a Smart Card symbol must be displayed after starting the monitor (see graphic to the right).

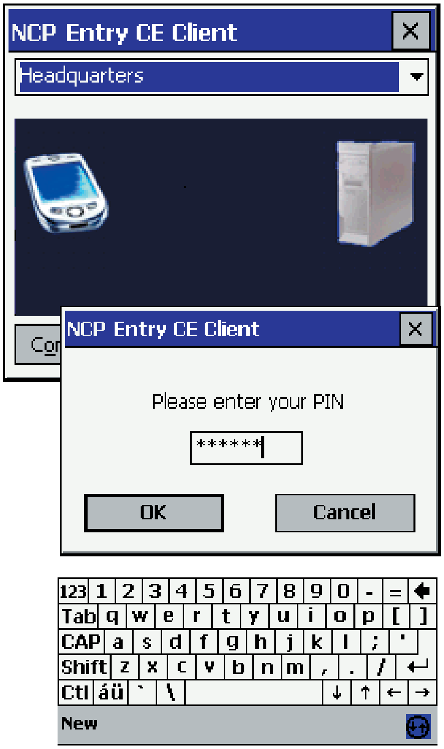


6.4 Connect

Regardless of the manner in which the connection is established, the monitor always displays the status of the connection establishment (assuming the monitor is in foreground) as in the following example:



First the destination system is selected via the selection button.

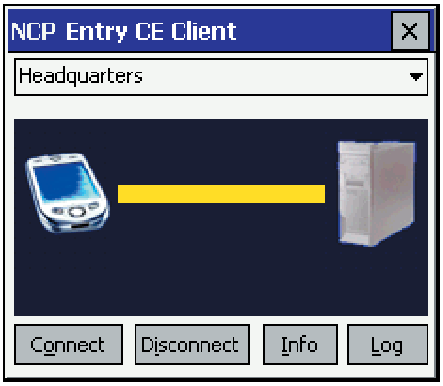


Please enter your PIN

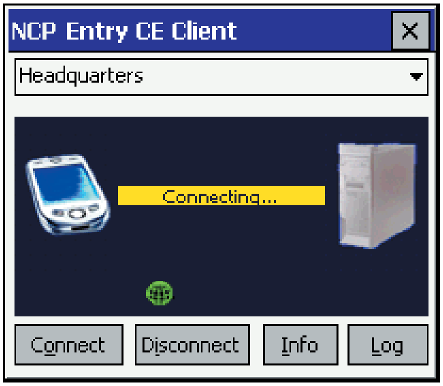
******

Then the connection is established – here manually via the “Connect” button.

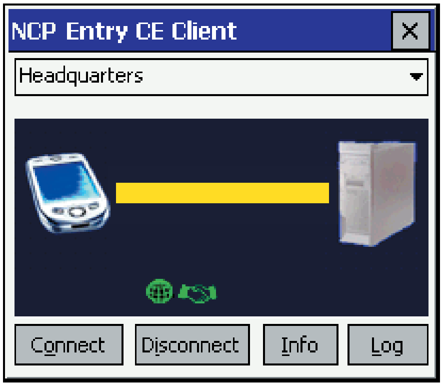
If the use of a (soft) certificate has been configured – like with the test connection with SSL – then the PIN must be entered first.



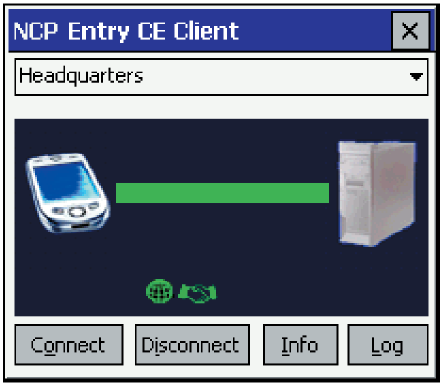
Afterwards a connection to the Internet Service Provider (ISP) is established (yellow line).



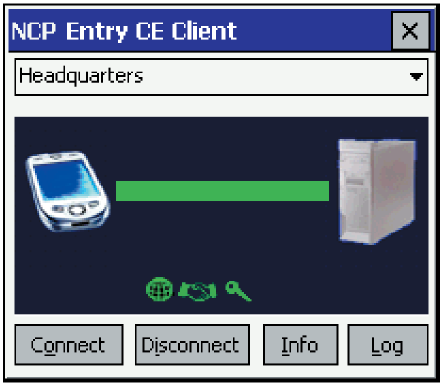
If the green globe appears, then dial-in to the ISP was executed successfully.



The authentication on the VPN gateway is represented as a handshake.



The successful stations run-through are displayed as small symbols under the green line.



In addition, an encryption can still be configured (key).

(If the configuration of the correspondent has been set for compression, then compression can also be configured.)

If the last station of the connection establishment (here the encryption, or the decryption) has been run through, then the connection is thus established.

6.4.1 Passwords and user names

The password is required to identify yourself relative to the Network Access Server (NAS) when the connection has been established. The password may be up to 256 characters long. Usually a “user” will be assigned to you by the destination system, because you must also be recognized by the destination system. You get the name from your company, from the Internet Service Provider or from the system administrator.

When you enter the password, all characters will be displayed as asterisks (*) to hide them from undesired observers. It is important that you enter the password precisely according to the specification and respect capital and lower case letters.

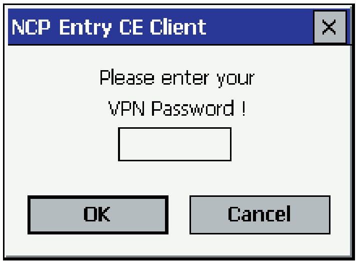
User names and passwords for the dial-in to the VPN gateway (see → Tunnel parameters) can be completely entered in the configuration of the destination system. The “VPN User ID” must be entered during the configuration.

If you have enterd a password it is stored until
– the profile will be changed
– the service is restarted or
– by establishing a connection manually another password is entered.

If it is not entered, then it will be requested in a dialog during the VPN dial-in.

6.4.2 Storing Access Data in the Password and XAUTH Dialog

It is either the passwor dialog or the XAUTH dialog box where it is possible to store the access data of the actual profile.



Please enter your
VPN Password !

■ **XAUTH dialog box with tokencode entry field**

If the option “OTP for NAS - or VPN password” is active then two entry fields will be displayed in the XAUTH dialog box:
– one for the PIN (with masked entry)
– one for the tokencode (with readable entry)
The final password is derived by combining the values of both fields.

If a password is saved (see above) this dialog box is not displayed. If the password is entered incorrectly, or if it must be changed, then the standard XAUTH dialog boxes are displayed with the entry fields specified by the gateway.

6.4.3 Disable Auto-poweroff

If the PDA is not used for a longer period of time, then it switches off automatically into power save mode. This can also occur while a VPN connection is active. This automation mechanism can be switched off in the client monitor. Proceed as follows for this: Hold the entry pen on the graphic field of the monitor for several seconds, a pop-up menu will appear that shows the current setting and which allows you to change the current setting.

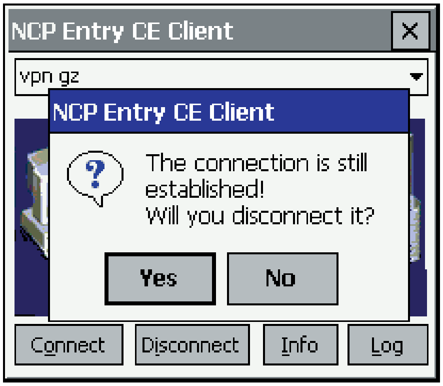
6.5 Disconnect

With the “Disconnect” button in the PDA monitor, the dismantling of the currently existing connection will be manually executed. If you want to retain the possibility of dismantling the connection at any time, then set the connection establishment to “Manual” with the PC component and deactivate the automatic timeout by setting it on zero (0) (see → Connection establishment).

6.5.1 Disconnecting and ending the monitor

If a connection still exists, and if the PDA monitor is ended with the close button, then the connection will not be disconnected automatically. If the connection (possibly involving telephone charges) is to remain intact, although the monitor is ended, then confirmation of this desire will be expressly requested by the software (see graphic below).

If you click on “No” in this confirmation screen, then you will no longer have an icon and no longer have a message to the effect that a connection is still active and charges could accrue. In this case you must restart the monitor to correctly terminate the existing connection!



NCP Entry CE Client

vpn gz

NCP Entry CE Client

The connection is still established!
Will you disconnect it?

7. Examples and Explanations

This section of the handbook discusses some essential routing concepts. The Secure Client configuration is illustrated with several different examples.

7.1 IP Functions

To correctly configure an IP network, you must adhere to the procedure for IP addressing. Below you will find some guidelines and terminology. For additional information about IP networks the standard literature is recommended.

7.1.1 IP Network Devices

IP addresses are assigned to the component interfaces of an IP network. These components are also called hosts or computers. Multiple networked components (e.g. routers) may also be allocated to various addresses. The term host-address marks the IP address of the host of an IP process, regardless of the actual physical structure of the components or the interfaces.

7.1.2 IP Address Structure

IP addresses have a length of four octets, 32 bits (4 bytes) and are written in dotted decimal or hexadecimal notation. E.g.:

```
198.10.6.27 or
C6.0A.06.1B or
0xC6.0x0A.0x06.0x1B
```

The addresses are divided into a network segment, which identifies the network, and a local address, the host segment, identifying the host of the network. All hosts within a unique network share the same host segment. All devices inside a unique network share the same network segment. Each also has a unique host segment.

There are three classes of Internet addresses each is used according to how many bytes the IP address uses for network segment and host segment.

