Bintec
Secure IPSec Client

Version 1.0
July 2004

Total production of this manual:
Michael Lösel
Documentation + Publication
ml-service@t-online.de
Arndtstraße 5
D-90419 Nürnberg
Germany

Telephone: +49-911-355916
Fax: +49-911-3665718

How to reach Bintec:
Bintec Access Networks GmbH
Suedwestpark 94
D-90449 Nuremberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0

Liability

While every effort has been made to ensure the accurancy of all information in this manual, Bintec Access Networks GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of ist terms of scale and delivery.

The information in this manual is subject to change without notice. Additional information can be found at www.bintec.de.

Contents

1. Product Overview

This manual describes Installation, Configuration, Features and User Interface of the Bintec Secure IPSec Client and its Components.

The Bintec IPSec 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 Bintec website www.bintec.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.

Chapter 1: Product overview with brief description of the performance range of the software
Chapter 2: Installation instructions
Chapter 3: Description of the graphic user interface, as well as the configuration possibilities
Chapter 4: Description of the parameters listed in the profile settings
Chapter 5: Description of a connection establishment
Chapter 6: Examples and explanations, particularly for IPsec
Glossary with abbreviations and terms
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 Bintec Secure IPSec Client – Universal Solution for Secure VPN Solutions

The Bintec Secure IPSec Client can be used in any VPN environment. The client communicates on the basis of the IPsec standard 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 Client Software emulates an Ethernet LAN adapter. The Client has additional features that introduce the user into a holistic remote access VPN solution.

The IPSec 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)
- ☑ Higher speed in the ISDN (channel-bundling)
- ☑ Saving telephone charges (charges and connection management)
- ☑ Convenient operation (graphic interface)

1.3 Performance range

The IPSec client supports all major operating systems (Windows 98se, ME, NT, 2000 and Windows XP). Connecting to the corporate network is media-type independent, e.g. in addition to ISDN, PSTN analog telephone network, GSM, GPRS, and xDSL, LAN technologies such as WLAN (on the corporate campus and hotspots) or local area networks (branch office network) are also 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
– in the home office via xDSL, cable, or ISDN

1.3.1 Client Monitor – graphical user interface (GUI)

The graphical user interface (see → Client Monitor) of the IPSec client provides transparency during the dial-in process and data transfer. Among other things it provides information on actual data throughput.

The user knows whether his PC is online at all times, and if necessary what charges have been incurred.

1.3.2 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
– controlling the bandwidth (channel bundling) in the ISDN
– integrated personal firewall mechanism
– protection against "automatic dialers"

1.3.3 Line Management

In order to guarantee fast and cost effective data communications over public networks, all products include various automated processes and features for efficient Line Management, such as: Inactivity Timeout (Short Hold), Multilink support (Channel Bundling), Data Compression, Filtering, Spoofing, Local Termination etc. Optimal economy of scale achieved through intelligent features that minimize transmission times and connection costs.

This takes care of optimized costs transparence and a better overview: It allows the system administrator to determine certain limits for remote connections (e.g. maximum connection time, maximum number of connections established and units of charge) as well as automatic monitoring of the same by having the connection control in operation.

1.3.4 Personal Firewall

The IPSec client provides all the personal firewall functionalities to fully secure the workstation against attacks from the Internet, wireless LAN, or the local network. 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 Internet 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 accordance a sophisticated filter, which rejects those that match the defined parameters. Source ports are also screened to prevent any masquerading. In other words: 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 IPSec client becomes part of a Public Key Infrastructure (PKI).

Public Key Infrastruktur

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.

2. Installation

A Setup program performs the installation of the Client Software quickly and smoothly. The following text describes the procedures for installing the Client Software under Windows 98/ME and Windows NT/2000/XP.

Prior to executing Setup be sure that the following prerequisites are fulfilled.

2.1 Installation Prerequisites

System Requirements

In order to be able to communicate with the Client Software it is essential to have either Microsoft Windows 98, Windows ME, Windows NT (3.5 or later) with the service pack 4.0 (or later), Windows 2000 or Windows XP installed on your PC (min. 32 MB RAM).

During the installation you are asked to have your or disks ready, as these will be needed for updating your PC's driver database files. Please insert these when prompted to do so.

Remote Destination

The parameters of the remote destination must be entered in the profile settings. In order to communicate with the remote destination it must support one of the following media types: ISDN, PSTN (analog modem), LAN over IP or PPP over Ethernet (PPPoE).

Lokales System

One of the following communication devices and its respective drivers must be properly installed on the Client Software PC.

- **ISDN adapter (ISDN)**

The device (e.g. internal or external adapter) must support the ISDN CAPI 2.0 Kernel Mode standard. When using PPP Multilink the software can bundle up to 8 ISDN B-Channels. Any ISDN device supporting the ISDN CAPI 2.0 can be used. Please check your device to be sure that such a driver is available. The Client Software does not support TAPI based ISDN devices.

- **Analog Modem (Modem)**

The Client Software can communicate with any industry standard analog PC modem, provided that it and the modem drivers have been properly installed and the modem initialization string and the COM port definition for the modem is correct. The modem has to support Hayes AT commands.

Mobile (cellular) telephones can also be used for data communication, after the associated software has been installed that presents itself to the client precisely as if it were an analog modem. The serial interface, IR (infrared) interface, or Bluetooth can be used as interface between mobile phone and PC. The opposite side must have the appropriate dial-in platform depending on the transfer rate (GSM, v.110, GPRS or

HSCSD). The initialization string in the Secure Client modem configuration must be obtained from the ISP or the manufacturer of the mobile (cellular) phone.

- **LAN adapter (LAN over IP)**

When the Link Type LAN has been defined the Client Software may be used as a IPSec client in a LAN that communicates across a LAN network and associated router to a central site VPN Gateway. When defined as a LAN Client, the Client Software can also be used as a VPN or VPN/PKI plugin for Microsoft's RAS (Dial-Up Network) client.

Adapters for a wireless LAN (WLAN adapter) are handled exactly like normal LAN adapters. "LAN (over IP)" must also be selected for WLAN.

- **Broadband Device (xDSL (PPPoE))**

Cable modems, splitters (e.g. for ADSL), etc. can be used in conjunction with PPP over Ethernet (PPPoE), which is supported by the Client Software.

- **xDSL (AVM - PPP over CAPI)**

The link type "xDSL (AVM - PPP over CAPI)" has been added in the "Destination" configuration field in the telephone book. If an AVM Fritz DSL card is to be used then this link type may be selected . AVM specific initialization strings may be entered in the field "Destination Phone Number" ("Dial-Up Network" group) for the connection.

It is recommended to use the standard setting "xDSL (PPPoE)" with Windows operating systems as this provides direct communication over the network interfaces.

No additional network card is necessary with the AVM Fritz! DSL card.

Prerequisites for Strong Security

If you are using the Client Software with certificates (X.509), then the following prerequisites must be fulfilled:

- **TCP/IP**

The protocol TCP/IP must be installed on your PC.

- **Smart Card Reader**

The Client Software supports all Smart Card readers that are PC/SC conform. Subsequently such readers will only be entered in the Client Software Smart Card reader list after the Smart Card reader including the associated driver software has been installed on the PC. The Client Software detects the Smart Card reader automatically after the PC has been booted. The Smart Card reader can then be selected as described above and used accordingly.

In order to use the features of the Smart Card, configure the Smart Card by selecting "Configuration → Certificates" in the pull-down menu of the Client Software Monitor. When you insert your Smart Card in the Smart Card reader, you can enter your PIN.

■ Smart Card Reader (CT-API conform)

Please note the following instructions when using a Smart Card reader that is CT-API conform:

☑ The current software includes drivers for the Smart Card readers SCM Swapsmart and SCM 1x0 (PIN Pad reader). These Smart Card readers can be set in the Monitor under "Configuration → Certificates". If, however, the Smart Card reader does not work with the drivers, which are included in the software, or a Smart Card reader is to be used, which does not show up in the configuration selection of supported readers, then ask the supplier or producer of the Smart Card (or the respective website) reader for the current hardware driver and install it. In this case the client software requires some modifications:

☑ Use an ASCII editor to edit the NCPPKI.CONF file. You find this file in the WINDOWS\SYSTEM directory (Windows 95/98) or in the SYSTEM32 directory (Windows NT/2000). Enter the name of the connected Smart Card reader as "ReaderName" (xyz) and the name of the installed driver as DLLWIN95 or DLLWINNT respectively. The default name for CT-API conform drivers is CT32.DLL.

Important: Only those drivers that have been appropriately set with "visible = 1" will be displayed in the list!

Modulname	= SCM Swapsmart (CT-API)	→ xyz
DLLWIN95	= scm20098.dll	→ ct32.dll
DLLWINNT	= scm200nt.dll	→ ct32.dll

☑ After rebooting the PC the new "ReaderName" is displayed in the Monitor under "Configuration → Certificates → Smart Card reader". Now you select that Smart Card reader.

■ Smart Cards

Currently, the following Smart Cards are supported:

☐ Signtrust

☐ NetKey 2000

☐ TC Trust (CardOS M4)

■ Soft Certificates (PKCS#12)

Instead of a Smart Card you can also use soft certificates or tokens.

Smart Cards or Token (PKCS#11)

Drivers in the form of a PKCS#11 library are supplied with the software for the card reader or token. This driver software must first be installed. Then the NCPPKI.CONF file must be edited.

☑ Edit the NCPPKI.CONF file located in the windows\system directory (Windows 95/98) or system32 directory (Windows NT/2000), with an ASCII editor by entering the name of the connected reader or token (xyz) as “module name”. The name of the DLL must be entered as PKCS#11-DLL. The associated “Slotindex” is manufacturer-dependant (standard = 0).

Important: Only those drivers are visible in the list that have been set to visible with “visible = 1”.

Modulname = xyz
PKCS#11-DLL = Name of the DLL
Slotindex =

☑ After rebooting the PC the new “ReaderName” is displayed in the Monitor under “Configuration → Certificates → Smart Card reader”. Now you select that Smart Card reader.

2.2 Installing the Client Software

The initial installation steps for the Client Software are almost the same for both Windows 98/ME and Windows NT/2000/XP.

You can download the software as ZIP file from the Bintec websites at www.bintec.de.

Please note when installing the Software under Windows XP:

Microsoft Windows XP informs the user as soon as a driver software is being installed which is not licensed by Microsoft. Windows XP runs a Microsoft specific “compatibility test” and warns the user not to install the software. This test does not check the compatibility of the software with Windows XP. Since the client software is not licensed by Microsoft, the warning occurs when the client is installed on a Windows XP machine. What to do:

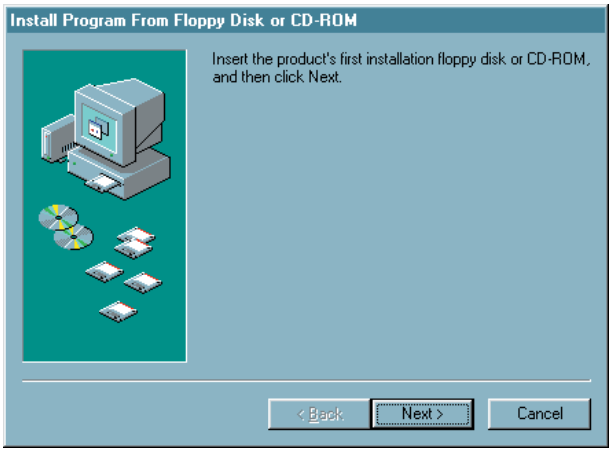
☑ You can modify the Windows XP default settings so that any software can be installed without the Microsoft compatibility check. Open the Windows Control Panel and then “System (Properies) - Driver Signing”. Set the install procedure to “Install the software anyway and dont’t ask for my approval”!

☑ You can ignore the warning when installing the client. After the warning pops up you click on “proceed Installation” Windows XP will let you install the client adapter. The installation will not have any negative effect on the operating system.

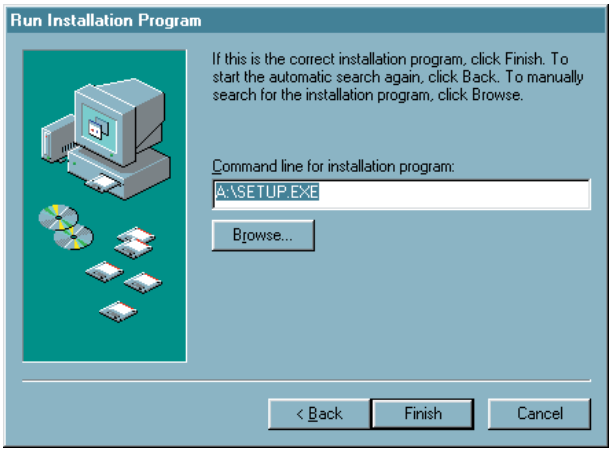
2.2.1 Default Installation

First you copy the ZIP file you have got with a download or with the CD onto the hard disk of your PC. After this extract the data in any directory. Extracting the data the directories “DISK1”, ”DISK2”, “DISK3” etc. will be made automatically. To install the software select in the windows main menu ”Start → Settings → Control Panel.”

Select “Add/Remove Programs” in the Control Panel and then click on the “Install” button.



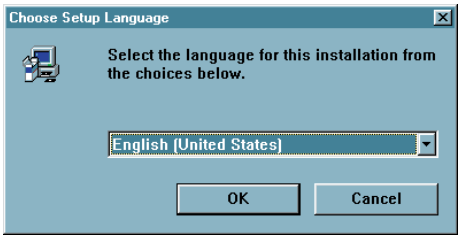
Click on “Next” when the window on the left hand appears.



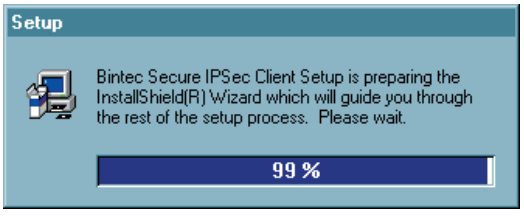
When the following window appears click on “Browse” to select SETUP.EXE in the directory “DISK1" underneath the directory with the ZIP file.

When SETUP.EXE appears click on “Finish”.

→ *continue next page*

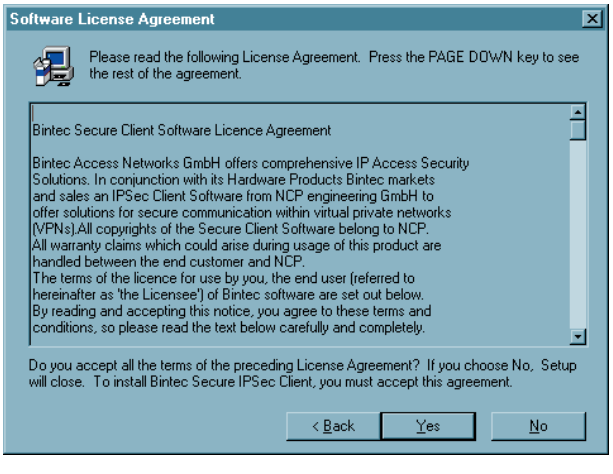


A window appears where you can select the language to be used for the installation and then click “OK”.