Class A, large networks: network numbers 1 - 127

For class A addresses the highest bit is equal to zero, the next seven bits represent the network segment and the remaining 24 bits represent the host segment.

The network segment needs 1 byte (max. 126 different networks)

The host segment needs 3 bytes (max. 2 to the 24th power = 16.777.216 various hosts).

In this manner a maximum of 127 different networks, each with maximum of 16.777.216 different hosts may be addressed.

Class B, mid-size networks: network numbers 128 -191

For class B addresses the two highest bits have the values 1 and 0, the following 14 bits represent the network segment and the remaining 16 bits represent the host segment

The network segment needs 2 Byte (max. 16.384 various networks)

The host segment needs 2 bytes (max. 2 to the 16th power = 65.526 different hosts)

In this manner a maximum of 16.384 different networks, each with maximum of 65.526 different hosts may be addressed.

C*lass C*, small networks: network numbers 192 - 223

For class C addresses the three highest bits have the values 1, 1 and 0, the following 21 bits represent the network segment and the remaining 8 bits represent the host segment.

The network segment needs 3 bytes (max. 2.097.152 various hosts)

The host segment needs 1 byte (max 256 various hosts)

In this manner a maximum of 2.097.152 various networks, each with maximum of. 256 different hosts may be addressed.

e.g.:

```
            Network         Host
Class A:  122. | 087.  156.  045
Class B:  162.  143. | 085.  132
Class C:  195.  076.  212. | 024
```

Please note, when assigning the addresses, that each physical host must be able to use several IP addresses. A workstation can function with one IP address. A router needs an IP address for each interface however at least two – one for the connection to the local network (LAN IP Address) and one for the connection to the WAN side.

7.1.3 Subnet Masks

In a wide area network various physically separated nets (LANs) may belong to the same network (WAN) with the same network number. On the basis of the network number alone no router can decide if it should create a connection to a physically different network within the WAN or not. Thus the network (WAN) must be subdivided into smaller segments (LANS) that each receive their own address block. Each address block of the individual physical networks is designated as a subnet. Through this subdivision of a network into subnets the hierarchy network and computer is extended to a hierarchy of network, subnet, and computer.

This extended hierarchy makes it easier to locate a computer in the total network (WAN). An example using the telephone nomenclature can illustrate how this works. The area code designates in which area the telephone is located. This hierarchy insures also a certain access security. For example a computer on a subnet will not automatically have access to the resources of another subnet. Or to use a specific case a production worker does not have access to the personnel department data provided that the subnet masks have been selected according to corporate departments.

The subnet mask indicates the location of the subnet field in an IP address. The subnet mask is a binary 32-bit-number like an IP address. It has a “1" in every position of the network segment and an IP address (according to the network class within the first to the third octet). The next octet shows the position of the subnet field. The digits 1 adjacent to the subnet field indicate the subnet bits. All remaining positions with ”0" remain for the host segment.

Examples

Example 1:

The subnet mask is used for the interpretation of the IP address. Accordingly an address 135.96.7.230 with the mask 255.255.255.0 may be interpreted as follows: The network has the address 135.96.0.0, the subnet has the number 7, the host number 230. An IP address with 135.96.4 belongs a to a different subnet (4) on the same network.

Binary representation:

```
135.96.7.230    = 10000111 11000000 | 00000111 | 11100110
135.96.4.190    = 10100000 10010101 | 00000100 | 10111110
255.255.255.0   = 11111111 11111111 | 11111111 | 00000000
                  Network           | Subnet   |
255.255.248.0   = 11111111 11111111 | 11111|000  00000000
```

If the net mask did not have a standard value of 255.255.255.0 in the example shown above, but rather an IP address of 255.255.248.0 then the IP addresses would be located in the same subnet, and routing would not take place.

Example 2:

Two IP addresses with 160.149.115.8 and 160.149.117.201 and the subnet mask 255.255.252.0 are located in the same network, but belong to different subnets.

Binary description:

```
160.149.115.8   = 10100000 10010101 | 011100|11 00001000
160.149.117.201 = 10100000 10010101 | 011101|01 11001001
255.255.252.0   = 11111111 11111111 | 111111|00 00000000
                  network           | subnet|
```

The choice of a suitable subnet mask depends on the network class, the quality of the possible subnets, their quantity and their growth potential. For planning purposes please refer to the standard tables or to a subnet calculator.

Subnet tables class C:

Subnet bits	Host bits	netmask	subnets	host
2	6	255.255.255.192	2	62
3	5	255.255.255.224	6	30
4	4	255.255.255.240	14	14
5	3	255.255.255.248	30	6
6	2	255.255.255.252	62	2

(Calculation: 2 to the power of n minus 2 = quantity of subnets / computers
where n is the quantity of subnets / host bits)

With the subnet mask 255.255.255.240 a class C network is divided into subnets. This net mask allows a total of 14 subnets each with a maximum of 14 computers.

```
255.255.255.240  11111111 11111111 11111111 | 1111 | 0000
199. 9. 99.130  11000111 00001001 01100011 | 1000 | 0010  Subnet-Nummer 8
199. 9. 99.146  11000111 00001001 01100011 | 1001 | 0010  Subnet-Nummer 9
                 Netzwerk                   |Subnet| Host
```

Standard masks

Subnet mask for class A:255. 0. 0. 0

Subnet mask for class B:255. 255. 0. 0

Subnet mask for class C:255. 255. 255. 0

■ Reserved addresses

Some IP addresses may not be assigned to network devices. These include the network or subnet address and the circular address for networks ref. subnets. Network addresses consist of network number and the host field filled with binary 0's (e.g. 200.1.2.0, 162.66.0.0., 10.0.0.0) – also Loop Back, there is no transmission into the network. The circular address consists of network numbers and the host segment with binary 1's (e.g. 200.1.2.255, 162.66.255.255., 10.255.255.255) – therefore also an "All One Broadcast", all components of a network will be addressed.

Example:

198.10.2.255	addressed to all stations in the network 198.10.2.
255.255.255.255	addressed to all stations of all connected nets
0.0.0.0	All Zero Broadcast: invalid address.

Please note that this is often used for standard settings.

7.1.4 Using IP Addresses:

□ Each address in your enterprise-wide network should be unique. Make sure that this is the case when connecting to the Internet or linking new networks.

□ Use a logical, comprehensible addressing scheme, e.g. organized according to administrative units, buildings, departments etc.

□ For connection to the Internet, you will need an official, unique, Internet address.

□ If possible, do not assign any addresses in which the network or host segment end in "0". This might lead to misinterpretations and to undefined errors in the network.

□ Subnet masks will only be evaluated by the Internet protocol, if the network numbers of all communication partners are the same.

The subnet masks have network segments of different length just as do the address classes.

7.2 Security

Configuration parameters for IPSec for implementation in remote access environments are collected in the parameter field “IPSec General Settings”. This section describes some possibilities of configuration.

7.2.1 IPSec – Overview

IPSec can only be implemented for IP data traffic. The IPSec specification includes not only Layer 3 tunneling but also includes all necessary security mechanisms like strong authentication, key exchange and encryption.

The IPSec RFC’s (2401-2409) permit the development of a VPN with specified IP security. IPSec tunneling and security are thoroughly described making a complete VPN framework available. In principle it is possible to use vendor-independent components. For site-to-site VPN’s the gateways may be supplied by different manufacturers, for end-to-site gateways the clients may be supplied by another manufacturer.

The establishment of a connection to IPSec traffic is based on the Internet Key Exchange Protocol (IKE).

■ IPSec – General Functional Description

In every IP host (client or gateway) that supports IPSec there is an IPSec module i.e. an IPSec engine. This module examines each packet for certain characteristics in order to apply the appropriate security negotiation to it.

Testing of the outgoing IP packets from the IP stack occurs relative to a Secure Policy database (SPD). With this all configured SPDs will be processed. (When using the IPSec Client, the SPDs are only stored at the central site gateway.)

The SPD consists of multiple entries (SPD entries), which in turn contain a filter portion. The filter portion or Selector of an SPD entry consists primarily of IP addresses, UPD, and TCP ports as well as other IP header-specific entries. If the values of an IP packet agree with the values from the SPD entry Selector portion, then further determination as to what should be done with this IP packet is made from the SPD Entries. The packet can simply be allowed through (permitted), or discarded, or certain security policies of the IPSec process can be imposed on the packet. These security policies are also described in the SPD entry.

If, in this manner, it is determined that an IP packet is linked with an SPD entry that triggers an IPSec process, then it will be examined to see whether a security association

(SA) exists for this SPD entry. If an SA does not yet exist then first an authentication and a key exchange will take place before the negotiation of an SA (see below → IPSec Negotiation Phase 1)

After the SA negotiation, negotiations follow for data packet encryption (ESP) and/or authentication (AH) of the data packets.

The SA describes which security protocol should be used. ESP (Encapsulating Security Payload) supports the encryption and authentication of IP packets. AH (Authentication Header) supports only the authentication of IP packets. The SA also describes the operating mode in which the security protocol should be used either Tunnel or Transport mode. In Tunnel mode an IP header is inserted, in Transport mode the original header is used. Additionally the SA describes which algorithm will be used for authentication, which encryption method (for ESP) and which key should be used. Of course the other side should work according to the same SA.

If the SA is negotiated, then each packet will be processed according to the operating mode and protocol, either Tunnel or Transport, and either ESP or AH respectively. The IPSec Client uses always the IP protocol in Tunnel mode.

7.2.2 Firewall Settings

The firewall settings consists mainly of IP addresses, UDP and TCP ports, as well as other IP header-specific entries. If the values of an IP packet agree with values from the selector portion, then further determinations from the SPD entries specify how to proceed with this IP packet.

Following, the entries for configuring the IPSec Client:

□ Command

permit, deny, disabled

□ IP Protocol

This is the transport protocol that can be ICMP, TCCP, or UDP. One of these offered protocols can be selected or (any) can be used.

□ Source IP address

This can be a simple IP address or an address range. The latter is necessary if a shared SA, behind a firewall, supports multiple output systems for example.

□ Destination IP address

This can be a simple IP address or an address range. The latter is necessary if a shared SA, behind a firewall, supports multiple output systems for example.

□ Source Port

These can be either individual TCP or UDP port numbers or a range of port numbers. You determine the port numbers with allocated service by using the Select button [...].

□ Destination Port

These can be either individual TCP or UDP port numbers or a range of port numbers. You determine the port numbers with allocated service by using the Select button [...].

7.2.3 SA Negotiation and Policies

In order to initiate the IPSec filter process the SA must first have been negotiated. One SA negotiation takes place for the phase 1 (IKE policy) and at least two (for incoming and outgoing connection) for phase 2 (IPSec policy). [For every destination network (see → Profile Settings, Remote Networks) two SAs are also negotiated.].

- **Phase 1 (IKE Policy)**

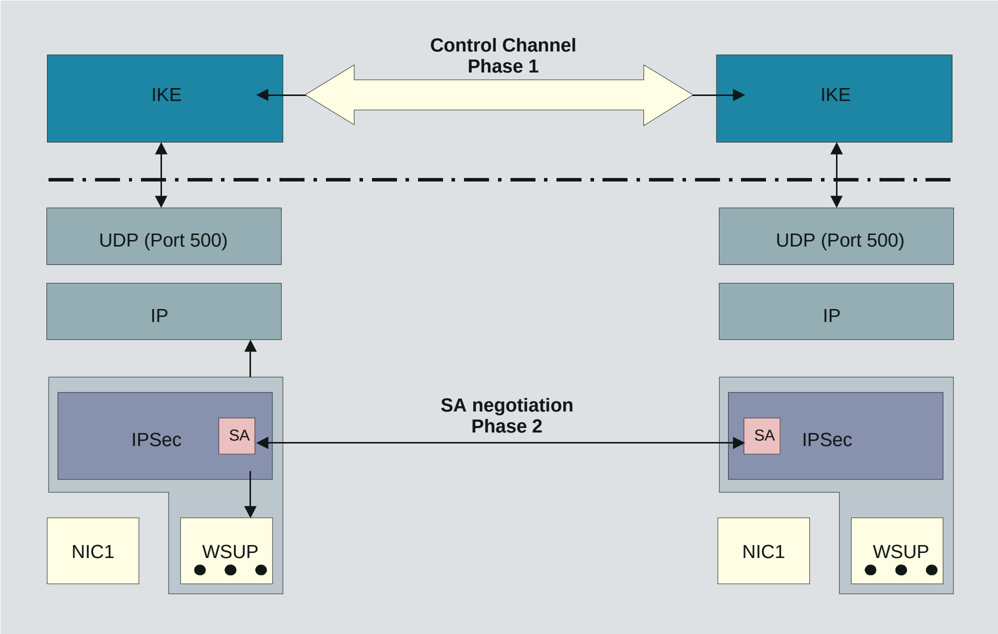
IPSec establishes the control channel in tunnel mode over the IKE protocol to the IP address of the secure gateway. In Transport mode it is established directly to the IP Address of the other side.

You define parameters to determine encryption and authentication type over the IKE protocol in the IKE Policies. Thus an authentication can be achieved via a pre-shared key or RSA signature. (These IKE guidelines are referenced in the IPSec editor.)

- **Phase 2 (IPSec Policy)**

The SA negotiation is concluded over the control channel. From the IPSec engine the SA is handed-off to the IKE protocol that it transmits over the control channel to the IPSec engine.

Control Channel and SA Negotiation



Description of the Graphic:

The SA must first have been negotiated in order for the IPSec process to start. This SA negotiation takes place once per SPD (which can be created for different ports, addresses, and protocols). This SA negotiation requires a control channel.

First the client must create a Layer 2 (PPP) link to the provider. With this link the client is assigned a new IP address each time he dials in. The IPSec module in the client receives an IP frame with the destination address of the corporate network. An SPD entry for this IP frame will be found but no SA exists at this time. The IPSec module then issues a request to the IKE module to negotiate an SA. Thus the requested security policies as present in the SPD entry are handed off to the IKE module. Negotiating an IPSec-Security Association (IPSec-SA) is considered a Phase 2 negotiation. However before an IPSec-SA can be negotiated with the other side (Secure Server) a kind of control channel from the client to the Secure Server (VPN) gateway must first exist. This control channel is established via the Phase 1 negotiation whose result is an IKE- Security Association (IKE-SA). Thus the Phase 1 negotiation undertakes the complete authentication of the client relative to the Secure Server and generates an encrypted control channel. Then the Phase 2 negotiation (IPSec-SA) can immediately take place over this control channel. The Phase 1 negotiation is a handshake over which the exchange of certificates is possible and it contains key exchange for the control channel.

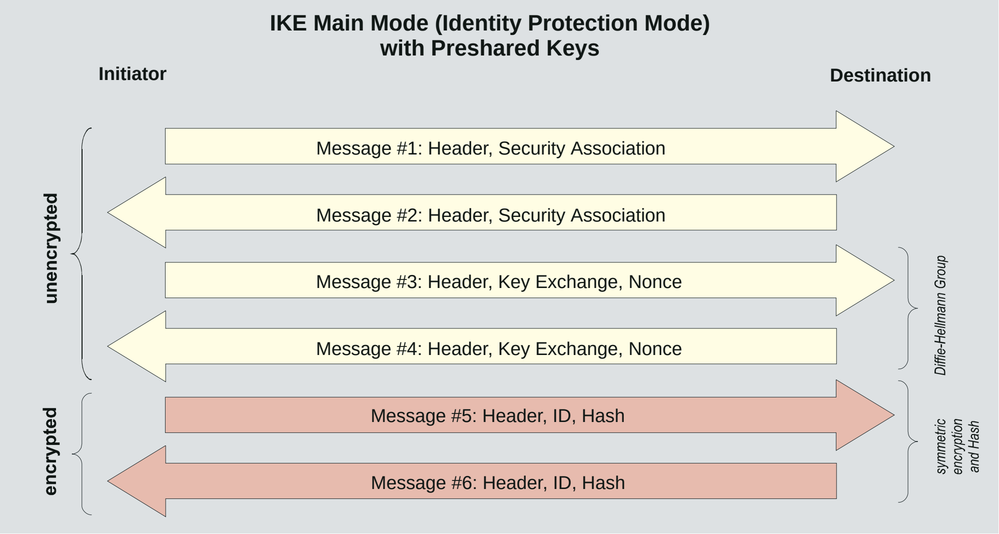
IKE Modes

Essentially two types of IKE policies can be configured. They differ according to the type of authentication, which can be either over Pre-shared Key or RSA signature. Each of the two types of Internet Key Exchange can be executed in two different modes. These are; Main Mode also referred to as Identity Protection Mode or Aggressive Mode. These modes are differentiated by the number of messages and by the encryption.

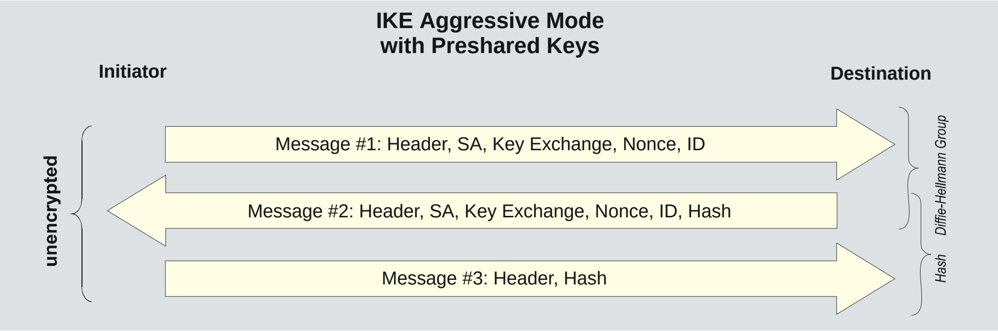
In Main Mode (standard setting) six messages are sent over the Control Channel and the last two messages are encrypted. The last two messages contain the user ID, the signature, the certificate and, if required, a hash value. This is why it is also known as Identity Protection Mode.

In Aggressive Mode only three messages are sent over the Control Channel and nothing is encrypted.

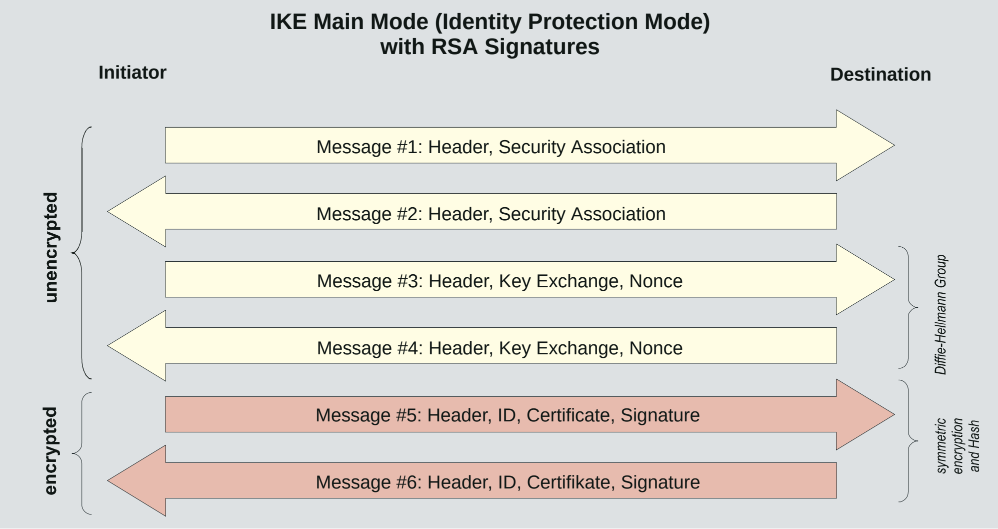
You determine the IKE mode (Exchange Mode), Main Mode or Aggressive Mode “Security” parameter fields under “Link Profiles” (for a dynamic SPD) and under “IP-Sec, Secure Policy Database” (for a static SPD). (See also → Exchange Mode).