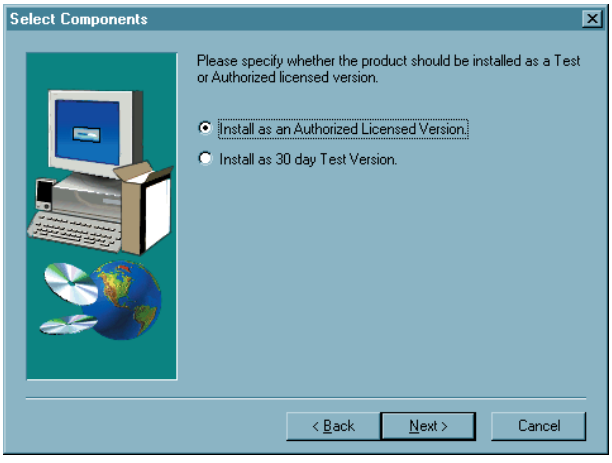
The “Install Shield Assistant” is now started. It will guide you through the installation.

Read the terms of the Software License Agreement carefully and click on “Next”.



The next window displayes the software Licensed Agreement. In order to proceed with the installation of the licensed version click on “Yes”. Clicking “No” will stop the installation process.

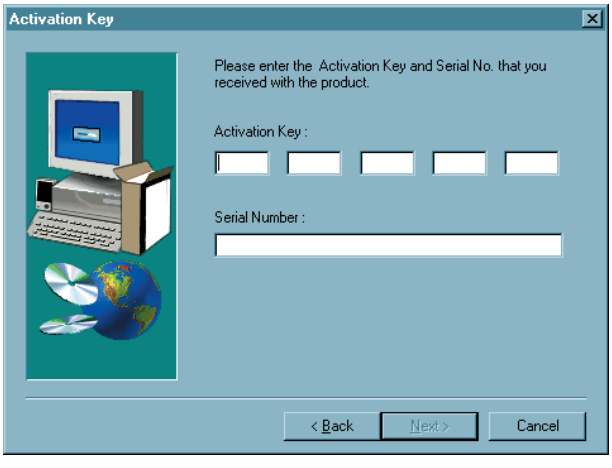
→ *continue next page*



If you are not possession of an Authorized Client Software Lizense, select in this window install as a test version.

If you install the free 30 day limited test version, it is valid only for a period of 30 days from the day of installation. Thereafter it cannot be used.

→ *weiter nächste Seite*

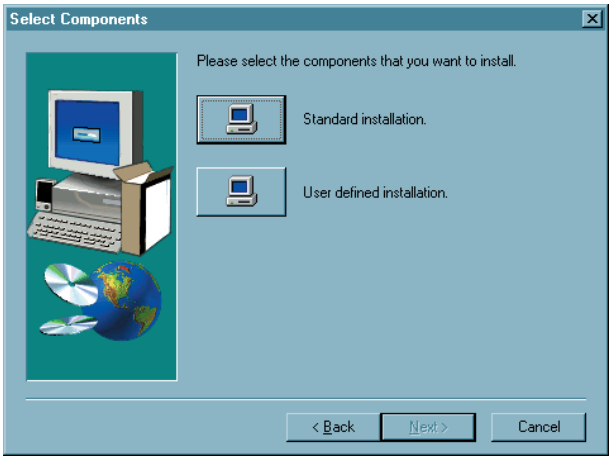


If you are in possession of a license, select in this window "Install as Authorized Licensed Version" and click on "Next".

Enter the serial number of your software license and the activation key in the appropriate fields when prompted to do so. (Activation Key and Serial Number you will find inside the cover of your software!)

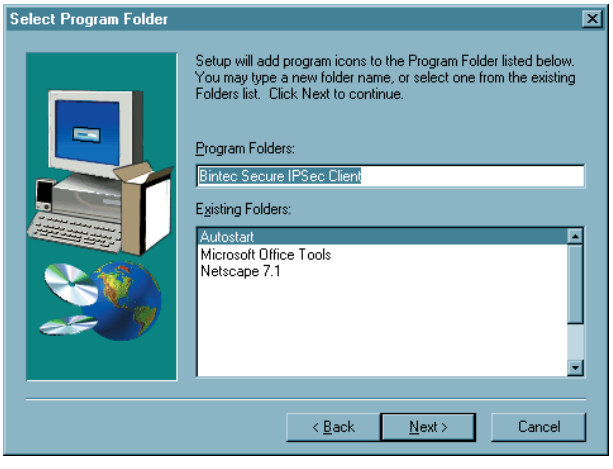
Upon entering these codes correctly, the "Next" button will be activated. By clicking on "Next" the Client Software will be activated as an authorized license version.

→ *continue next page*

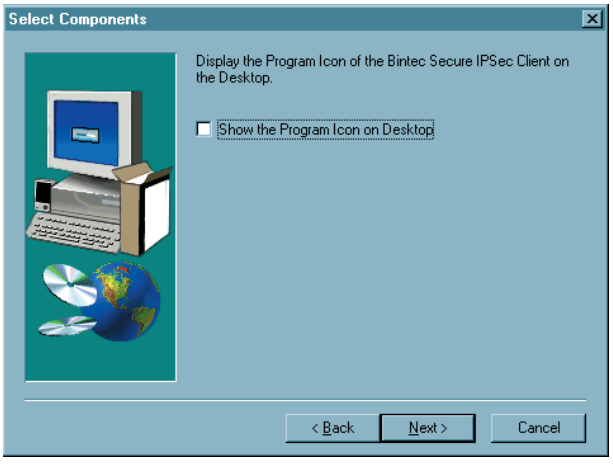


If you select "Standard Installation" in this window the installation will continue automatically and the setup is finished.

Selecting the "User Defined Installation" you can define settings according to your requirements.



In the following window of the "User defined Installation" you define the programmfolder for the client software. (Default setting "Bintec Secure IPSec Client")



In the next window you can define whether the Program Icon should be displayed on the desktop or not.

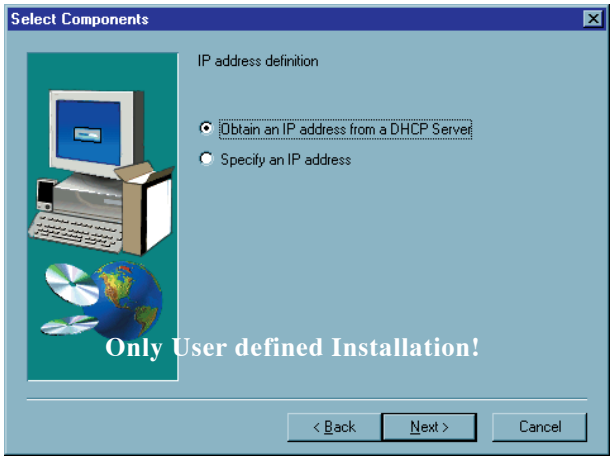
Please contact your system administrator or your internet service provider for additional information about your communication gateway.

→ *for Windows 98/ME continue 2.2.2*

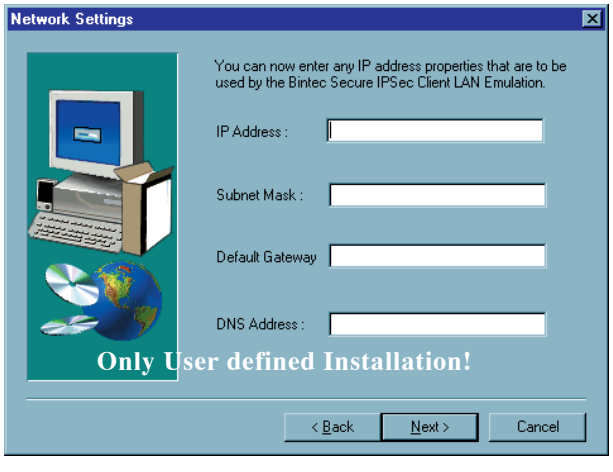
→ *for Windows NT/2000/XP continue 2.2.3*

Following are a list of minor differences in the installation procedures for Windows 98/ME and Windows NT/2000/XP.

2.2.2 User defined Installation and Completion under Windows 98/ME

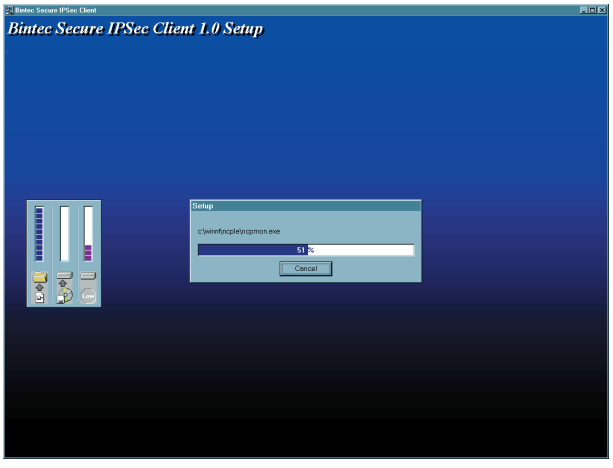


Communication with DHCP (Dynamic Host Control Protocol) means that a temporary IP Address will be assigned automatically for each communication session. If required, click on “Obtain an IP Address from DHCP Server”.



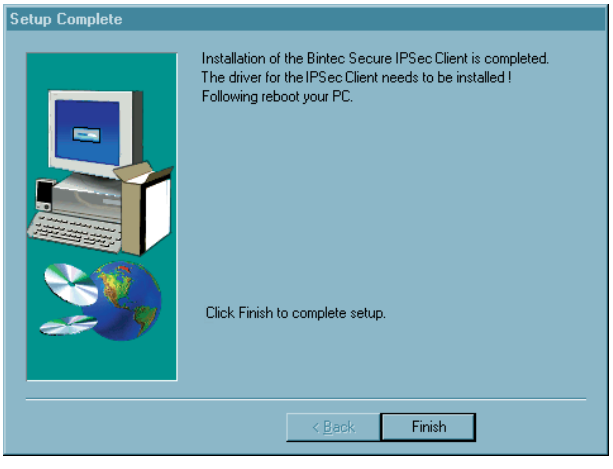
If you “Specify an IP Address”, enter the IP address in this window. Default Gateway: If a network adapter with a Default Gateway is already installed, you will have to delete this Default Gateway Address. It is not possible to have more than one network adapter with a Default Gateway. DNS Address: You should only enter a DNS Address if you have been assigned one from your system administrator or ISP.

End of User defined Installation!
→ to complete continue next page

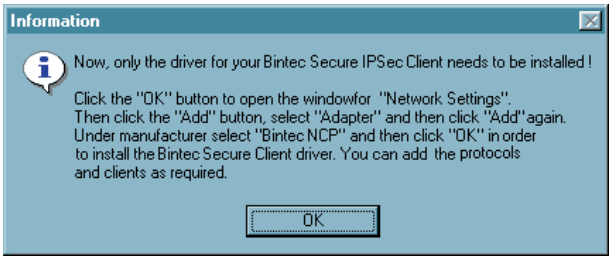


[If you already have the software installed on your PC, this will be detected by the installation program. You will be prompted and asked if you wish to “Update” the current Secure Client or if you wish to cancel the installation (see → “Update and Uninstalling”).]

Now the data will be loaded and copied.

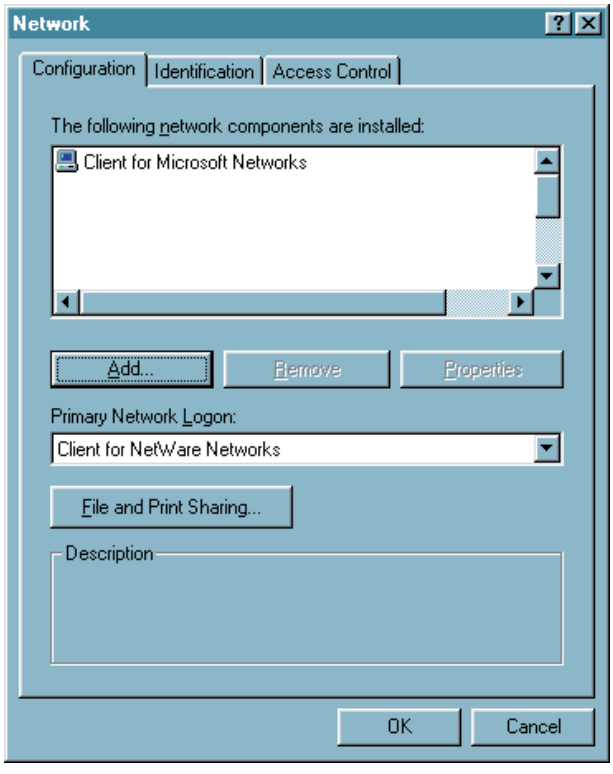


After all data from the CD or Diskette have been loaded, click on “Finish” to complete the setup.



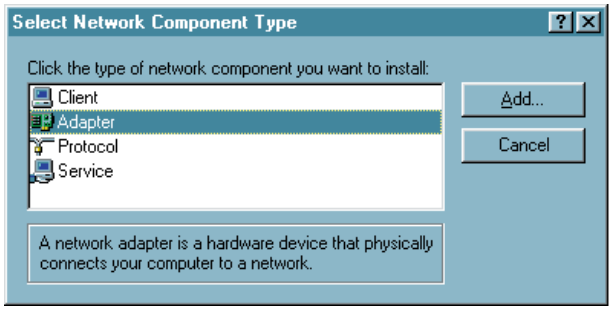
Now you will be prompted to install the driver. To proceed, click on the “OK” button.

→ *continue next page*

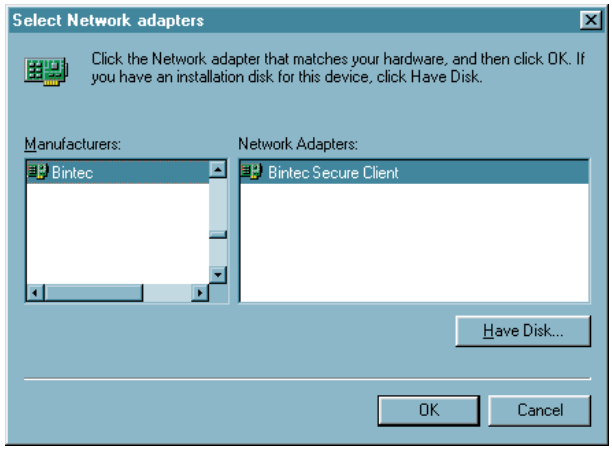


Afer clicking “OK” the Network window will appear. Click on “Add” ...

(Under Windows ME a correspondend dialogue “add hardware” is displayed).

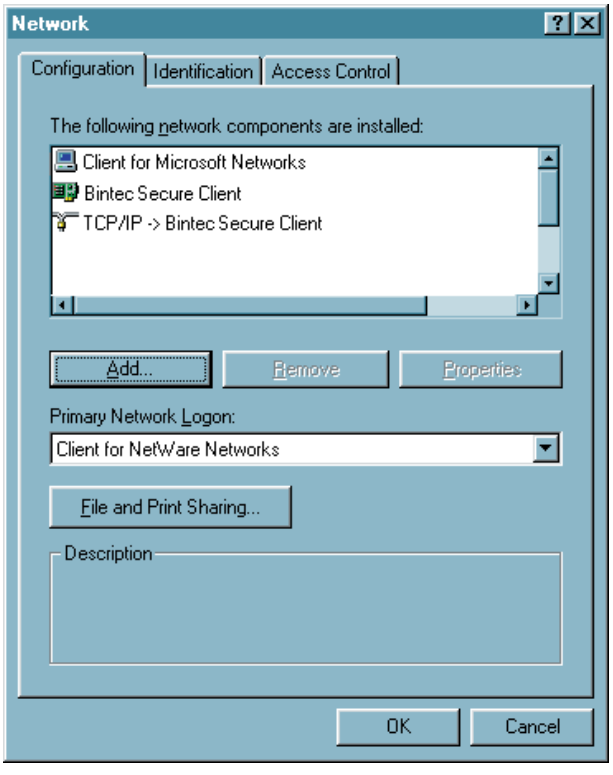


Select Network Component and then click on “Add” again.