IKE Main Mode (Identity Protection Mode)
with Preshared Keys
Initiator
Destination
unencrypted
encrypted
Message #1: Header, Security Association
Message #2: Header, Security Association
Message #3: Header, Key Exchange, Nonce
Message #4: Header, Key Exchange, Nonce
Message #5: Header, ID, Hash
Message #6: Header, ID, Hash
Diffie-Hellmann Group
symmetric encryption and Hash

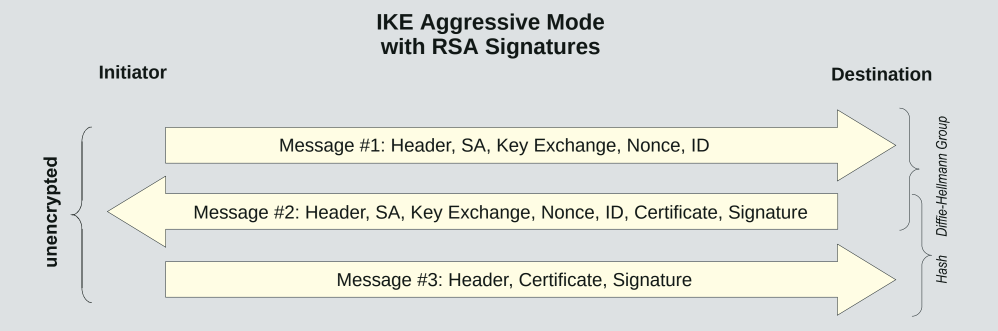
If the pre-shared key method is used in Main Mode then the client on the VPN/Gateway must be clearly identifiable by his IP address. This is because the pre-shared key will be introduced into the symmetric key calculation and encrypted before the transfer of any other information that could identify the client. However a client dialing in to the provider is not identifiable by an IP address because he receives a new one with each dial in. This means that in Main Mode only the same pre-shared key can be given out which weakens the authentication.



One possibility to avoid a general pre-shared key would be to use the Aggressive Mode (see above graphic), however in this case the client ID is not encrypted.


IKE Main Mode (Identity Protection Mode)
with RSA Signatures
Initiator
Destination
unencrypted
encrypted
Message #1: Header, Security Association
Message #2: Header, Security Association
Message #3: Header, Key Exchange, Nonce
Message #4: Header, Key Exchange, Nonce
Message #5: Header, ID, Certificate, Signature
Message #6: Header, ID, Certifikate, Signature
Diffie-Hellmann Group
symmetric
encryption
and Hash

If RSA signatures have been set (Graphic above and below), then this means that certificates will be used and thus pre-configuration of all "secrets" is no longer relevant.


IKE Aggressive Mode
with RSA Signatures
Initiator
Destination
unencrypted
Message #1: Header, SA, Key Exchange, Nonce, ID
Message #2: Header, SA, Key Exchange, Nonce, ID, Certificate, Signature
Message #3: Header, Certificate, Signature
Diffie-Hellmann Group
Hash

7.2.4 IPSec Tunneling

The compatibility with other manufactures relies on the ability to conform to the IPSec RFC's and to some drafts (official or not). The IPSec Client running in IPSec compatible mode supports the following RFC's and drafts:

RFC 2104 - Keyed-Hashing for Message Authentication
RFC 2401 - Security Architecture for the Internet Protocol
RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH
RFC 2404 - The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2406 - IP Encapsulating Security Payload (ESP)
RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 - The Internet Key Exchange (IKE)
DRAFT - draft-beaulieu-ike-xauth-05 (XAUTH)
DRAFT - draft-dukes-ike-mode-cfg-02 (IKECFG)
DRAFT - draft-ietf-ipsec-dpd-01 (DPD)
DRAFT - draft-ietf-ipsec-nat-t-ike-01 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-02 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-03 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-05 (NAT-T)
DRAFT - draft-ietf-ipsec-udp-encaps-06 (UDP-ENCAP)

- **Implemented Algorithms for Phase 1 and 2:**

Supported authentication methods for phase 1 (IKE policy)

– RSA signature.

– PSK (Pre-shared Key)

Supported symmetric encryption algorithms (phase 1 & 2)

– DES.

– 3DES.

– AES-128, AES-192, AES-256.

Supported asymmetric encryption algorithms (phase 1 & 2)

– DH 1,2,5 (Diffie-Hellmann)

– RSA

Supported hash algorithms

– MD5

– SHA-1

Additional phase 2 support

– PFS (Perfect Forward Secrecy)

– IPCOMP (LZS)

– Seamless re-keying

When a profile entry with IPSec tunneling is defined some defaults will be set automatically.

These defaults are:

– IKE phase 1 policies - Automatic Mode

– IKE phase 2 policies - Automatic Mode

– IKE phase 1 mode RSA - Main Mode.

– IKE phase 1 mode PSK - Aggressive Mode.

These policies and negotiation modi are set automatically but, alternatively they can be configured manually in the Phonebook. They can therefore be modified if necessary for other requirements.

Default mode proposals

1. With the setting “Assigned by Destination” and the “Preshared Key” field left empty, the following proposals for the IKE policy will be sent to the destination by default and a certificate will be used for authentication (refer to → IKE Policy, Phase 1 Parameter):

Notation:

```
EA    = Encryption Algorithm (Verschlüsselung)
HASH  = Hash Algorithm (Hash)
AUTH  = Authentication Method (Authentisierung)
GROUP = Diffie-Hellmann Group Number (DH-Gruppe)
LT    = Life Type (Dauer)
LS    = Life Seconds (Dauer)
KL    = Key Length (Schlüssellänge)
```

```
EA      HASH AUTH      GROUP LT      LS    KL
AES_CBC SHA  XAUTH_RSA DH5   SECONDS 28800 256
AES_CBC MD5  XAUTH_RSA DH5   SECONDS 28800 256
AES_CBC SHA  RSA       DH5   SECONDS 28800 256
AES_CBC MD5  RSA       DH5   SECONDS 28800 256
AES_CBC SHA  XAUTH_RSA DH2   SECONDS 28800 256
AES_CBC MD5  XAUTH_RSA DH2   SECONDS 28800 256
AES_CBC SHA  RSA       DH2   SECONDS 28800 256
AES_CBC MD5  RSA       DH2   SECONDS 28800 256
AES_CBC SHA  XAUTH_RSA DH5   SECONDS 28800 192
AES_CBC MD5  XAUTH_RSA DH5   SECONDS 28800 192
AES_CBC SHA  RSA       DH5   SECONDS 28800 192
AES_CBC MD5  RSA       DH5   SECONDS 28800 192
AES_CBC SHA  XAUTH_RSA DH5   SECONDS 28800 128
AES_CBC MD5  XAUTH_RSA DH5   SECONDS 28800 128
AES_CBC SHA  RSA       DH5   SECONDS 28800 128
AES_CBC MD5  RSA       DH5   SECONDS 28800 128
AES_CBC SHA  XAUTH_RSA DH2   SECONDS 28800 128
AES_CBC MD5  XAUTH_RSA DH2   SECONDS 28800 128
AES_CBC SHA  RSA       DH2   SECONDS 28800 128
AES_CBC MD5  RSA       DH2   SECONDS 28800 128
DES3    SHA  XAUTH_RSA DH5   SECONDS 28800 0
DES3    MD5  XAUTH_RSA DH5   SECONDS 28800 0
DES3    SHA  RSA       DH5   SECONDS 28800 0
DES3    MD5  RSA       DH5   SECONDS 28800 0
DES3    SHA  XAUTH_RSA DH2   SECONDS 28800 0
DES3    MD5  XAUTH_RSA DH2   SECONDS 28800 0
DES3    SHA  RSA       DH2   SECONDS 28800 0
DES3    MD5  RSA       DH2   SECONDS 28800 0
```

If a specific IKE proposal is entered in the IPSec configuration of profile settings, the same proposal will automatically be generated with Extended Authentication and sent.