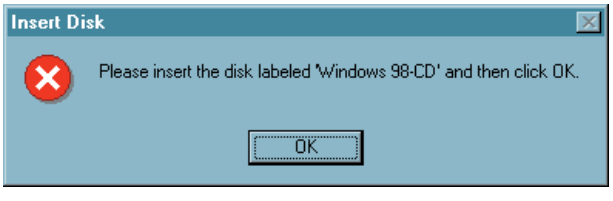


Under “Manufacturer” select Bintec and then select the driver “Bintec Secure Client” in the window on the right. Click on “OK” in order to install the driver. This completes the installation of the Client Software with setup under Windows 98/ME.

→ *continue next page*

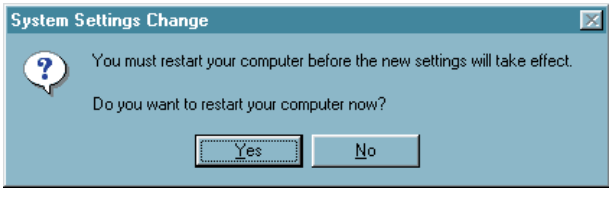


Upon doing so the driver will be installed and displayed in the list of adapters in the Network window. TCP/IP will also be installed and bound to the Bintec Secure Client.



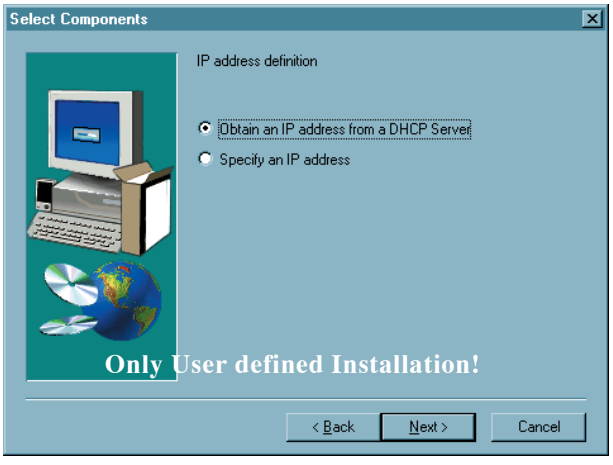
Thereafter it will be necessary to copy files from the operating system in order to update the driver data base.

Insert the respective CD or enter the path for the operating system.

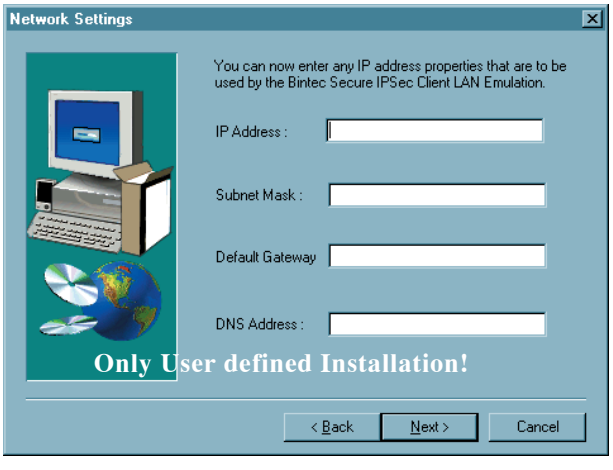


Click “Yes” and wait till you are prompted to reboot your system.

2.2.3 User defined Installation and Completion under Windows NT/2000/XP

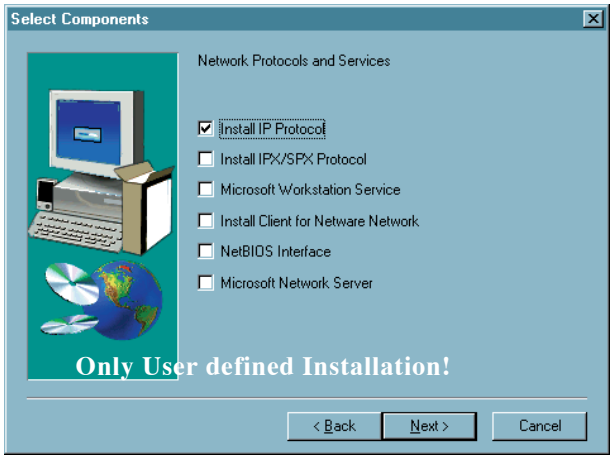


Communication with DHCP (Dynamic Host Control Protocol) means that a temporary IP Address will be assigned automatically for each communication session. If required, click on “Obtain an IP Address from DHCP Server”.



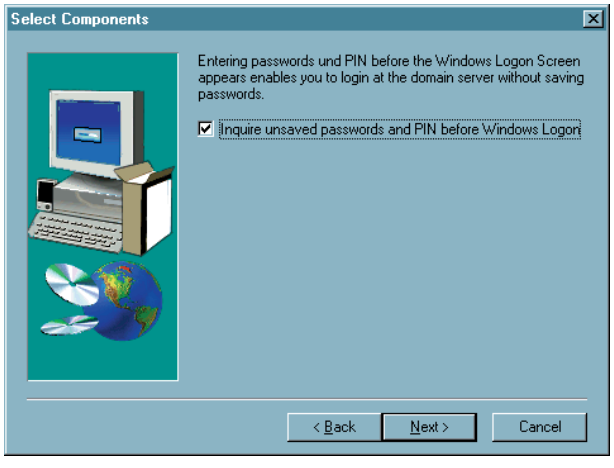
If you “Specify an IP Address”, enter the IP address in this window. Default Gateway: If a network adapter with a Default Gateway is already installed, you will have to delete this Default Gateway Address. It is not possible to have more than one network adapter with a Default Gateway. DNS Address: You should only enter a DNS Address if you have been assigned one from your system administrator or ISP.

→ *continue next page*



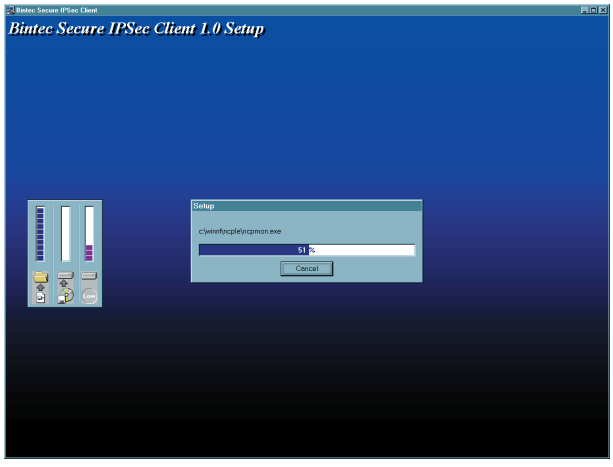
Now you can define any additional protocols and services to be installed. Be sure to have the operating system CD or Diskettes available, as you may need a driver for the installation. Click on “Next” to conclude the User defined Installation.

End of User defined Installation!



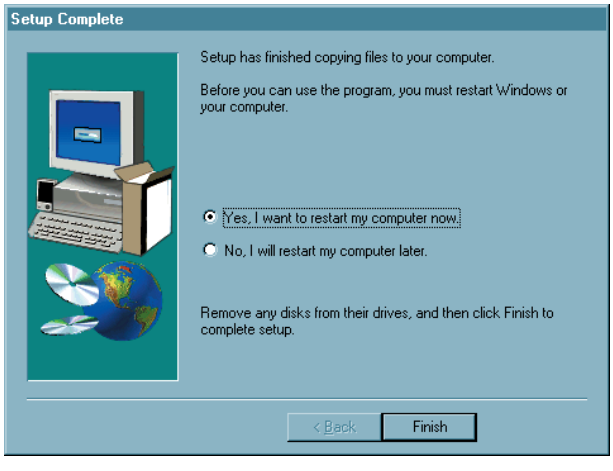
Thereafter you can define whether a logon to a remote domain should occur after establishing a connection to the remote destination’s NAS, which may necessitate entering the PIN for your certificate and/or your Password (if not already stored in the Client Software). After establishing a connection to the remote destination’s NAS, you can logon to the remote domain. This logon will be encrypted.

→ *weiter nächste Seite*



The data of the Client Software will now be copied.

The associated network components will now be installed.



This completes the installation of the Client Software under Windows NT/2000/XP. Click the “Finish” button. Before using the Client Software it is necessary to reboot your PC. Click on “Yes, I want to restart my computer now” and then click on “Finish” to reboot your PC.

Remove any Diskettes or CDs out of the Drives!

Refer to the file named SECCLIENT_NTD.TXT to find notes for User Rights (see → “Using the Client Software under Windows NT).

2.2.4 Using the Client Software under Windows NT/2000/XP

In order to use the Client Software without administration rights, read/write rights must be defined for the following files:

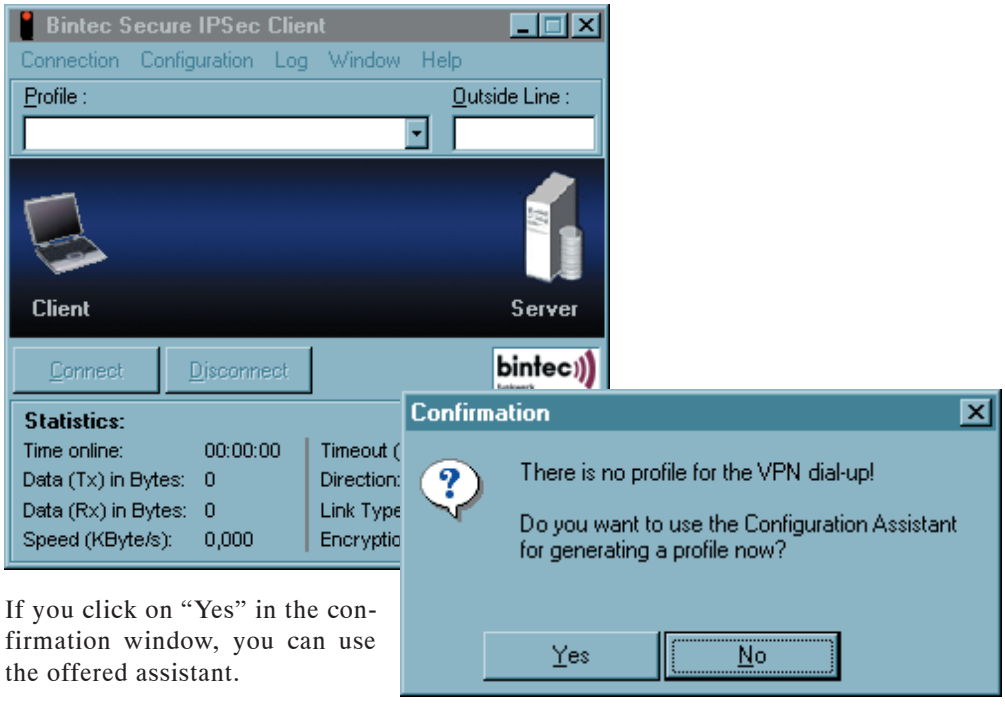
☑ All files in the directory NCPLE under Windows NT must be defined for read authorization. The file NCPPHONE.CFG requires write authorization and it must be possible to generate files in this directory.

☑ The file NCPBM.DAT requires read/write authorization (e.g. for statistics, call control manager).

☑ The file NCP.DB in the directory WINDOWS\SYSTEM32\DRIVERS also requires read/write authorization.

2.3 Before starting

After installing, the Client Monitor is displayed on the screen of your PC. To use the client you first have to generate an entry in the profile settings, what means that you have to define a profile according to a destination system to which an IPSec connection can be established.



If you click on “Yes” in the confirmation window, you can use the offered assistant.

The assistant can also be started later. Therefore you activate the menu item “Profile Settings” in the main menu of the monitor under “Configuration” (see → 3. Client Monitor, Configuration, Profile Settings).

For further configuration refer the descriptions under “3. Client Monitor, Profile Settings” and “4. Configuration Parameters, IPSec General Settings”.

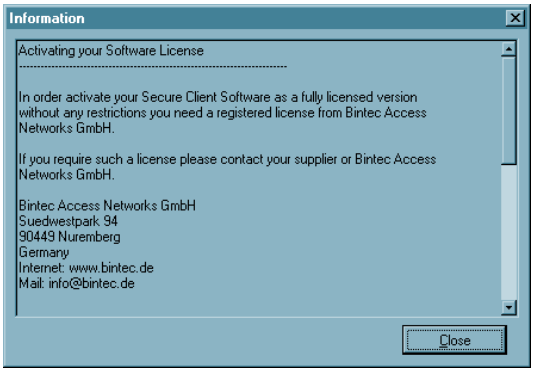
Only if a profile has been defined, a connection to the according destination system can be established. See “ 5. Establishing a Connection”.

In order to guarantee the proper functionality of your IPSec client Bintec offers a public VPN test access. A detailed step-by-step guidance how to use this test access and how to set the needed configurations correctly can be found on the Bintec websites at www.bintec.de.

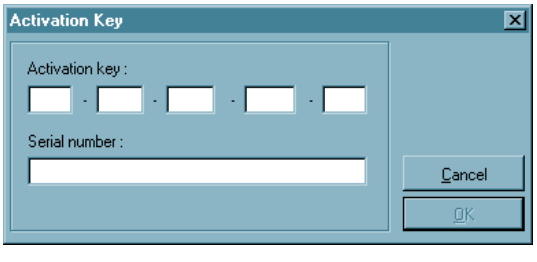
2.4 Activating the Authorized License Version

If you have installed a Client Software 30 day limited test version, and now wish to purchase and convert this to an authorized licensed version follow the steps below:

1. Go to “Start” → “Programs” → “Bintec Secure IPSec Client” and select the program “Secure Client Popup”. The window left side will apear.



2. Under the menu item “Info” in the upper taskbar you will find information about where and how to procure the License for the software.

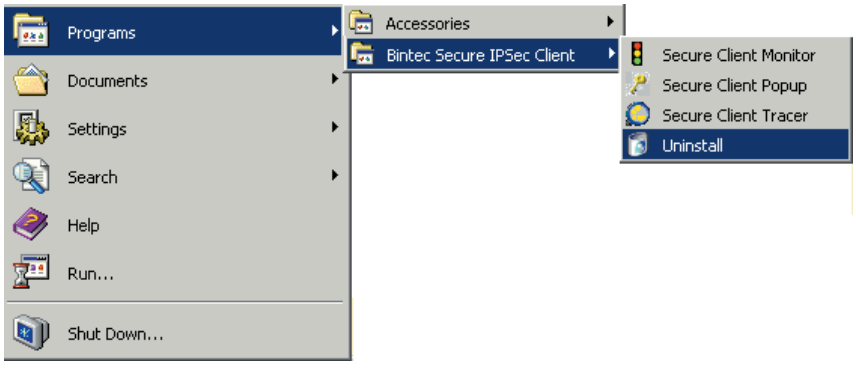


3. After clicking the menu item “Activation Key” in the upper taskbar of the Popup menu a window appears where you can enter your license data. Please enter this information carefully and then click on the “OK” button. Assuming that you have entered valid data and have made no mistakes, then the client will be activated as a licensed version.

2.5 Uninstalling

There are two methods to remove the software from your machine:

1. Navigate to, and select the Uninstall option from the Windows Start Menu in the “Bintec Secure IPSec Client” program group (see illustration below).



A confirmation request will be made- if confirmed, the Uninstall Shield will commence with removing the software from the system.

2. Using the “Start → Settings → Control Panel → Add/Remove Software” option select the Client from the list of programs and Windows components currently installed on the system. Click “Change/Remove” button to run the Uninstall Shield and remove all the software from your system.

Important: After the removal of the software components, the profile and configuration settings are still saved and can be restored in the event a newer version of the client is installed. In order to completely delete everything; manually remove the ncple directory located in either

```
C:\Windows
```

or

```
C:\WINNT
```

3. Client Monitor

Once you have installed the Client the Monitor should appear automatically on PCs screen. To manually display the Monitor click on: Start → Programs → Bintec Secure IPSec Client → Secure Client Monitor. The Client Monitor will be loaded and displayed on the screen or in the task bar.

Note: When the monitor is loaded it will either be displayed on the screen (as well as the taskbar) or if it is not displayed but loaded it appears in the taskbar.

The Client Monitor serves 4 important purposes:

☑ to display the current communications status

☑ for selection of Link Type

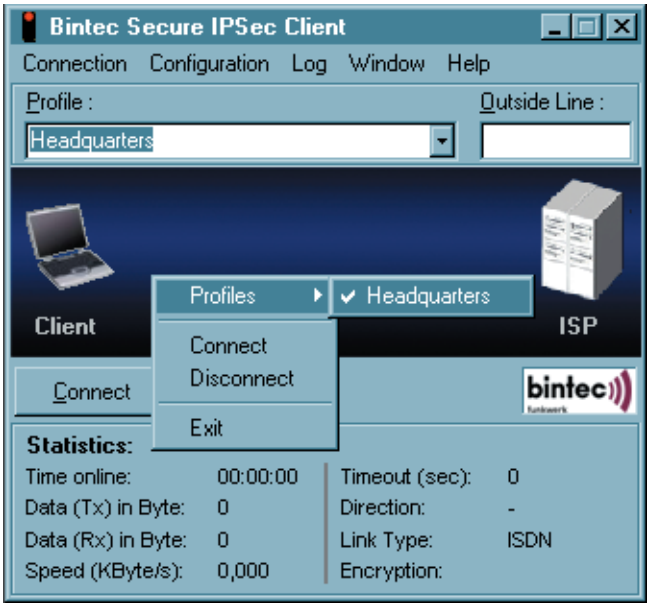
☑ for definition of Call Control parameters

☑ for definition of Profiles and associated Destination and Security parameters

3.1 Monitor Use

Dialing-up und selecting the Destination system

Once the software has been installed and a profile has been configured correctly (see → 3.2.3 Configuration), you are ready for dialing up to the selected destination.



The profile can be selected in two ways: either from the pull-down menu, or from the pop-up menu invoked by clicking on the right mouse button. (see illustration)

In order to establish a connection it is therefore not necessary to start the client monitor itself or to dial-up manually. The only software that must be started is the desired application software (Email, Internet browser, terminal emulation, etc.). The connection will then be established automatically (see → Line Management, Connection Mode, automatically).

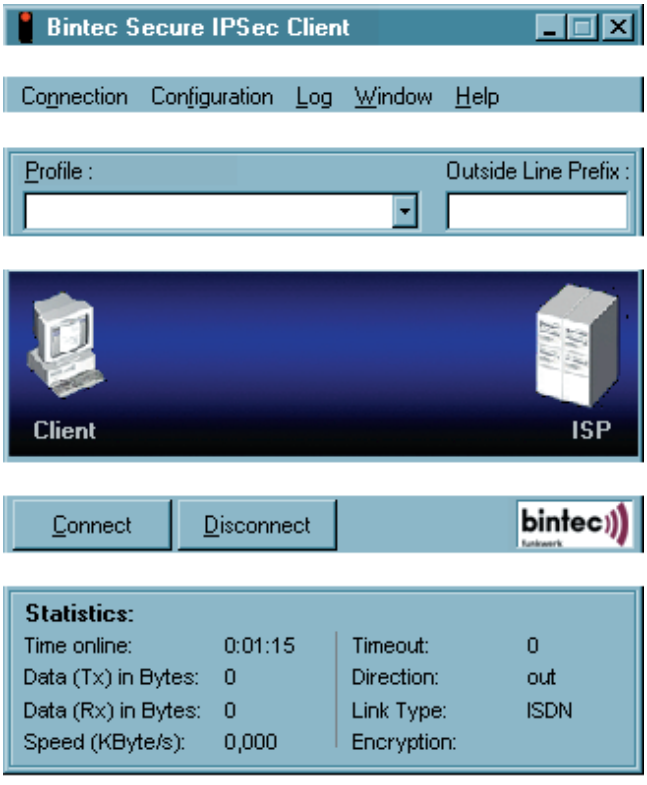
It is also possible to manually establish the connection to a selected destination by selecting “Connection” in the main menu and click on “connect” Alternatively you can click on the “connect” button in the tool bar.

When the connection is established (see → illustration above), the monitor displays a thick green bar from the Client to the Server under which the text “Connection is established” is displayed. At the same time, the traffic lights change from red to green. The green traffic light denotes an established connection and occuring costs.

3.1.1 The Client Monitor User Interface

The Client Monitor consists of:

- A title header indicating the security version of the client,
- the main menu bar,
- A display of the currently selected Profile and a window for Outside Line Prefix if so needed,
- the graphic status field, displaying the communication status,
- the button bar with “connect” and “disconnect”
- and the statistics field



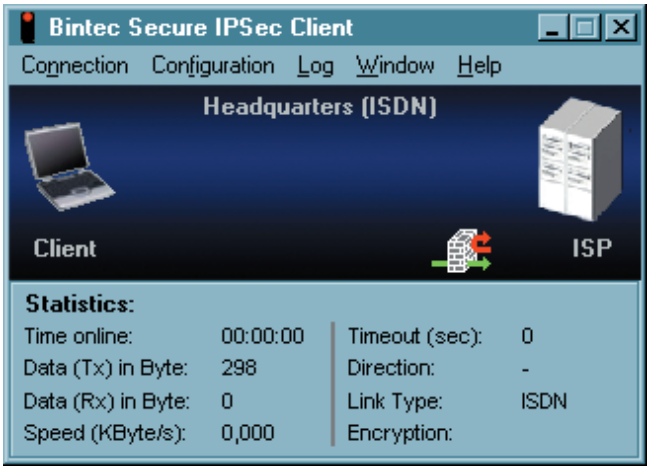
The user interface is conform Windows standards, and operation is similar to that of other Windows applications.

The monitor can either be operated by using pull down menus from the menu bar, or by using buttons from the button bar, or via the context menu (right mouse button).

3.1.2 The Apperance of the Monitors

The monitor can be displayed in different sizes according to the setup in “Window” from the monitor menu (see → 3.2.5 Window).

The Link Type is shown in the statistic window or can be entered by defining the profile so that is displayed in the status field as well.



Modification of the Interface

The monitor appearance can be modified by the administrator. This is particularly relevant for the menu choices “Link Information”, “Certificates”, “Link Control” and “Logon Options”. Also the administrator can suppress profile parameter fields and can suppress individual parameters or set them to “non configurable”. The suppressed and deactivated features and parameters simplify software operation, they do not influence the performance of the software or your work. Refer the section 3.3 Configuration, 3.3.8 Configuration Locks.

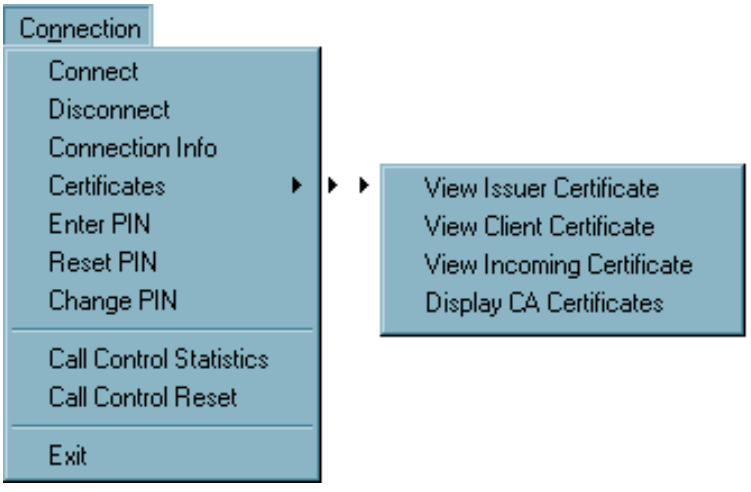
3.2 Using the Client Monitor

The description follows the menu items in the menu bar.

The menu-bar consists of the following items from left to right:

- ☐ Connection
- ☐ Configuration
- ☐ Log
- ☐ Window
- ☐ Help

3.2.1 Connection



With this choice you will find commands for Link establishment and Link break-off. You will also find information windows displaying the current link establishment and the implemented certificates. In addition Link control statistics can be read here and if required the Link control barrier can be deleted if a threshold value that you have set is exceeded.

Connect

This command is used to initiate a connection. A connection can only be made if a profile has been properly defined and selected in the Profile Settings (see → Profile Settings, Basic Settings). The selected profile is displayed in the “Profile” field of the monitor.

Selecting the function “Connect” the connection will be established manually to the destination system.

Whether the link is built manually or automatically depends on the “Connection Mode” defined for the profile in the Line Management folder of the profile settings as well as the Link Type being used (see → Profile Settings, Line Management, Connection Mode).

Disconnect

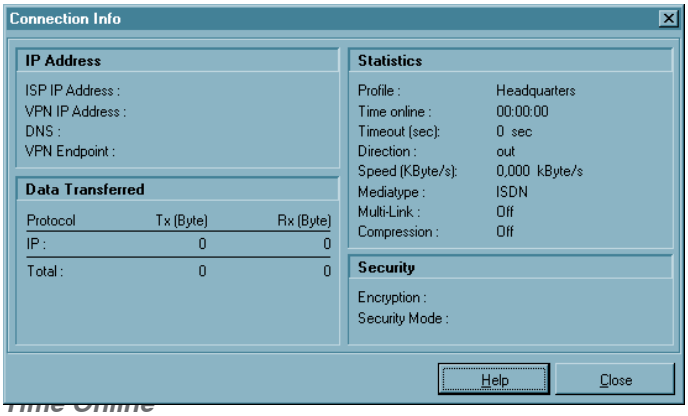
A connection can be terminated manually by clicking on “Disconnect” in the Connection pull-down menu or by clicking the right mouse button.

As soon as the connection has been terminated, the “traffic light” switches from green to red.

Connection Info

Upon selecting the menu parameter “Connection Info” link statistics are displayed. The window also displays the type of security features being used as well as the IP addresses that have been assigned between the IPSec client and the destination resulting from the PPP negotiation. The information in the connection info window is “read-only” and has no influence on the functionality of the IPSec client.

The field “Connection Info” could be suppressed by the administrator. In this case the menu item could not be activated.



If the connection info is faded, the most important information concerning data transfere, statistic and security can be seen in the statistic field of the monitor (see → Window, Show Statistics).

Time Online

Time Online indicates the total amount of time that the PC is actually connected to the destination, regardless of any timeouts (disconnects). The value is reset to zero (0) either as a result of (re)booting your PC or when you change the destination.

Timeout

The Client Monitor displays the time remaining until the next timeout (disconnect) occurs, which begins immediately following the last exchange of data over the Link (including any handshaking). The “Inactivity Timeout” value can be set in the Phonebook under “Line Management”.

Direction

Direction indicates the current direction of communications as follows:

Out	=	outbound or outgoing call is currently being executed.
In	=	inbound or incoming call is currently taking place.

Speed

The displayed number varies according to the current data throughput.

Media Type

The following Media Types are supported: ISDN, Modem, LAN over IP, xDSL (PPPoE), xDSL (AVM - PPP over Capi), GPRS and PPTP.

Multilink

If a connection is established via several ISDN-B channels, the statistic showes “on”.

Compression

Compression is always defined by the gateway. IPSec compression is displayed with “IPSec Compression (LZS)”.

Encryption

The used encryption type is diasplayed. Following types of encryption are supported: AES, Blowfish, 3DES. The encryption type is assigned by the central site (gateway).

Key exchange

Display what Session Key exchange method is used:

Static Key	=	The same Static Key must be used at both endpoints of communication. It is entered under “Profile Settings → Identity”
IKE (IPSec)	=	To transfer the Session Key, the encrypted Control Channel of Phase 1 negociation is used.

Rx and Tx Bytes

Rx and Tx Bytes indicates the amount of data being sent (out) and received (in) for each protocol and for each communications session. The amount of data is expressed in Bytes (1 byte = 1 character). The total amount of data sent and received for all protocols is also displayed.

Certificates

In the pulldown menu “Connection” you will find the entry “Certificates” which consists of the following submenus “Configuration”, “View Issuer Certificate”, “View Client Certificate”, “View Incoming Certificate” and “Display CA Certificate”.

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”.

View Issuer Certificate

In order to view the Issuer Certificate select “Connection → Certificate → View Issuer Certificate”. Upon doing so the individual assigned data will be displayed (read-only) for your review purposes.

Certificate Authority (CA)	=	The CA and the issuer of a Issuer Certificate are normally identical (self-signed certificate). The CA of the Issuer Certificate has to be identical with the CA of the Client Certificate (see → View Client Certificate).
Serial Number	=	The serial number of the certificate can be compared with the registered serial number in the Revocation List of the Certification Authority.
Validity	=	The validity of certificates is limited. Normally the validity of a Issuer Certificate is longer than the validity of a Client Certificate. Upon expiration of the Issuer Certificate, the validity of the Client Certificate of the same CA expires as well.
Fingerprint	=	Hash value. The Hash value is the signature of the certificate. The Hash value is encrypted with the private key of the CA.

View Client Certificate

In order to view the Client Certificate select “Connection → Certificate → View Client Certificate”. Upon doing so the individual assigned data will be displayed (read-only) for your review purposes.

Certification Authority (CA)	=	The CA and the issuer of a Client Certificate is normally identical (self-signed certificate). The CA of the Client Certificate has to be identical with the CA of the Issuer Certificate (see → Issuer Client Certificate).
Serial Number	=	The serial number of the certificates can be compared with the registered numbers in the Revocation List of the Certification Authority. (see → strong Radius Authentication)
Validity	=	The validity of certificates is limited. Normally the validity of a Issuer Certificate is longer than the validity of a Client Certificate. The expiration of validity erases the functionality of certificates.
Fingerprint	=	Hash value. The Hash value is the signature of the certificate. The Hash value is encrypted with the private key of the CA.

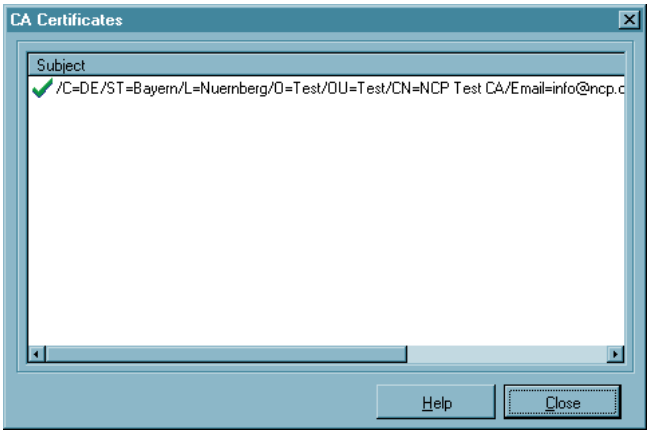
View incoming Certificate

Display of the certificate that is communicated in the SSL negotiation from the other side (Secure Server). You can see, for example, whether you have accepted the issuer displayed here in the list of your CA certificates (see below).

If the incoming user certificate is one of the CAs not known from the list “Display CA Certificates”, then the connection will not take place.