2. If a string is entered in the “Preshared Key” field, the following proposals for the IKE policy will be sent to the destination by default and no certificate will be used for authentication.

```
EA      HASH AUTH      GROUP LT      LS    KL
AES_CBC SHA  XAUTH_PSK DH5   SECONDS 28800 256
AES_CBC MD5  XAUTH_PSK DH5   SECONDS 28800 256
AES_CBC SHA  PSK       DH5   SECONDS 28800 256
AES_CBC MD5  PSK       DH5   SECONDS 28800 256
AES_CBC SHA  XAUTH_PSK DH2   SECONDS 28800 256
AES_CBC MD5  XAUTH_PSK DH2   SECONDS 28800 256
AES_CBC SHA  PSK       DH2   SECONDS 28800 256
AES_CBC MD5  PSK       DH2   SECONDS 28800 256
AES_CBC SHA  XAUTH_PSK DH5   SECONDS 28800 192
AES_CBC MD5  XAUTH_PSK DH5   SECONDS 28800 192
AES_CBC SHA  PSK       DH5   SECONDS 28800 192
AES_CBC MD5  PSK       DH5   SECONDS 28800 192
AES_CBC SHA  XAUTH_PSK DH5   SECONDS 28800 128
AES_CBC MD5  XAUTH_PSK DH5   SECONDS 28800 128
AES_CBC SHA  PSK       DH5   SECONDS 28800 128
AES_CBC MD5  PSK       DH5   SECONDS 28800 128
AES_CBC SHA  XAUTH_PSK DH2   SECONDS 28800 128
AES_CBC MD5  XAUTH_PSK DH2   SECONDS 28800 128
AES_CBC SHA  PSK       DH2   SECONDS 28800 128
AES_CBC MD5  PSK       DH2   SECONDS 28800 128
DES3    SHA  XAUTH_PSK DH5   SECONDS 28800 0
DES3    MD5  XAUTH_PSK DH5   SECONDS 28800 0
DES3    SHA  PSK       DH5   SECONDS 28800 0
DES3    MD5  PSK       DH5   SECONDS 28800 0
DES3    SHA  XAUTH_PSK DH2   SECONDS 28800 0
DES3    MD5  XAUTH_PSK DH2   SECONDS 28800 0
DES3    SHA  PSK       DH2   SECONDS 28800 0
DES3    MD5  PSK       DH2   SECONDS 28800 0
```

The client sends the following IPSEC (phase2) default proposals.

Notation:

```
PROTO  - Protocol (Protokoll)
TRANS  - Transform (Transformation (ESP))
LT     - Life Type (Dauer)
LS     - Life Seconds (Dauer)
KL     - Key Length (Schlüssellänge)
COMP   - IP Compression (Transformation (Comp))
```

```
PROTO TRANS AUTH LT      LS    KL  COMP LZS
ESP   AES   MD5  SECONDS 28800 128 Yes  Yes
ESP   AES   SHA  SECONDS 28800 128 Yes  Yes
ESP   AES   MD5  SECONDS 28800 128 No   No
ESP   AES   SHA  SECONDS 28800 128 No   No
ESP   AES   MD5  SECONDS 28800 192 Yes  Yes
ESP   AES   SHA  SECONDS 28800 192 Yes  Yes
ESP   AES   MD5  SECONDS 28800 192 No   No
ESP   AES   SHA  SECONDS 28800 192 No   No
ESP   AES   MD5  SECONDS 28800 256 Yes  Yes
ESP   AES   SHA  SECONDS 28800 256 Yes  Yes
ESP   AES   MD5  SECONDS 28800 256 No   No
ESP   AES   SHA  SECONDS 28800 256 No   No
ESP   DES3  MD5  SECONDS 28800 0   Yes  Yes
ESP   DES3  MD5  SECONDS 28800 0   No   No
```

7.2.5 Further Configuration

Pre-shared Key or *RSA Signature*: According to the defaults through the other side, the automatic setting “Automatic Mode” can be changed as IKE policy to, “Preshared Key” or “RSA Signature” (certificate). If the other side expects “Pre-shared key”, then the key must be entered in the field. (The “Preshared Key” must be identical for all clients in this case.)

IP addresses and *DNS server* are assigned via the IKE Config Mode protocol (Draft 2) (currently compatible only against Cisco). All previous WAN interfaces can be used for the NAS dial-in.

The *authentication* for IPSec Tunneling is handled via the XAUTH protocol (Draft 6). If “IPSec Tunneling” is used, then additionally the following parameters must still be set in the “Identities" configuration field:

Username	=	User Name of the IPSec user
Password	=	Password of the IPSec user
User access data from configuration	=	optional

DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background for “IPSec Tunneling” when supported by the destination. The IPSec client uses DPD to check, in regular intervals, whether the other side is still active. If the other side is inactive, then an automatic connection-disconnect occurs. Using NAT Traversal is automatic with the IPSec client and is always necessary if network address translation is used on the side of the destination system device.

■ Basic configurations depending on the IPsec gateway

The configuration possibilities that you must be aware of depending on whether the Ipsec gateway supports Extended Authentication (XAUTH) and IKE config mode or not, are listed below.

Gateway does not support XAUTH

As initiator, the IPSec Client always suggests Extended Authentication as standard. This property cannot be configured. If the gateway does not support Extended Authentication, then it will not be executed.

Gateway supports IKE config mode

If the gateway supports the IKE config mode, the function “Use IKE Config Mode” in the paramaeter field “IP Address Assignment” could be activated.

Gateway does not support IKE config mode

If the gateway does not support the IKE config mode, then two configurations are possible.

1. The IP address is defined as “Manual IP address” (see → Profile Settings, IP Address Assignment), the IP address must be entered which has been specified by the gateway or by the administrator.

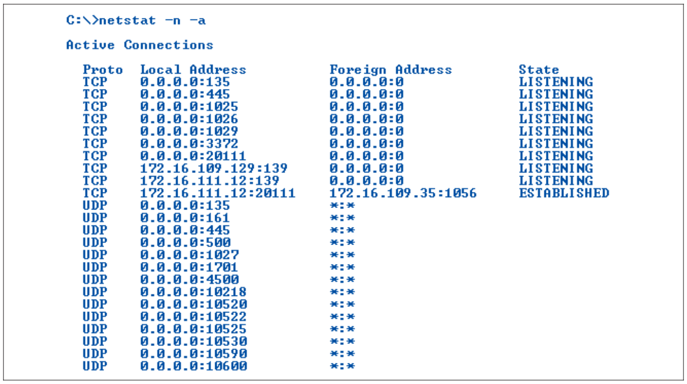
2. The function “Use local IP address” (see → Profile Settings, IP Address Assignment) causes the private IP address to be set equal to the public IP address, that the client gets per each Internet session from the provider, or if under the “LAN” connection type, the address that the LAN adapter has.

   If the “private IP address” has been set and the ”Type" is set to “IP address” in the parameter folder “Identities”, then there is no need to enter an IP address in the field for the “ID”. This is the only way to ensure that each current public IP address will be transferred to the gateway automatically for phase 1 identification.

7.2.6 IPsec ports for connection establishment and data traffic

Please note that the server requires exclusive access to UDP port 500. If NAT Traversal is used, then access to port 4500 is also required. Without NAT Traversal the IP protocol ESP (protocol ID 50) is used. Port 500, which is used for connection establishment under Windows systems, is used as standard by the IPsec policies. To change this, proceed as follows:

1. To determine which ports are currently being used by your system, you can enter the following command under the Command Prompt:
   `netstat -n -a`
   to display current network status.

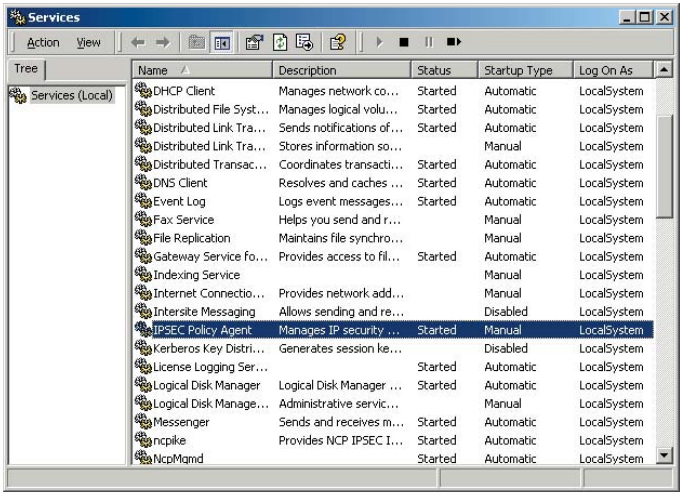


```
C:\>netstat -n -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:20111          0.0.0.0:0              LISTENING
  TCP    172.16.109.129:139     0.0.0.0:0              LISTENING
  TCP    172.16.111.12:139      0.0.0.0:0              LISTENING
  TCP    172.16.111.12:20111    172.16.109.35:1056     ESTABLISHED
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:161            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1027           *:*
  UDP    0.0.0.0:1701           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:10218          *:*
  UDP    0.0.0.0:10520          *:*
  UDP    0.0.0.0:10522          *:*
  UDP    0.0.0.0:10525          *:*
  UDP    0.0.0.0:10530          *:*
  UDP    0.0.0.0:10590          *:*
  UDP    0.0.0.0:10600          *:*
```

2. If the port is used, then the “System / Services - Administration” window must be opened in the Windows Start menu. The “IPsec policy agent” is highlighted in this window, the service stops and the “Autostart type” is set to “Manual”.



Name	Description	Status	Startup Type	Log On As
DHCP Client	Manages network co…	Started	Automatic	LocalSystem
Distributed File Syst…	Manages logical volu…	Started	Automatic	LocalSystem
Distributed Link Tra…	Sends notifications of…	Started	Automatic	LocalSystem
Distributed Link Tra…	Stores information so…		Manual	LocalSystem
Distributed Transac…	Coordinates transacti…	Started	Automatic	LocalSystem
DNS Client	Resolves and caches …	Started	Automatic	LocalSystem
Event Log	Logs event messages…	Started	Automatic	LocalSystem
Fax Service	Helps you send and r…		Manual	LocalSystem
File Replication	Maintains file synchro…		Manual	LocalSystem
Gateway Service fo…	Provides access to fil…	Started	Automatic	LocalSystem
Indexing Service			Manual	LocalSystem
Internet Connectio…	Provides network add…		Manual	LocalSystem
Intersite Messaging	Allows sending and re…		Disabled	LocalSystem
IPSEC Policy Agent	Manages IP security …	Started	Manual	LocalSystem
Kerberos Key Distri…	Generates session ke…		Disabled	LocalSystem
License Logging Ser…		Started	Automatic	LocalSystem
Logical Disk Manager	Logical Disk Manager …	Started	Automatic	LocalSystem
Logical Disk Manage…	Administrative servic…		Manual	LocalSystem
Messenger	Sends and receives m…	Started	Automatic	LocalSystem
ncpike	Provides NCP IPSEC I…	Started	Automatic	LocalSystem
NcpMgmd		Started	Automatic	LocalSystem

3. If the Autostart type change has been executed, then the command:
   `netstat -n -a`
   can be executed again. In this case UDP port 500 should no longer be listed under the active connections.