If no certificates are stored in the Windows directory NCPLE\CACERTS\, then no verification takes place.

Display CA Certificates



Multiple issuer certificates are supported with the client software (multiple CA support). The issuer certificates must be collected in the Windows directory NCPLE\CACERTS\ for this. In the client monitor the list of CA certificates read in is displayed 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 for the issuer certificate, first on Smart Card or in the PKCS#12 file, and then in the NCPLE\CACERTS\ directory.

If the issuer certificate is not known, then the connection will not be established (No Root Certificate found). If no CA certificates are present in the Windows directory NCPLE\CACERTS\, then a connection that implements certificates is not permitted.

Display and analysis of extensions for incoming certificates and CA certificates

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.

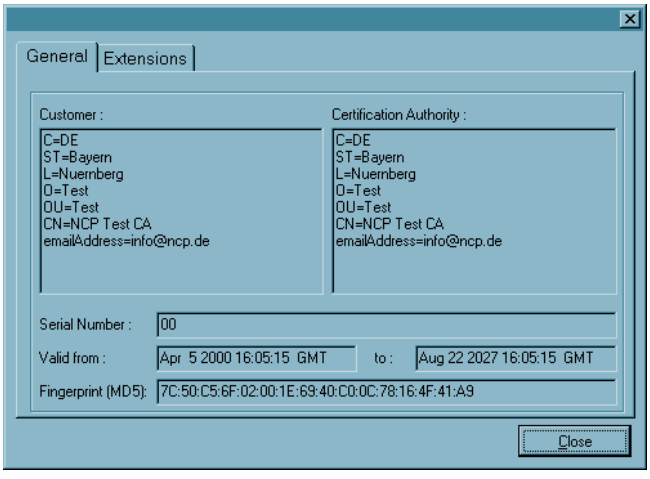
Three extensions are significant for the IPSec client and the gateway:

☑ extendedKeyUsage

☑ subjectKeyIdentifier

☑ authorityKeyIdentifier

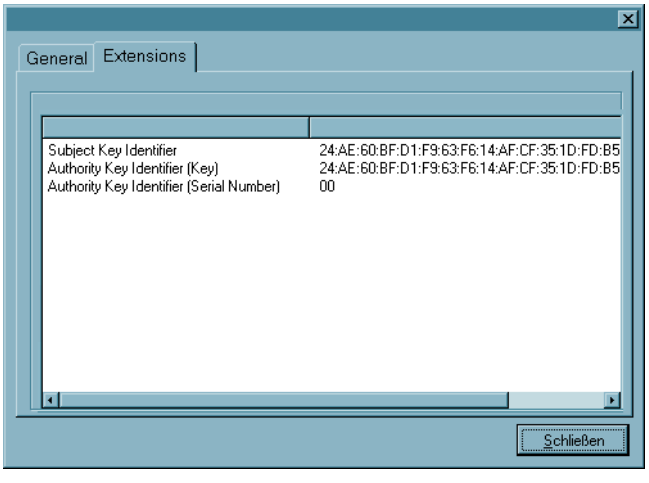
Display of extensions



To display the extensions of an incoming or CA certificate you have to proceed as follows:

The Ca certificate which extension should be displayed, has to be opened by a doubble click in the window of Ca certificates. Upon doing so the next window with general information is opened.

For the incoming certificate this window is already opened after “View incoming certificate” was selected in the certificate menu.



The window “General” displays the general certificate data

The window “Extensions” displays the certificate extensions if available.

Extension checks

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.

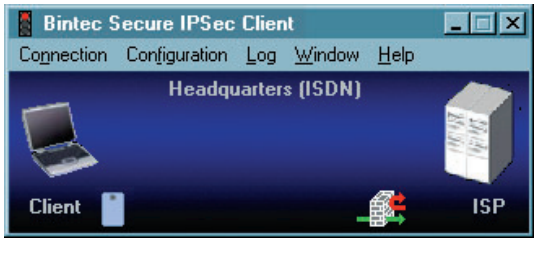
The keyidentifier designates the public key of the certification authority and thus not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determining a certificate path. In addition, the certificates that possess the authoritykeyidentifier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

Enter PIN

The PIN entry can be executed before establishing a connection, after the monitor has been started. If a connection requiring a certificate is established at a later time, then the PIN entry can be omitted - unless the configuration for the certificate requests it (see → Configuration, Certificates).

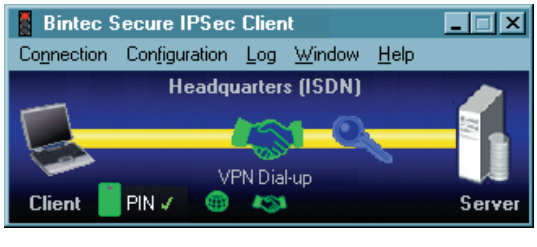
If you have selected the menu item “Connection - Enter PIN”, then the PIN (at least 6 digits) can be entered in the open entry field, and confirmed with “OK”. The digits of the PIN are displayed as asterisks “*” on the screen (picture left side).

If the PIN has not been entered before a connection establishment, then the PIN entry dialog appears when the first connection requiring the use of a certificate is to be established to a destination at the latest. Thereafter the PIN entry can be omitted in the case of repeated manual connection establishment, if this has been configured (see → Configuration, Certificates).



If you have configured the IPSec client for the use of a Smart Card or of a PKCS#11 module (see → Configurat-ion, Certificates), then a light blue symbol for the Smart Card appears in the status field. If you have inserted your Smart Card in the card reader, the symbol color changes from light blue to green.

If the IPSec client has been configured for the use of a soft certificate (see → Configuration, Certificates), then no symbol appears in the status field.



If the PIN has been correctly entered, then this fact is indicated in the monitor interface by a green check mark behind “PIN” (picture left side).

Incorrect entries and incorrect PINs are acknowledged with the error message “Incorrect PIN!” after approximatly 3 seconds. At this point a connection establishment is not possible.

Please note that a Smart Card or a token can be blocked after multiple incorrect PIN entries. In this case, please contact your remote administrator.

The connection establishment can only be executed after correct PIN entry.

An established connection will, by default, be disconnected if the Smart Card or token is removed during the operation.

This behavior can be changed, and is determined by whether or not the “Do no disconnect when Smart Card is removed” has been enabled. This toggle can be found in the main menu of the monitor “Configuration → Certificates”.

The policies for PIN entry can be specified in the main menu under “Configuration → Certificates” (see → Configuration, Certificates, PIN Policies). These policies must also be observed when the PIN is changed (see → Connection, Change PIN).

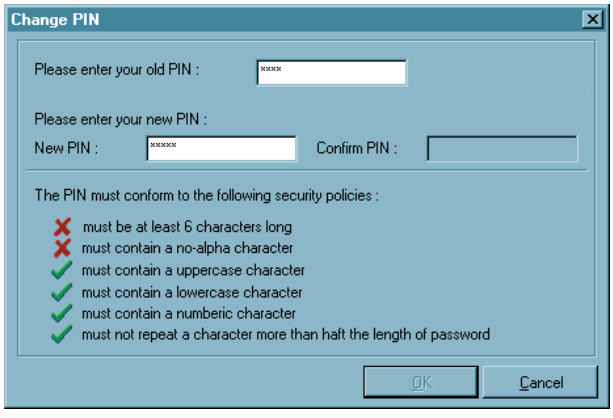
The PIN for a smart card or a certificate can be changed under the “Change PIN” menu item, if the correct PIN has been correctly entered prior to this. This menu item will not be activated without the prior entry of a valid PIN.

■ Reset PIN

This menu item is active only when the PIN has been entered correctly, i. e. the certificate is used for the connection to be established.

If you reset the PIN this certificate could not be used to establish a connection anymore until the correct PIN is entered again.

Change PIN



The PIN for a Smart Card or for a soft certificate can be changed under the menu item “Change PIN”, if the correct PIN number has previously been entered. This menu item will not be activated without the previous entry of a valid PIN number.

For security reasons, after opening this dialog the still valid PIN must be entered a second time. This is to insure PIN change for the authorized user only. The digits of the PIN are displayed in this entry field, and in the next entry fields as asterisks “*”.

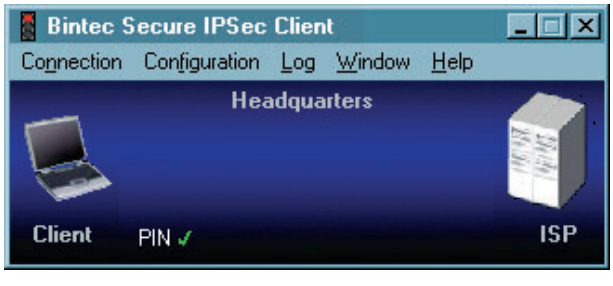
Then enter your new PIN and confirm it by repeating it in the last entry field. With a click on “OK” you have changed your PIN.

PIN policies that need to be complied with are displayed under the entry field. They can be set in the main menu under “Certificate → PIN Policies”.

Changes in PIN handling

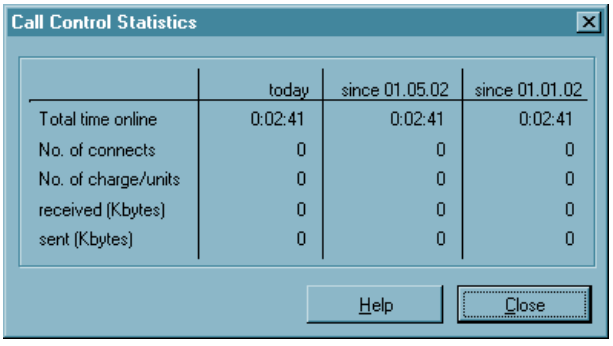
When a user logs off Windows NT/2000/XP the PIN cache is cleared and must bereentered at next logon. When the machine enters sleep mode the PIN cache is also cleared.

PIN state symbol visible in the Client Monitor.



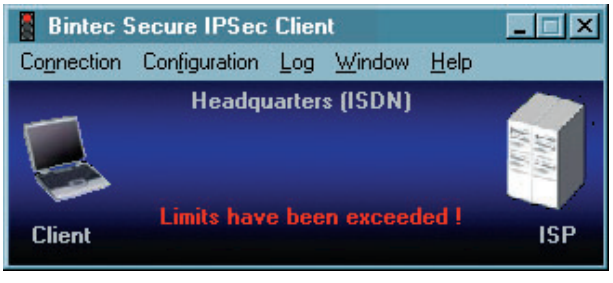
If a valid PIN is entered this is symbolized by means of a green check next to the PIN display in the client monitor.

Call Control Statistics



Call Control Statistics provide you with an overview of your communications on a daily, monthly and yearly basis. It accurately displays the following information:
– total time online
– total number of connects (outgoing calls)
– total number of charge/units (if available)
– total amount of data (expressed in Bytes) sent and received

Call Control Reset



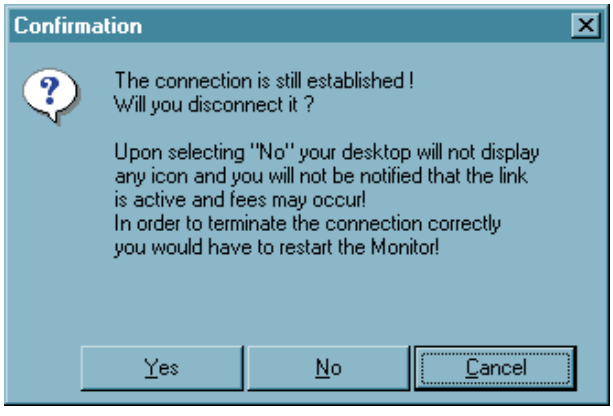
If the “Limits” defined in the Call Control Manager have been exceeded, the IPSec client issues a “Warning Message” and blocks any further communications until such time that the “Call Control Reset” has been activated (see → “Connection” pull-down menu in the Monitor).

A connection can only be established after clicking “Call Control Reset”.

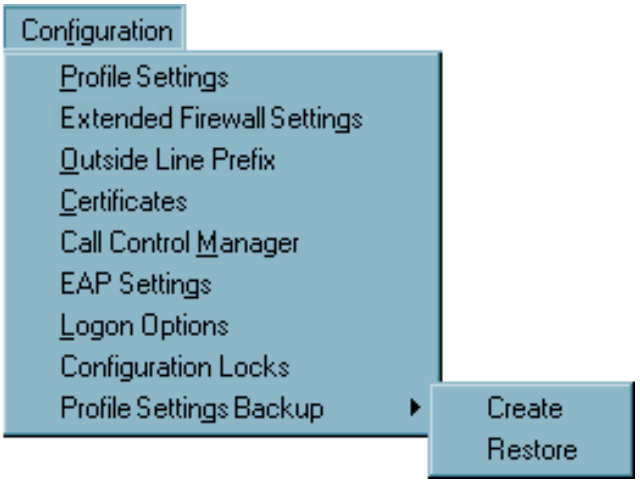
Exit (Disconnect the Monitor)

Have you already disconnected the link, a click on this menu item or on the “Disconnect” button closes the monitor. If the connection is still established, with a click on this menu item or on the “Disconnect” button the monitor can be closed as well. Please note that closing the Monitor does not automatically terminate the connection. If the link should be established although the monitor is closed and fees may occur, the software asks you explicitly for a prompt.

Upon selecting “No” your desktop will not display any icon and you will not be notified that the link is active and fees may occur! In order to terminate the connection correctly you would have to restart the Monitor!



3.2.2 Configuration



You can specify all settings for work with the IPSec Client, which should work longer than one session, with this menu choice. Specifically this means creating profiles, configuration for IPSec links, choosing communication media, as well as obtaining an outside line for connections to telecommunications systems.

In addition you can individually configure precisely how certificates should be used, how the call control manager should work and which configuration rights the user receives.

In order to guarantee the proper functionality of your IPSec client Bintec offers a public VPN test access. A detailed step-by-step guidance how to use this test access and how to set the needed configurations correctly can be found on the Bintec websites at www.bintec.de.

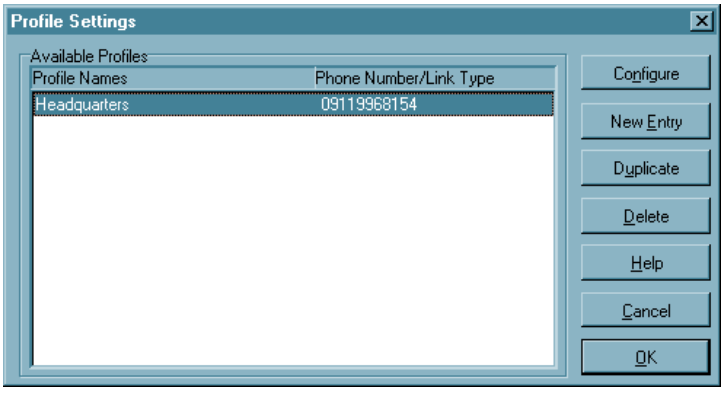
Profile Settings

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.

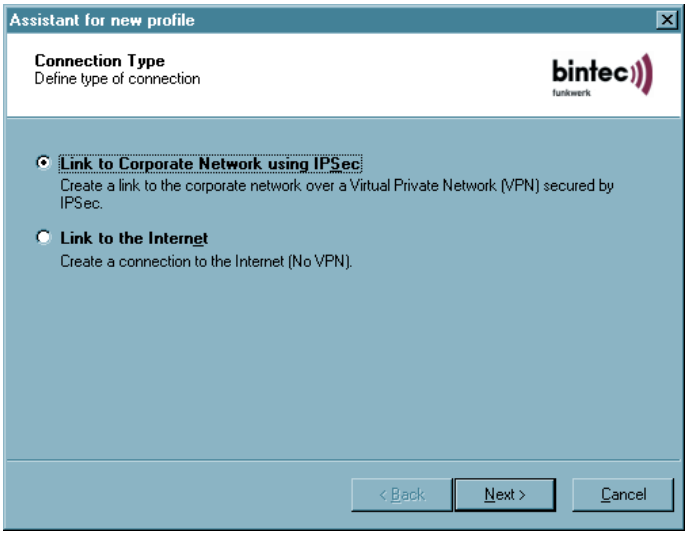
Upon clicking “Profile Settings” in the Monitor menu “Configuration” the menu is opened and displays an overview of the defined profiles and their respective names and the telephone numbers of the according destinations.