7.3 Certificate Checks

In addition to the certificate verification according to content a certificate check is executed on the Secure Client in many respects.

7.3.1 Selection of the CA Certificates

The corporate network administrator specifies which issuers of certificates can be trusted. This is done by copying the CA certificates of his choice into the \ncple\cacerts\ Windows directory. The copying over can be automated with diskettes in a software distribution, if the issuer certificates are located in the root directory of the first diskette at the installation. Afterwards issuer certificates can be automatically distributed via the Secure Update Server (see → Update Server Manual), or if the user has the requisite write authorizations in the designated directory – they can be set by the user himself (see → Display CA Certificates.

The formats *.pem and *.crt are supported for issuer certificates. They can be viewed in the monitor under the menu item “Connection – Certificates – Display CA Certificates”.

If the issuer certificate of another side is received, then the NCP Client determines the issuer, then searches the issuer certificate, first on Smart Card or PKCS#12, and then in the NCPLE\CACERTS\ directory. If the issuer certificate cannot be found, then the connection cannot be established. If no issuer certificates are present, then no connection will be permitted.

7.3.2 Check of Certificate Extensions

Certificates can experience extensions. These serve for the linking of additional attributes with users or public keys, that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written in the certificate by the issuing certificate authority.

Three extensions are significant for the Secure Client and the Secure Server:

□ extendedKeyUsage

□ subjectKeyIdentifier

□ authorityKeyIdentifier

- **extendedKeyUsage:**

If the extendedKeyUsage extension is present in an incoming user certificate, then the Secure Client checks whether the defined extended application intent is “SSL Server Authentication”. If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Please note that the SSL server authentication is direction-dependent. This means that the initiator of the tunnel establishment checks the incoming certificate of the other side, if the extendedKeyUsage extension is present, then the intended purpose must contain “SSL Server Authentication”. This applies as well for callback to the Client via VPN.

Exception: For a server call-back to the client after a direct dial-up, without VPN but with PKI, the server checks the client certificate for the extendedKeyUsage extension. If this is present, then the intended purpose “SSL Server Authentication” must be contained otherwise the connection will be rejected. If this extension is not present in the certificate, then this will be ignored.

- **subjectKeyIdentifier / authorityKeyIdentifier:**

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer’s public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA certificate is found then the connection is rejected.

The keyidentifier designates the public key of the certification authority and thus not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determining a certificate path.

In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

7.3.3 Checking Revocation Lists

The Secure Server can be provided with the associated CRL (Certificate Revocation List) for each issuer certificate. It will be copied into the \ncple\crls\ Windows directory. If a CRL is present, then the Secure Client checks the incoming certificates to see if they are listed in the CRL. The same applies for an ARL (Authority Revocation List) that must be copied into the \ncple\arls\ Windows directory.

If incoming certificates are contained in the CRL or ARL lists, then the connection is not permitted. If CRLs or ARLs are not present, then no check takes place in this regard.

7.4 Stateful Inspection Technology for the Firewall- Settings

The Stateful Inspection firewall technology can be used for all network adapters as well as for RAS connections. It is activated on the client in the telephone book under “Firewall settings” (see → Configuration parameters, Firewall settings). It is then active on the gateway if the “Protect LAN adapter” function has been switched on in the Server Manager under “Routing interfaces – General”.

The fundamental task of a firewall is to prevent hazards from other networks or external networks (Internet), from spreading in your own network. This is why a firewall is also installed at the junction between corporate network and the Internet, for instance. It checks all incoming and outgoing data packets and decides whether a data packet will be allowed through, or not, based on previously specified configurations.

Stateful Inspection is the Firewall technology that currently offers the highest possible security for Internet connections, and thus for the corporate network. Security is assured in two aspects. On one hand this functionality prevents unauthorized access to data and resources in the central data network. On the other hand, it monitors the status of all existing Internet connections as control instance. Furthermore the Stateful Inspection firewall recognizes whether a connection has opened “spawned connections” – as is the case for instance with FTP or Netmeeting – whose packets likewise must be forwarded. The Stateful Inspection Internet connection appears as a direct line to the communication partner, which may only be used for a data transfer according to the agreed upon rules. Alternative designations for Stateful Inspection are: Stateful Packet Filter, Dynamic Packet Filter, Smart Filtering, and Adaptive Screening.

Stateful Inspection conceptually unifies the protective possibilities of packet filter and application level gateways; this means it integrates the functions of both security processes as a hybrid and works on the network layer as well as on the user layer. With “condition-dependent packet filtering” not only are the Internet and transport layer taken into consideration, but the dependencies from the state of a connection are also taken into consideration. All current and initiated connections are stored with address and allocated port in a dynamic connection table. The Stateful Inspection filter decides which packets belong to which connection based on a specified raster (information). States can be: connection establishment, transfer, or connection disconnect, and they apply for TCP as well as for UDP connections. An example using a Telnet session: The state “Connection establishment” is defined in that user authentication has yet taken place. If the user has logged in with user name and password, then this connection is set to the “normal connection” state. Because the respective state of a connection is constantly monitored, access to the internal corporate network remains denied to unauthorized parties.

The advantage relative to static packet filters is that the decision whether an NCP Secure Gateway or Client will forward a packet or not, is not based on source address, destination address or ports. The security management also checks the state of the connection to a partner. Only those packets are forwarded that belong to an active connection. Data packets that cannot be assigned to an established connection are rejected and recorded in the log file. New connections can only be opened according to the configured rules.

In the simplest firewall function, only the incoming and outgoing connections are tested and monitored relative to the protocol (TCP/IP, UDP/IP, ICMP, IPX/SPX), the appropriate ports, and the participating computers. Connections are permitted or blocked depending on a specified system of rules. Further tests (such as content or transferred data) do not take place.

The Stateful Inspection filters are a further development of the dynamic packet filter and offer a more complex logic. The firewall checks whether a connection allowed on the port filter can also be established for the defined purpose.

The following additional information about a connection is also managed:

– Connection identification number
– State of the connection (such as establishment, data transfer, disconnect)
– Source address of the first packet
– Destination address of the first packet
– Interface through which the first packet came
– Interface through which the first packet was sent

Based on this information the filter can decide which subsequent packets belong to which connection. Thus a Stateful Inspection system can also eliminate the UDP problem. This involves the relative ease with which UDP packets can be forged, such as is the case with UDP-based DNS service. Because Stateful Inspection filters can note the current status and context information of a communication relationship, it is necessary that source and destination address as well as source and destination port, and also the DNS header in the query packet be included when saving the status and context information. The system executes an interpretation on the application layer.

Example: An incoming connection to port 21 of a computer is an FTP connection for a pure port filter. An additional test does not take place. On the other hand, the Stateful Inspection filter additionally checks whether the data transferred via this connection belong to an established FTP connection. If not, then the connection will be disconnected immediately. In addition, a Stateful Inspection filter is able to adapt rules depending on necessary communication processes. If, for example, an outgoing FTP connection is allowed, then the firewall also automatically enables the establishment of the associated reverse channel. The corresponding information (ports) is read out of the control connection.

One advantageous aspect of Stateful Inspection filters is the capability to check the data on all protocol layers (this means from the network layer to the application layer). Thus for example an FTP-GET can be allowed, however an FTP-PUT can be prohibited. A positive effect of the increased intelligence relative to conventional packet filters is the option of assembling individual packets during a communication relationship, and thus bring extended possibilities for user authentication to the application. Stateful Inspection filters are not immune to certain attacks that take place on the lower protocol layers as a consequence of the undependable separation of the network segments. Thus for instance, fragmented packets (usually from outside to inside) will be allowed through without further testing.

Abbreviations and Technical Terms

3DES

TripleDES. Standard of Encryption with 112 Bits.

AES

Abbreviation for Advanced Encryption Standard. It is a European development of Belgian encryption experts Joan Daemen and Vincent Rijmen (“Rijndael algorithm”), and supercedes DES (Data Encryption Standard). This is an encryption algorithm that has key lengths of up to 256 bits. Thus N to the 256th power is the measuring unit for the number of possible keys that can be generated with this algorithm. In spite of increasing processor speeds it is expected that the AES algorithm will offer acceptable security for the next 30 years. AES will soon find wide distribution in VPN and SSL encryptions.

AH

Authentication Header RFC 2402

Analog Interface

This is an interface for connecting analog devices (e.g. modems, facsimile group 3 machines, analog telephones etc.). The current international standard connector for analog devices is RJ11.

Asymmetric Encryption

(Public Key Process) In an asymmetric encryption each participant has two keys: a secret private key and a public key. Both keys stand in a mathematically defined relationship to each other (2 Key Service). The participant’s private key is strictly secret; the public key is available to anyone. Key management is straightforward even with large numbers of participants. For example: Two keys per participant generate a total of 2000 keys to enable secure communication for 1000 participants in all sender-recipient combinations. RSA is the best-known asymmetric encryption process. The disadvantage of the asymmetric encryption process is that it is calculation-intensive and thus comparatively slow.