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.



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:

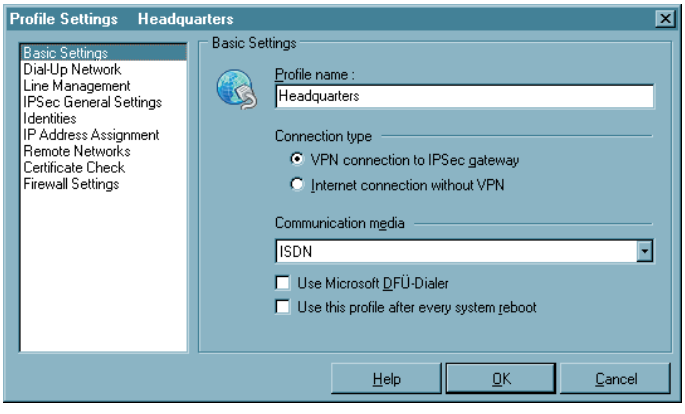
Link to Corporate Network using IPSec:
→ Profile Name
→ Link Type
→ Access data for Internet Service Provider (User ID, Password, Phone Number)
→ VPN-Gateway selection (Tunnel Endpoint IP address)
→ Access data for VPN Gateway (XAUTH, User ID, Password)
→ IPSec Configuration (Exch. Mode, PFS Group, Compression)
→ 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
→ Link Type
→ 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:



Basic Settings
Dial-Up Network
Modem
Line Management
IPSec General Settings
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.

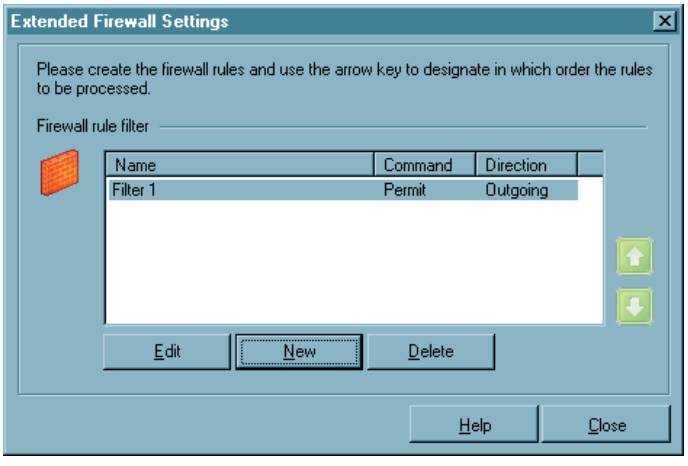
Important: It is not possible to have 2 or more profiles with identical names. Each profile must be assigned its own unique name.

Delete – Profile

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

Extended Firewall Settings

Filters for incoming and outgoing data traffic can be defined with this filter editor. The filters can be set for protocols, network IP addresses, and host IP addresses.



After you have selected this menu item, a list of the firewall filtering rules will appear in this window. Each rule has a name that can be freely assigned, the execution of the filter rule can be approved or rejected, and the direction can be defined as outgoing or incoming.

The sequence of filter rules can be specified with the green arrow keys.

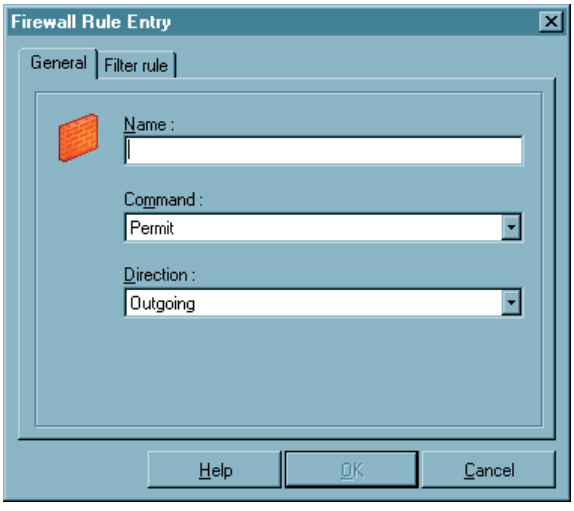
The buttons, “Edit”, “New”, and “Delete” refer to each marked filter rule.

Please note that a deleted filter rule cannot be restored.

Use the buttons, “New” and “Edit”, to open additional windows for filter definition:

– General | Firewall
– Filter rule | Firewall

General | Firewall



Name | Firewall

Enter a name for this filter rule.

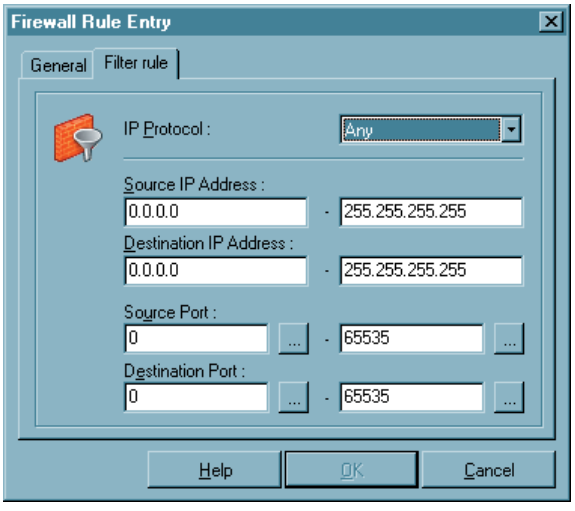
Command | Firewall

disabled	=	this filter rule is turned off and is not implemented; it is not necessary to delete it.
Deny	=	all IP packets with addresses from the defined range will be discarded.
Permit	=	IP packets with addresses from the defined range are allowed through without implementing the SPD.

Richtung | Firewall

incoming	=	the filter rule is valid for incoming IP packets
outgoing	=	the filter rule is valid for outgoing IP packets

Filter rule | Firewall



In this window you can specify the protocol, the IP address range, and the port address range to which the filter rules will apply.

IP Protocol | Firewall

This is the transport protocol, which can be ICMP, TCP, or UDP. One of these offered protocols can be selected or (any) can be used.

Source IP Address | Firewall

This can be a host IP address or an address range.

Destination IP Address | Firewall

This can be a host IP address or an address range.

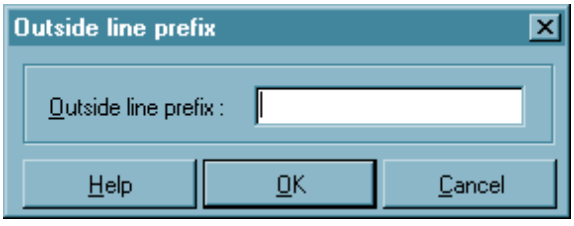
Source Port | Firewall

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 | Firewall

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 [...].

Outside Line Prefix



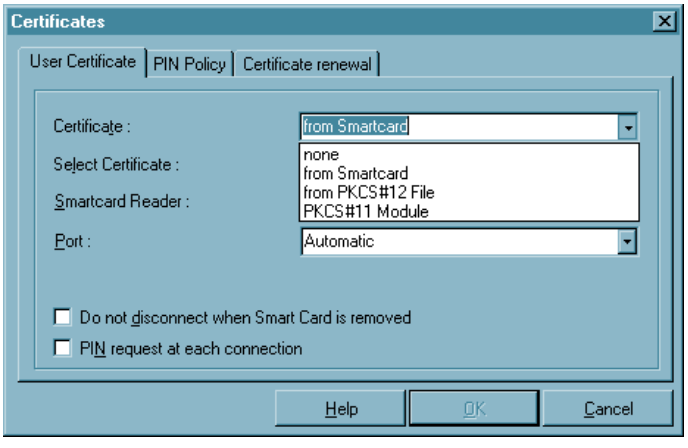
A special number or dial prefix is generally required when communicating via a PBX in order to acquire an outside line. This could, for example, be a 0 (zero) or 9 or any other number(s) depending on the PBX in use at your location. The number entered in this field, depending on the type of PBX, will then be used for all outgoing calls until changed or deleted. This eliminates the need for modifying the destination phone number(s) of the profile, particularly when travelling.

User 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.

Certificate



None: By choosing “Certificate” from the submenu you can determine whether or not you want to use the certificate and thus use the “Extended Authentication”. The default value is “None”.

from PKCS#12 File: In order to use a Soft Certificate select “from PKCS#12 File” and then define the directory (path) in which the PKCS#12 file is stored for access purposes. Normally you will receive this file (encrypted) from your network administrator or your CA (Certification Authority).

from Smart Card: In order to use Smart Card based Certificates select “from Smart Card” and then select the Smart Card Reader from the list of supported Smart Card Readers. (see also → Enter PIN)

PKCS#11-Module: Select “PKCS#11-Module” from the list in conjunction with “Extended Authentication” in order for the respective Certificate to be read from a Smart Card in a Smart Card Reader or from a Token.

Smart Card Reader

In order to use the Smart Card's Certificate with your card reader, select the respective Smart Card reader from the list (see also → PIN Entry).

Smart Card Reader (PC/SC conform)
The Client Software automatically supports all PC/SC conform Smart Card readers. The Client software automatically recognizes the Smart Card reader each time the PC is re-booted. Thereafter the installed Smart Card reader can be selected and used as required.

Smart Card reader (CT-API conform)
Together with the current Client Software the following drivers are included for: SCM Swapsmart and SCM 1x0 (PIN Pad reader). In the event that the Smart Card reader does not work together the drivers that are included or another Smart Card reader is installed, then please contact the respective manufacturer. Also make the following settings in the Client Software: With an ASCII Editor edit the file NCPPKI.CONF, which is located in the Directory \WINDOWS\SYSTEM (Windows 95/98) or in the Directory SYSTEM32 (Windows NT/2000) by entering the "ReaderName" of the Smart Card reader (xyz) connected to your PC and enter as DLLWIN95 or DLLWINNT the name of the installed driver. (The default name for CT-API conform drivers is CT32.DLL).

Important: Only those drivers that have been appropriately set with "visible = 1" will be displayed in the list!

```
ReaderName = SCM Swapsmart (CT-API) -> xyz
DLLWIN95   = scm20098.dll           -> ct32.dll
DLLWINNT   = scm200nt.dll           -> ct32.dll
```

The "ReaderName" will be displayed in the Monitor Menu after re-booting.

Port

If the Installation has been executed correctly, the card reader will automatically be assigned a port. Should problems arise, COM Ports 1-4 can be manually assigned.

Certificate Selection

1. Certificate ... 3.: (Standard = 1) Up to 3 different certificates, located on the Smart Card, can be selected from the list. The number of certificates on the Smart Card is dependent on the Registration Authority that has issued the Smart Card. For further information please contact your System Administrator.

The Smart Cards issued by Signtrust and NetKey 2000 come with three certificates:
(1) for digital signing,
(2) for encryption and decryption,
(3) for Authentication (optional with NetKey 2000)

PKCS#12 File Name

If you are using the PKCS#12 format, then you will receive a file from your system administrator that must be copied to your PC's hard disk. In this case enter the path and filename of the PKCS#12 file or alternatively after clicking the selection button select the file. Instead of entering the entire directory name, it can be dynamically defined. E.g.:

```
%SYSTEMRROT%\ncple\user1.p12
%SYSTEMDRIVE%\winxxx\ncple\user1.p12
```

Important: The strings for the File Name can be entered with variables. This simplifies in particular the handling of the configuration files with the Client Manager, because the same strings including environment variables can be entered for all Users.

PKCS#11 Module

If you are using the PKCS#11 format, then you will receive a DLL from your Smart Card reader manufacturer that must be copied to your PC's hard disk. In this case enter the path and filename of the driver. Instead of entering the entire directory name, it can be dynamically defined. E.g.:

```
%SYSTEMRROT%\ncple\pkcs#11.dll
%SYSTEMDRIVE%\winxxx\ncple\ pkcs#11.dll
```

Important: The strings for the File Name can be entered with variables. This simplifies in particular the handling of the configuration files with the Client Manager, because the same strings including environment variables can be entered for all Users.

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 the menu item "Configuration - Certificates".

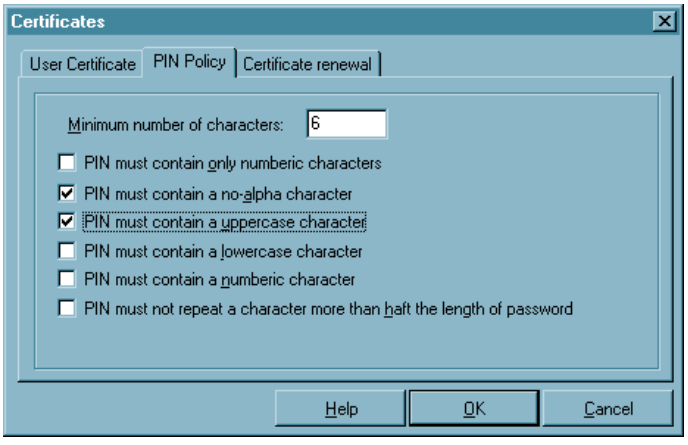
PIN request at each manual connect

Default: If this function is not used, the PIN request is displayed only for the first connect of the VPN/PKI Client.

If this function is activated, the PIN will be requested at each connect.

Important: If the monitor has not started, then no PIN dialog will take place. In this case, the connection will be established without renewed PIN entry in the case of an automatic connection establishment.

PIN Policy



You can specify PIN guidelines that must be complied with during PIN entry or PIN modification.

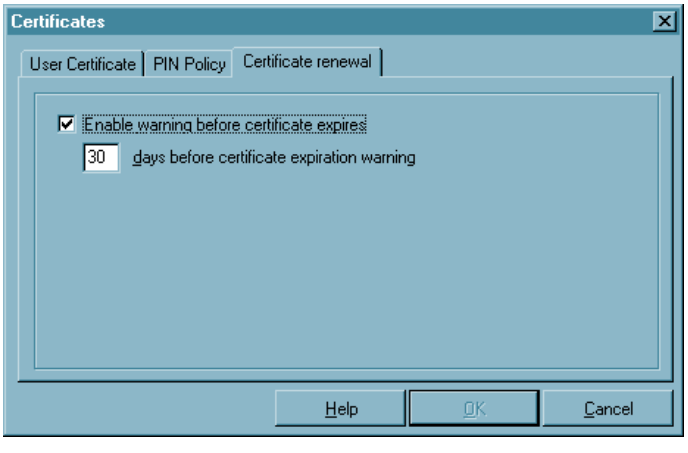
Minimum number of characters

Standard is a 6-digit PIN. An 8-digit PIN is recommended for security reasons.

Further policies

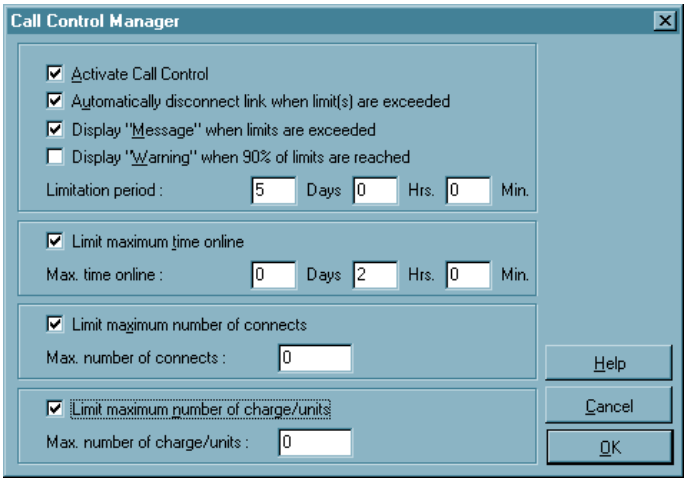
It is recommended to implement all PIN policies, other than the one specifying that only numbers may be contained. Additionally, the PIN should not begin with a number.The specified policies are displayed when the PIN is changed, and the policies that are only fulfilled at entry are highlighted in green (see → Change PIN).

Certificate renewal



In this configuration field you can specify whether a message is given out that warns of the expiration of validity, and you can specify how many days before the certificate validity expiration this message should go out. As soon as the set time frame before expiration goes into effect, a message will appear each time a certificate is used, indicating the expiration date of the certificate.

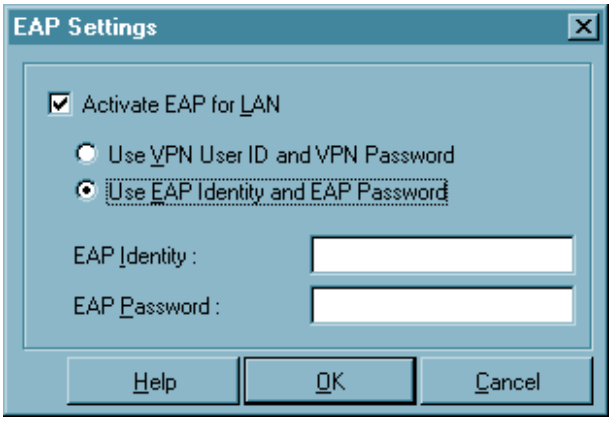
Call Control Manager



The Call Control Manager is a feature devised to help control and limit communication costs. The following "Limit" factors can be defined:
– the maximum time online
– the maximum number of connects (outgoing calls)
– the maximum number of charge/units that may be incurred.

The time period for which these limits are to adhere to may also be defined. It is possible to define that a "Warning Message" be displayed upon reaching 90% of any limit. In the event that the set "Limit(s)" are exceeded, the link will be automatically disconnected and a "Warning Message" will be displayed in the monitor. Any further communications is denied until the "Call Control Reset" is activated (see → "Connection" pull-down menu in the monitor).

EAP Settings



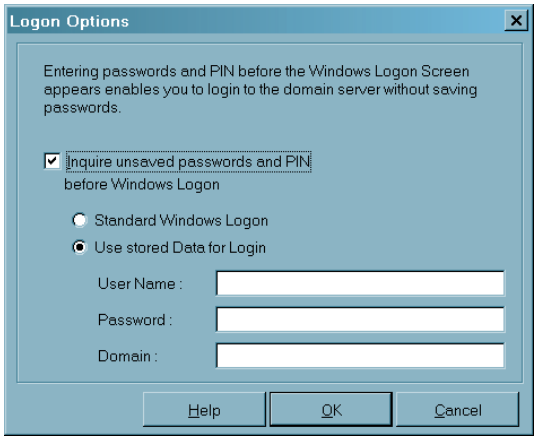
Use of the Extended Authentication Protocol Message Digest version 5 (EAP MP5) can be specified via the main menu of the monitor under “Configuration - EAP Settings”. This protocol can then be used if a switch, a hub, or if an access point is used, which support 802.1x and the according Authentication 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 “Username” with “Password” (from the configuration field “Identity”) or your own “EAP User ID” with an “EAP Password”.

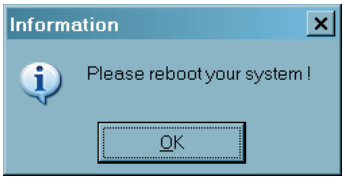
Logon Options

This option is only available under Windows NT, Windows 2000 and Windows XP.



Select this menu item enable domain logon next time the machine started. You may choose to save your domain logon credentials locally, or simply enter them when prompted to do so. An attempt to establish a VPN connection will be made during the boot process in order to logon to the domain. The VPN connection is then necessary in order to reach the domain controller. When establishing the connection you may be required to enter your password, if this was not “saved” under password in the Phonebook.

Once the Client has established a connection to the destination, you will be able to sign-on to the remote domain. This sign-on (domain logon) process, because it is done through the VPN tunnel, is encrypted.



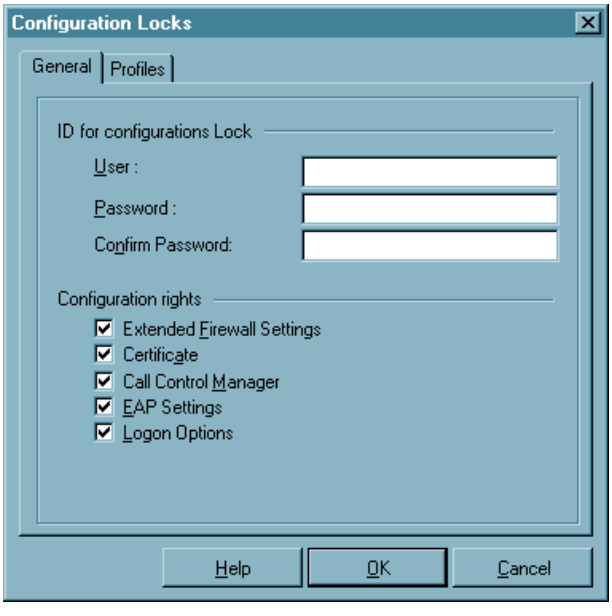
You must reboot you PC after making any changes to the “Logon Options”.

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



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.

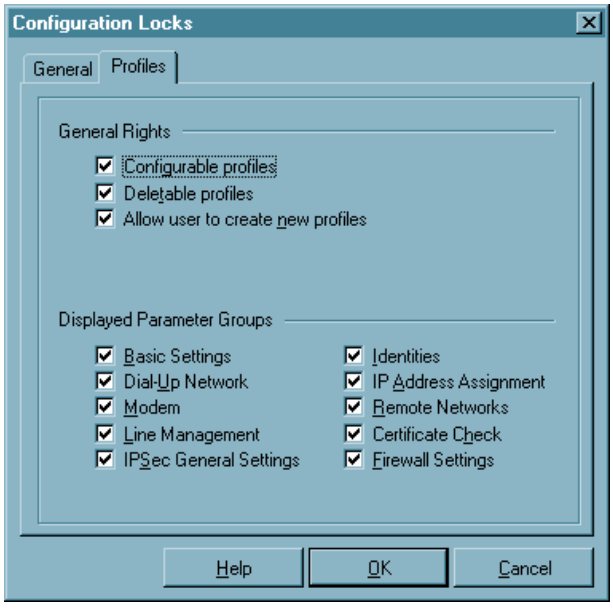
Please note that identification is absolutely necessary for the configuration block, in order to activate the blocks, or to cancel the configuration blocks. If the identification is forgotten there is no other possibility to cancel the blocks!

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

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

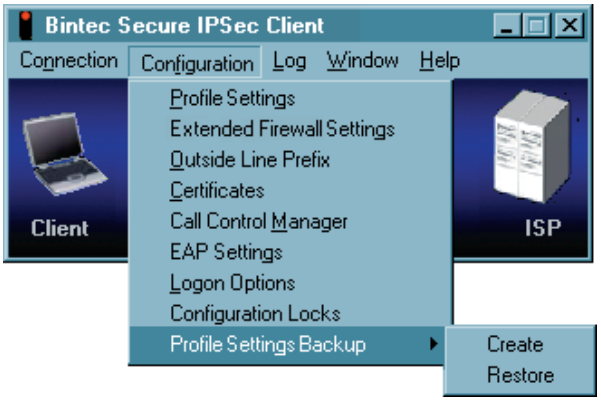
The parameter fields of the profile settings can be suppressed for the user.

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

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



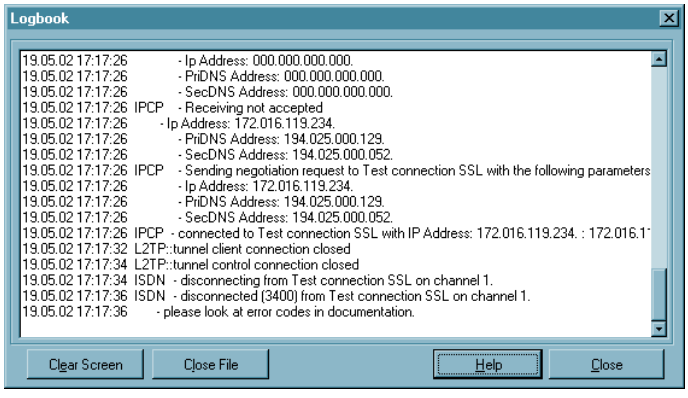
A profile setting backup will be created after each click on “Create” menu item, and after a confirmation question, that contains the configuration up to this point.

Restore

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.

3.2.3 Log

This feature automatically logs (records) all communication transactions (but not the data) going via the Client. Selecting the Log function will open the window of the log-book.



The contents of the log are stored in memory and are accessible until such a time that you (re)boot your PC.

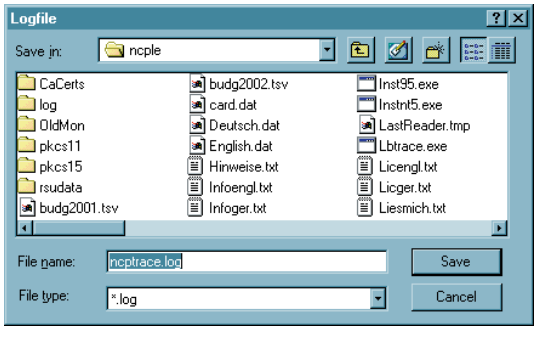
Alternatively, if required, the log can also be written (stored) to a file. The log function automatically stores all actions of the Client for a period of seven days. Log files older than 7 online days will be automatically deleted. This is where the log files are stored and are named NCPyymmdd.LOG (yy=year, mm=mouth, dd=date). The file can be opened and analyzed with a text editor.

■ Logbook

The buttons of the “Logbook” window have the following functions:

– Create File
– Close File
– Clear Screen
– Close - Logbook

Create File



Clicking this button will open a window where you can enter the name and path of the file to be created for the log feature to write (record) to (default name = ncptrace.log).

All communication transactions (but not the data) will then be written to the file until such a time that the “Close File” command is initiated. Creating a log file will enable you to make a more detailed review or analysis of your communication transactions over a longer period of time.

Close File

Clicking on the “Close” button will close the file that was established with “Create File”. Once the file has been closed it can then be used to make a detailed review or analysis of the communication transactions that have been stored.

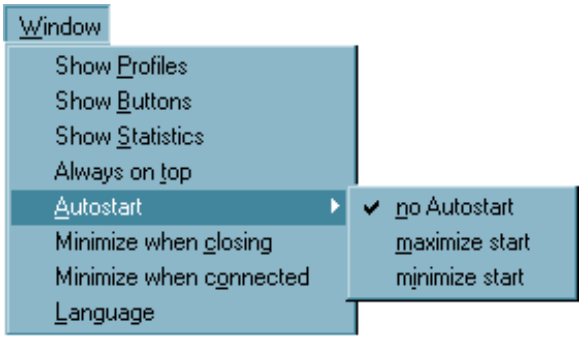
Clear Screen

Clicking this button will delete the contents of the log screen and empty the buffers.

Close - Logbook

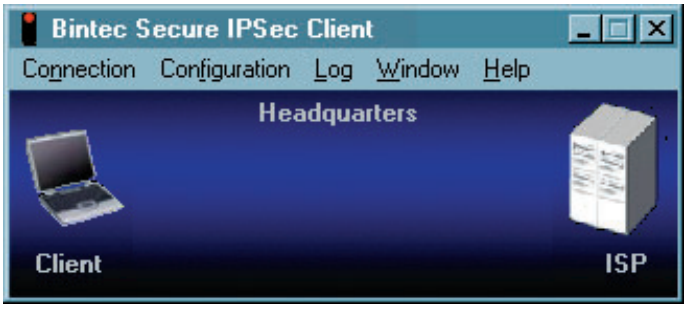
When you click on “Close” the logbook closes and returns to the monitor. Any recorded data remains unchanged.

3.2.4 Windows

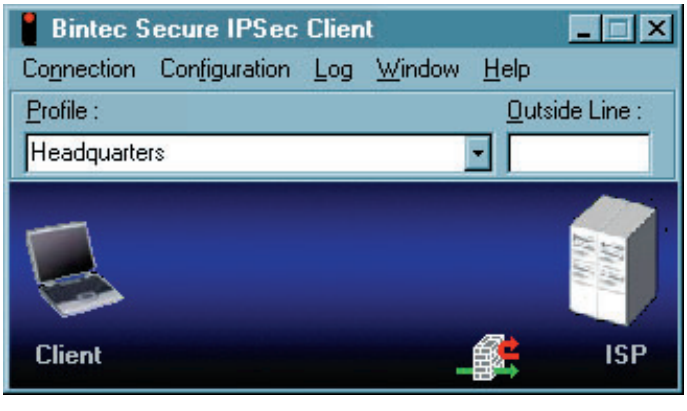


This feature lets you influence the way in which the monitor is displayed on your screen.

■ **Show Profiles**



Left side the minimized representation.



When “Show Profiles” is activated the configured destinations could be selected by clicking on the listed names (picture left side).

Show Buttons

When “Show Buttons” is activated the buttons concerning to “Connect” and “Disconnect” are displayed therefore the size of the window is larger.

Show Statistics

When “Show Statistics” is activated all information available from the monitor is displayed; the size of the window will be larger.

Always on top

When “Always on Top” is activated the monitor will always be displayed in the foreground of your desktop regardless of what application is currently active.

Autostart

This menu item allows to set the monitor to be started after booting. Use this menu item to set the following options:

- ☐ no Autostart: after booting do not automatically start the system
- ☐ minimize start: after booting start the monitor and minimize the display
- ☐ maximize start: after booting start the monitor and display it in its normal size

If you require the use of the IPSec client often and need the information displayed on the monitor, you should select the Autostart option “maximize start”. It is, however, not mandatory for communicating with the destination to start the monitor.

Minimize when closing

If the monitor is closed during an existing connection via the close button [x] in the upper right hand side of the (active) titel bar [Alt + F4], then a message window alerts you that no icon (tray icon) will appear in the task bar, this means that the user then cannot recognize on his screen whether connection charges are accrueing, how long connection charges will accrue, or whether the connection has already ended.

(In this case, the monitor must be restarted to determine the status of the connection and to correctly end the connection.)

The “Minimize when closing” menu item has been added under “Window”. If this menu item is active, then the monitor is only minimized when closing via the [x] in the (active) titel bat or via [Alt + F4]. Clicking on the close button [x] in the header has the same effect in this setting as clicking on the minimize button [-] in the (active) titel bar.

(The possible destination system can be read and the connection can be established or terminated with a right mouse click on the icon, or the monitor can also be ended if the connection is terminated.

By clicking “Disconnect” in the connection menu the monitor can be terminated.

■ **Minimize when connected**

If this menu item is activated the monitor will be minimized when the connection is established successfully.

Closing the monitor is only possible via the main menu “Connection – Exit”.