Basic Connection (So / BRI = Basic Rate Interface)
A type of ISDN connection with So-interface. (“S” stands for subscriber interface: user interface). It consists of a D-Channel (bandwidth: 16 kBits/s) for controlling and two B-Channels (bandwidth: 64 kBits/s each) for data transmission.

Basic Rate Interface (BRI)
An ISDN subscriber service that uses 2 B-Channels (64 Kbps) and 1 D-Channel (16 Kbps) to transmit data, audio, voice and video signals over a digital dial-up circuit. BRI’s are available from your local PTT.

BCP
Bridge Control Protocol

BITS
Bump In The Stack - A type of IPSec implementation.

BITW
Bump In The Wire - A type of IPSec implementation.

Blowfish
Encryption Standard with 128/448 Bit

Browser (Web Browser)
This is the user interface to the Internet. With its HTTP (Hypertext Transfer Protocol) capability it can handle different formats (for example HTML, GIF, CAD) that are required for a multi-media (sound and graphics) representation of the information.

CA (Certification Authority)
Also Trust Center (for example D-trust, a combined undertaking of Debis and the Federal Printing Office). With PKI Manager Software a CA issues digital, signed confirmations (certificates) and stores them on a Smartcard (Chipcard). A CA can be a private service provider or a public institution. These certifying authorities do not need government permission and the private service provider or public institution is liable for the correctness of the certificates.

CAPI
Common Application Program Interface. This interface is designated as a common ISDN API in ISDN and corresponds to the PCI interface (Programmable Communication Interface). The interface direct access to ISDN and the lower protocol layers (Layers 1-3). Higher-level protocols (applications) like telex and file transfer can be used regardless of the hardware platform implemented. There are two versions of CAPI, 1.1 and 2.0. The ISDN applications are programmed accordingly either for CAPI 1.1 or CAPI 2.0, or for the specific CAPI requirements. A hybrid CAPI allows implementati-

on of application software for CAPI 1.1 as well as for CAPI 2.0 (see Hybrid CAPI).

CCP Compression Control Protocol

Certificates Certificates are issued by a CA (Certification Authority) with a PKI Manager (software) and stored on a Smartcard. This Smartcard contains digital signatures in addition to the Certificates. These digital signatures are equivalent to a digital personal identity card.

CHAP Challenge Authentication Protocol

CLI Calling Line Identification (Caller ID - Euro-ISDN)

COSO Charge One Side Only. The low level callback is negotiated via D-Channel and uses call waiting via D-Channel. This method is very popular, because as opposed to PPP no local charge is assessed to the caller when dialing-up or connecting to the remote destination. The caller initiates the request for a connection on the ISDN D-Channel. The receiver establishes the connection and is charged.

Cryptography Applications are encryption, electronic signature, authentication, and Hash Value Calculation. These are mathematical processes that are used with a key.

CTAPI Interface to Smartcard Readers

CUG Closed User Group (Euro-ISDN)

DES Data Encryption Standard

DHCP Communicating with DHCP (Dynamic Host Control Protocol) means that an IP Address is automatically assigned to you for every session.

Directory Service Remote Accesses like Email addresses, telephone numbers etc. are stored in directories of various databases. Two problems are associated with this directory multiplicity, they are (1) large volumes of the same data must be captured many times (2) individual entries are not linked to each other. The maintenance required is enormous and inconsistencies cannot be ruled out. A standardized procedure is required that will facilitate the capture and maintenance of all information in a central directory. NCP Security Management supports the standardized protocols RADIUS (Remote Authorization dial-In User Service), and LDAP (Lightweight Directory Access Protocol). The latter insures access to centralized directory services.

DMZ Demilitarized Zone - an area between the Firewall and the enterprise network with Web Servers, Email Servers and VPN Servers.

DNS The Domain Name Server (DNS) makes the IP address available for an Internet session after dial-in with user name and password. It provides additional Internet routing in that it retranslates the given desired destination names into IP addresses and creates the connection to this address.

DNS Server A computer with a database containing all relevant host computers (domain name addresses) and their corresponding IP addresses. When queried, the DNS Server responds by returning the IP address corresponding to the domain name address.

D-Channel Protocol The D-Channel insures that terminals can communicate with the network. Among other things it monitors connection setup and breakdown. It includes Layers 2 and 3. HDLC is implemented on Layer 2 in ISDN for the logical data transfer. The actual D-Channel protocol resides on Layer 3. Currently DSS1 is available throughout Europe as D-Channel protocol.

DSA Directory System Agent

DSS1 Abbreviation for the European standard Digital Subscriber System No.1. This is the European ISDN protocol for D-Channel.

DUA Directory User Agent

ECP Encryption Control Protocol

EDI This is an abbreviation for Electronic Data Interchange, which is a set of standards for controlling the transmission of business documents (e.g. purchase orders and invoices) between computers.

ESP Encapsulating Security Payload RFC 2406

Euro-ISDN The International Telecommunications Union (ITU) standard for European ISDN, refers to the D-Channel Protocol DSS1 as well as various service features (e.g. Time & Charges, Completion of Calls to Busy Subscriber, Call Forwarding, Call Waiting, etc.). In Euro-ISDN the individual terminals are addressed with the D-Channel protocol DSS1 with the multiple subscriber number (MSN).

Firewall A division between public network and private network. It is a protection mechanism that regulates the station access. A firewall computer seals off a network from unauthorized access, particularly from the WAN side. For example, authorization of incoming and outgoing connections is regulated by filtering out certain network participants and network services and by determining access rights. From the WAN perspective it is usually web servers, Email servers, and VPN servers that are located behind the firewall in the DMZ.

FTP File Transfer Protocol. Based on TCP and TELNET (Port 21).

FTP Server A fileserver that supports the File Transfer Protocol enabling users to download or upload files through the Internet or any other TCP/IP Network.

GPRS Standard for fast handy communication

GRE Generic Router Encapsulation. CISO specific tunneling protocol.

GSM Global System Mobile. Standard for cellular communications

Hash Value see Signature

HBCI Standard for Smartcard Readers (Online Banking)

HTTP Hypertext Transfer Protocol. (Port 80)

Hybrid Encryption High performance and high security: Hybrid encryption combines the advantages of symmetric and asymmetric processes. While communication content is secured with fast symmetric algorithms, participant authentication and key exchange occur on the basis of asymmetric processes. Actual document data encryption is determined by a random number (session key) that is generated for each individual communication connection. This one-time key is encrypted with the recipient's public key and the message is added. Then the recipient reconstructs the session key with his private key and decrypts the message.

IETF

Internet Engineering Task Force.

IKE

Internet Key Exchange, which is part of IPsec for secure key management, separate security association negotiation, and key management protocol RFC 2409.

Internet

The Internet is a worldwide open computer network. It is open to all. Every company and each individual can connect to the Internet and can communicate with all other connected users regardless of the computer platform or the respective network topology. A general shared network protocol is necessary to insure that data exchange between the different computers and networks is possible (see TCP/IP).

Intranet

A network within a company or organization employing applications associated with the Internet, such as Web pages, Web browsers, FTP Sites, E Mail, etc. However these are only accessible to those within the company or organization.

IP Address

Each computer in the Internet has an IP address (Internet Protocol Address) that clearly identifies it for as long as it is part of the Internet. An IP address is 32 bits long and consists of four numbers separated from each other by a dot. There are 8 bits available for each number thus it can take on 256 values. However the total number of possible IP addresses remains limited. The internet user thus does not receive a one-time non-modifiable number assigned to him, rather for every one of his sessions he gets the IP address that has not yet been assigned. The IP addresses are assigned for the duration of a time slice. This assignment of address is usually an automatic PPP negotiation over DHCP. Special programs can translate the IP address into a name. These programs run on a Domain Server.

IP Network Address Translation IP Network Address translation is already setup when the workstation software is installed and it is activated as default when a new destination system is created! When IP network address translation is used all transmitted frames are sent with the negotiated (PPP) IP address. The workstation software translates this official IP address into the system's own Internet address, or in the case of a workstation, into its own user defined IP address. In general it is possible with NAT to work in a LAN with unofficial IP addresses that are not valid in the Internet and, in spite of that fact, access the Internet from the LAN. To make this possible the unofficial IP addresses are translated into official IP addresses by the software. This saves official Internet addresses, that are not available in unlimited numbers on the one hand, and on the other hand NAT establishes a certain protection (Firewall) for the LAN.

IPCP Internet Protocol Control Protocol

IPsec IETF Standards: RFC's 2401-2412 (12/98)

IPX Internet Packet Exchange, Netware protocol from Novell

IPXCP Internetwork Packet Exchange Control Protocol

ISDN Integrated Services Digital Network. A digital network that integrates all narrow band communication services (for example telephone, telex, fax, teletext, videotext) consisting of channels with a transfer speed 64.000 bit/s. A basic connection in the so-called narrow band ISDN has three transmission channels: channel B1 64,000 bits/ s, B2 64,000 bits/s, D-Channel 16,000 bits/s. The total transmission rate is 144,000 bits/s. By the end of the millennium this network should be uniformly extended throughout Europe. The specifications for ISDN are worked out by ITU and CEPT.

ISDN Adapter The products of the NCP Arrow family are ISDN adapters. They make it possible to connect existing non-ISDN capable terminals to the ISDN network. The adapter handles the software and the hardware adaptation of the terminal interface to the ISDN interface (So). An ISDN adapter with Upo terminal interface enables the conversion of ISDN two wire interface Upo (range 3.5 km) on bus-capable ISDN 4 wire interface So (range 150 m) with ISDN TK equipment in accordance with Telekom Guidelines.

ISP Internet Service Provider

ISO/OSI Reference Model The ISO standardized model that describes communication in 7 layers (7. Application Layer, 6. Presentation Layer, 5. Session Layer, 4. Transport Layer, 3. Network Layer, 2. Data Link Layer, 1. Physical Layer). Data transmitted in a network are processed consecutively 7 -1 as above. The order is reversed on the receiver side.

L2F Tunnel / VPN protocol Layer 2 Forwarding

L2TP Tunnel / VPN protocol Layer 2 Tunneling Protocol

L2Sec NCP designation, functional description in RFC 2716

LCP Link Control Protocol

LDAP Lightweight Directory Access Protocol (see Directory Service)

MAC Address This stands for Medium Access Control Layer Address. It is a physical address in the network.

MIB Management Information Base

MD5 Message Digit 5. Used to generate a hash value.

Name Exact Internet name, it is supposed to make it easier for the users to work on the Internet. The names are entered in the Internet browser and are then translated into IP addresses by the Domain Server.

NAS Network Access System

NetBios Network Basic Input Output System an interface that offers datagram and stream-oriented communication.

OCSP Abbreviation for Online Certificate Status Protocol. It is a protocol used for online verification of certificates.

PAP

PAP Password Authentication Protocol. Security mechanism inside the PP for authenticating the other side. PAP defines a method according to which the establishment of a connection whereby the rights of the sender are checked based on a user name and password. In this process the password is sent over the line in clear text. The recipient compares the parameters with his own data and if in agreement releases the connection.

PBX

An abbreviation for Private Branch Exchange, which is an automatic telephone switching system that enables users within a company to place calls to each other without having to go through the public telephone network. Users of course can also make calls and receive calls from the public telephone network.

PC/SC

Interface to Smartcard readers

PEM

An older form of Soft Certificates (without private key).

Personal Firewall

Client software security mechanisms combine tunneling processes and personal Firewalling, IP Network Address Translation (IP-NAT), as well as universal filter mechanisms. IP Nat is of central importance then it ensures that only outgoing connections from the computer to the Internet are possible. Incoming data packets are checked on the basis of refined filtering for precisely defined characteristics and are discarded if there is no agreement. This means that the Internet port of the respective computer is completely camouflaged and the establishment of undesired connections is impossible.

PIN

Personal Identification Number

PKCS

Abbreviation for Public Key Cryptography System, an encryption system with public key.

PKCS#10

A method defining how a certificate is transferred from the PKI manager to the CA (Certification Authority). Usually via Http - encrypted with SSL as Https.

PKCS#11

Basis for Smartcard standards

PKCS#12

Soft certificate. A standard that describes the data structure syntax.

PKCS#15

Smartcard pointer description. Indicates where what will be found on the Smartcard

PKI

This is used for Key Management. Transaction-based security requires a clear partner authentication by means of certificates that have been issued by a trustworthy PKI. Particularly for E-commerce PKI offers the framework for confidentiality (secrecy), Integrity (counterfeit security), authenticity (identity security) and indisputability.

PoP

Point of Presence

POP3

Protocol, used for downloading Emails. Counterpart to SMTP (Port 10).

PPP

Point-to-Point Protocol. Transmission protocol in connection oriented networks.

PPP negotiation

In a PPP negotiation the IP address is assigned automatically after the logon at the provider.

PRI

Primary Rate Interface. (ISDN interface, primary multiplex S2m with 30 B-Channels and 2 D-Channels.

Radius

Remote Authorization Dial-In User Service, see Directory Service

RA

Registration Authority. For the most part the registering location is the site that accepts the certificate application. The RA is also the site where the loss or deterioration of a valid certificate is reported. It is also the site that issues revocation lists for certificates that have become invalid.

RAS

Remote Access services. Company Specific (Microsoft) dial in help for Remote Access Routing Information Protocol, also routing mode.

Revocation list

The revocation list includes client certificates that have been revoked or blacklisted. When a user for example notifies the CA that their Smartcard has been stolen, the certificate will be revoked by the CA and entered in the Revocation List. Certificates that expire will not be listed in a revocation list. Revocation Lists are regularly updated.

RIP

Routing Information Protocol, also Routing Mode

RFC

Request for Comment. Blueprint for a standard or a pre-standard that is in discussion and will be kept in the list of RFC's as long as it proves itself in practice. Earlier forms of RFC's are drafts.

Routing Tables

Routers require information about the best routes from the source to the destination for route selection in the network. With the routing table's help these segments are calculated. With static routing the tables have been firmly defined. In dynamic routing the router receives information about the network through router information protocols (for example RIP, NLSP, OSPF) that is collected and continuously updated in self-learning router tables.

RSA

The first procedure that fulfilled the demands for public key cryptographics. Invented 1977 by Ron Rivest, Adi Shamier and Leonard Adlemann.

SHA

Secure Hash Algorithm, see also Signature

Signature

A digital signature requires the generation of a mathematical link between document and the secret personal signature key of the participant. The document sender generates a checksum or so-called Hash Value, this he in turn codifies with his secret key and thus creates a digital signature addition to the original document. The document recipient can check the signature with the sender's public key by constructing on his side the Hash value from the message and comparing it to the encrypted signature. Because the sender's signature is directly bound into the document every later modification would be noticed. Also interception or eavesdropping of the signature through data interception is to no avail. The digital signature cannot be emulated or copied because it uses the secret key. It is impossible to determine the secret key from the signature.

Smartcard

If you use the functionality of the Smartcard after CHAP Authentication (User ID and Password) then the Strong Authentication with the stored certificates on the Smartcard and the Gateway will be executed. Among other things the user certificate, the root certificate, and the secret private key, are stored on the Smartcard. The Smartcard can only be used with a valid PIN.

SMTP Simple Mail Transport Protocol. Internet standard to distribute Email. Based on TCP (Port 25). It is text oriented.

SNA Systems Network Architecture. Hierarchically oriented network for the control of terminals and for application access support in IBM host systems.

SNMP Simple Network Management Protocol. Network management protocol based on UDP/IP.

Source Routing The possibility to optimize route selection between bridges in Token-Ring networks. With SNA, route information hanging on the datablock is also transmitted. In this manner the confirmation route is also clearly manifest.

SPD Security Policy Database

SSL Secure Socket Layer. According to the SSL protocol Dynamic Key Exchange can be used. SSL, developed by Netscape, in the meantime has be-come the standard protocol for Dynamic Key Exchange

SSLCP Secure Socket Layer Control Protocol

STARCOS Operating system for Smartcards

Symmetric Encryption Sender and recipient use the same key for symmetric encryption and decryption. Symmetric algorithms are very fast and very secure - only if the key transfer between the sender and the recipient is not endangered. If an unauthorized person is in possession of the key then this person can decrypt all messages. In other words using the key he will appear as the message sender. If for larger groups of participants symmetric encryption is to be used so that each participant can only read messages addressed to him, then an individual key is required for each sender-recipient pair. This results in a somewhat cumbersome key management. For example, for 1000 participants 499,500 different keys are necessary (!) to support all possible relationships. Currently the best-known symmetric encryption is the DES algorithm.

TCP/IP An abbreviation for Transfer Control Protocol / Internet Protocol, which is a network protocol used by computers to communicate with each other. TCP/IP can be used in most any LAN or WAN, regardless of the underlying topology (Token Ring, Ethernet, X.25, ISDN, Frame Relay etc.). TCP/IP also includes various Internet standards: FTP: File Transfer Protocol (for File Transfer) / SMTP: Simple Mail Transport Protocol (for E Mail) / TELNET: Teletype Network (for Terminal Emulation) / RLOGIN: Remote Login (for remote control purposes)

TECOS Operating system for Smartcards (V. 1.2, 2.0)

Token Ring Ring structure network topology from IBM.

UDP User Data Protocol. This builds directly on the underlying Internet protocol. It was defined to also provide application processes with the direct possibility to send datagrams. UDP delivers over and above the capabilities of TCP/IP simply a port number and checksum of the data. Due to the lack of overhead such as receipts and security mechanisms it is particularly fast and efficient.

UMTS Universal Mobile Telecommunications Service. Future Standard for fast mobile phone communication.

VPN Virtual Private Network. A VPN can be implemented as a virtual network over all IP carrier networks - that means the Internet as well. Two specifications have crystallized for the realization of a VPN: L2F (Layer 2 Tunneling) and L2TP (Layer 2 Tunneling Protocol) both processes serve to establish a tunnel that can be considered a “virtual leased line”. In addition to IP frames also IPX data, SNA data, and NetBios data are transparently transmitted over such a logical connection. At the end of the tunnel the data packets must be interpreted and transformed into a DataStream on the basis of the protocol used.

WAN Abbreviation for Wide Area Network, which is a communications network that connects networks that are separated geographically. (normally LAN = Local Area Network). WANs are normally provided by PTTs or Carriers and generally speaking offer high speed connection (64 Kbps - 2 Mbps or higher).

WAP Wireless Application Protocol. Developed by Nokia, Ericsson and Motorola.

WINS An abbreviation for Windows Internet Naming Service, which is a Windows NT Server method for linking a computer's host name to its address. This was the original Microsoft derivative of DNS, and is also referred to as INS = Internet Naming Service.

X.25 An ITU (International Telecommunications Union) recommendation that specifies the connection between an end device (e.g. PC or terminal) and a packet switched network. X.25 and is based on three definitions. (1) the physical connection between the end device and the network, (2) the transmission access protocol, and (3) the implementation of virtual circuits between network users. Together, these definitions specify a synchronous, full duplex end device (terminal) to network connection.

X.509 v3 A Standard of Certification

Index