■ **Language**

The client software has been designed for international language support. The default language is English. In order to choose a language, click on “Language” in the Window pulldown menu and then select the desired language. In the near future the client will have additional language support.

3.2.5 Help

Clicking on “Help” opens a window displaying a table of contents for all available Help Text.

Clicking on “Info” opens a window displaying the Secure Client version installed on your PC.

4. Configuration Parameters

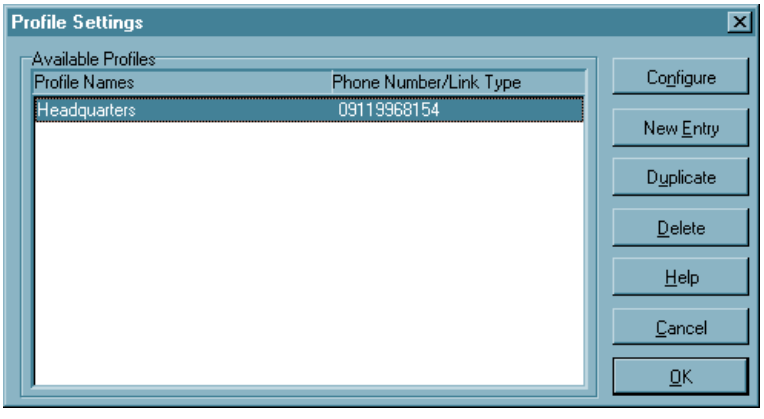
With the IPSec client you can define and configure numerous individual profiles for corresponding destinations, in accordance with your communication requirements.

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

In order to guarantee the proper functionality of your IPSec client Bintec offers a public VPN test access. A detailed step-by-step guidance how to use this test access and how to set the needed configurations correctly can be found on the Bintec websites at www.bintec.de.

4.1 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.



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***

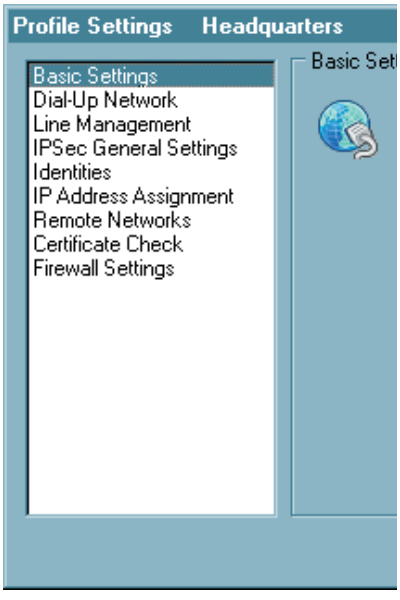
6 ***Identities***

7 ***IP Address Assignment***

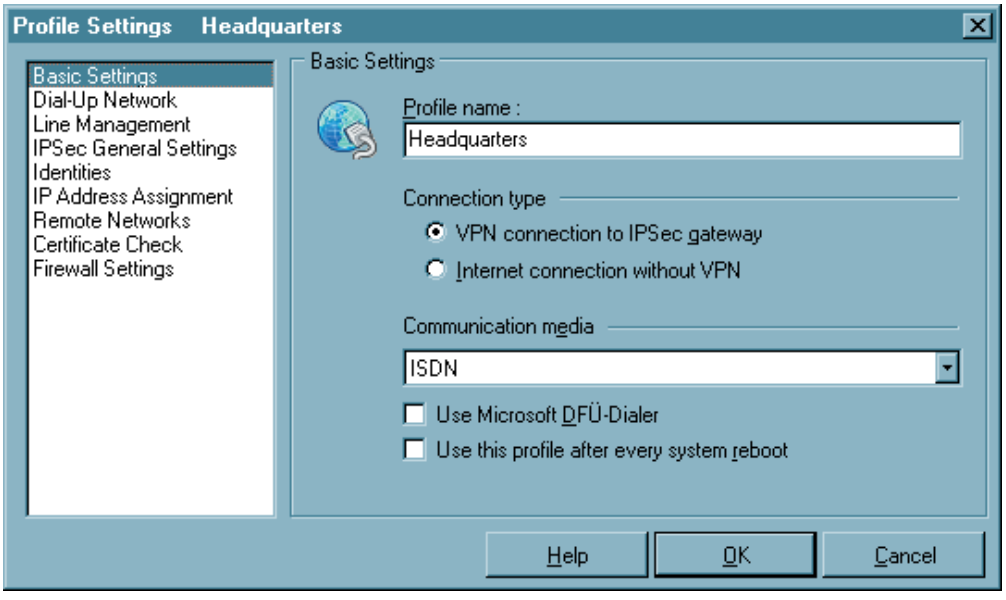
8 ***Remote Networks***

9 ***Certificate Check***

10 ***Firewall Settings***



4.1.1 Basic Settings



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
- ☐ Use Microsoft RAS-Dialer
- ☐ Use this phonebook entry after every system reboot

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.

ISDN:

Hardware: ISDN device;
Network: ISDN;
Remote destination: appropriate ISDN support;

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;

xDSL (PPPoE):

Hardware: Ethernet adapter;
Networks: Broadband (e.g. ADSL);
Remote destination: Access Router in the xDSL;

xDSL (AVM - PPP over CAPI):

If an AVM Fritz DSL card is to be used then this communication medium may be selected. AVM specific initialization strings may be entered in the field “Destination Phone Number” (“Dial-Up Network” group) for the connection. It is recommended to use the standard setting “xDSL (PPPoE)” with Windows operating systems as this provides direct communication over the network interfaces. No additional network card is necessary with the AVM Fritz! DSL card.

Networks: Broadband (e.g. ADSL);
Remote Destination: Access Router in the xDSL

GPRS / UMTS:

If a mobile (cellular) telephones is to be used (GRPS) then this communication medium may be selected. Note the description under “Installation Prerequisites” to “Analog modem”.

PPTP:

Microsoft Point-to-Point Tunnel Protocol;
Hardware: Ethernet-Adapter, xDSL Modem;
Networka: xDSL;
Remote destinations: Access Router in the xDSL;

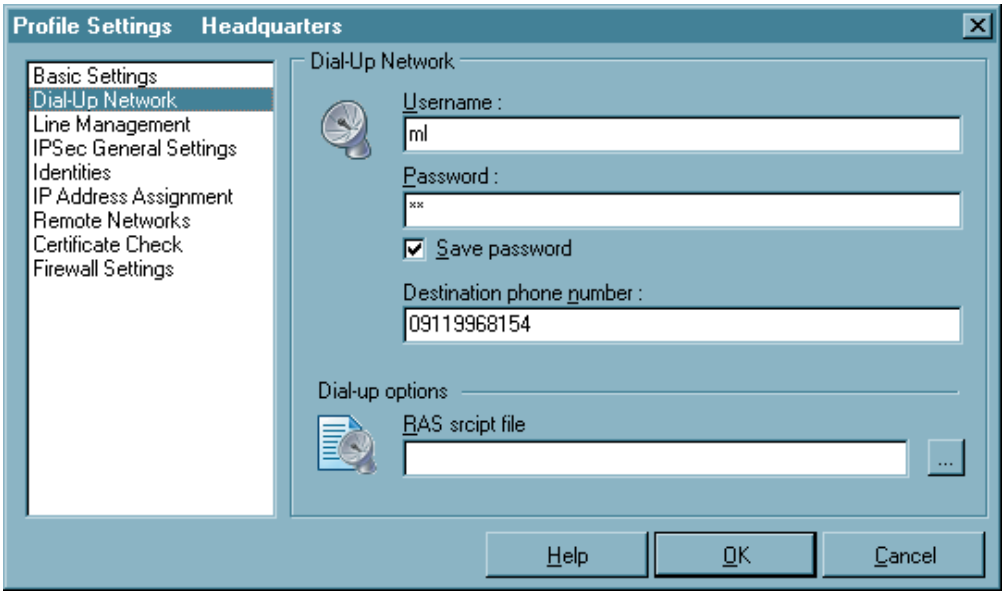
■ **Use Microsoft RAS-Dialer**

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).

■ **Use this phonebook entry after every system reboot**

Normally after a restart the Client Monitor opens with the last profile used. If this function is activated, then the profile referred to here is loaded after a system re-start, regardless of which profile was last used.

4.1.2 Dial-Up Network



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 the way in which it was assigned to you (also 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. Therefore caution should be used when your PC is left unattended.

Destination phone number

You must define a phone number for those destinations using ISDN/PSTN/GSM otherwise the Client will not be able to dial up and establish a connection to the destination or ISP. 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.

In order to acquire an outside line when communicating via a PBX it is necessary to define an “Outside Line Prefix” (see → Outside Line Prefix) in the monitor menu “Configuration”.

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 Phonebook as follows: 00441711234567.
The destination phonenumber may include up to 30 characters.

■ 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 IPSec 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.

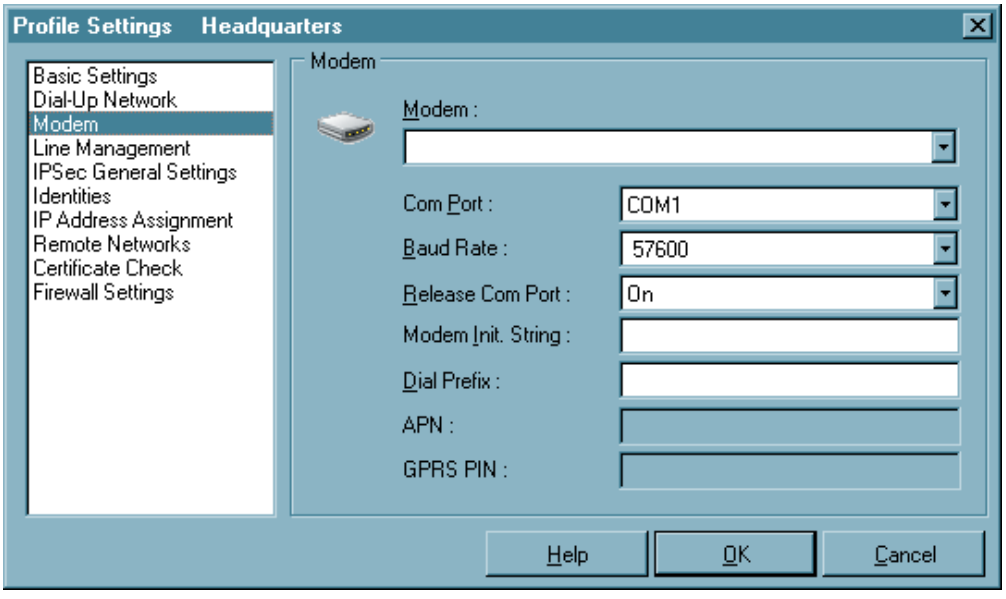
Important: This will only work if the protocol settings associated with alternate Destination phone number are the same as the primary Destination phone number

■ 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)

4.1.3 Modem



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

Parameters:

- ☐ Modem
- ☐ COM Port
- ☐ Baud Rate
- ☐ Release COM Port
- ☐ Modem Init. String
- ☐ Dial Prefix
- ☐ APN
- ☐ SIM PIN

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 Phonebook 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).

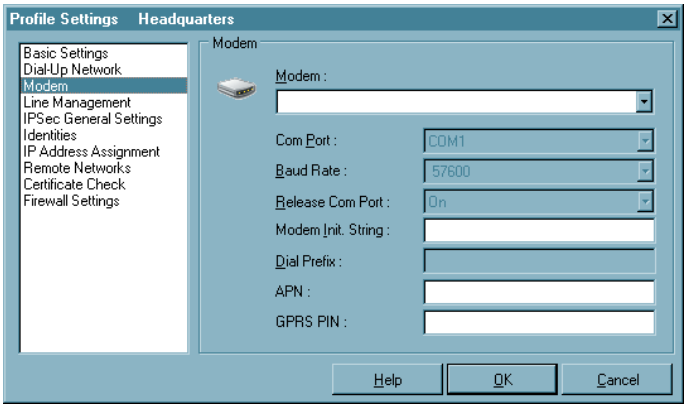
Dial Prefix

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

APN

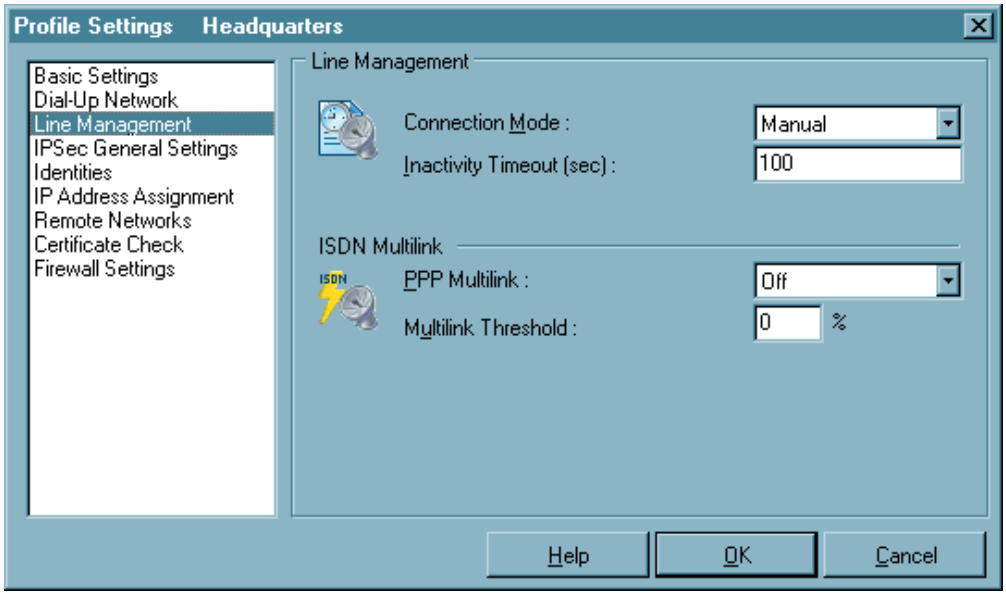
The APN (Access Point Name) is required for the GPRS and UMTS dial-in. You obtain this name from your provider. The APN is used particularly for administrative purposes.



SIM PIN

If you use an SIM plug-in card for GPRS (UMTS also), then enter the PIN for this card here. If you use a mobile phone, then this PIN must be entered on the mobile phone.

4.1.4 Line Management



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

If the client is using the communication medium “ISDN” you can activate channel bundling in this folder. In order for channel bundling to work requires that your PC be equipped with a communications device that supports multiple ISDN B-Channels. It is also necessary that the Network Access System (NAS) that you are communicating with support the same number of channels.

Parameters:

- ☐ Connection Mode
- ☐ Inactivity Timeout
- ☐ PPP Multilink
- ☐ Multilink Threshold

Connection Mode

You can define how the client builds a link via the profile to the destination. There are three Modes to select from:

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.

PPP Multilink

When using PPP Multilink the Secure Client can bundle up to 8 ISDN B-Channels, therefore in order to take advantage of this your PC must be equipped with the necessary number of ISDN BRI (Basic Rate Interface) ports.

In order for Multilink to work requires that your PC be equipped with an ISDN device that supports multiple ISDN B-Channels. It is also necessary that the Network Access System (NAS) that you are communicating with support Multilink operation. When using PPP Multilink additional costs will be incurred for each B-Channel used.

This parameter defines how additional links will be added if requested. There are 3 possible settings:

off	(default setting)
Tx	(links are added according to the bit rate demanded by the transmitter)
Rx	(links are added according to the bit rate demanded by the receiver)
TxRx	(links are added according to the bit rate demanded by both transmitter and receiver.

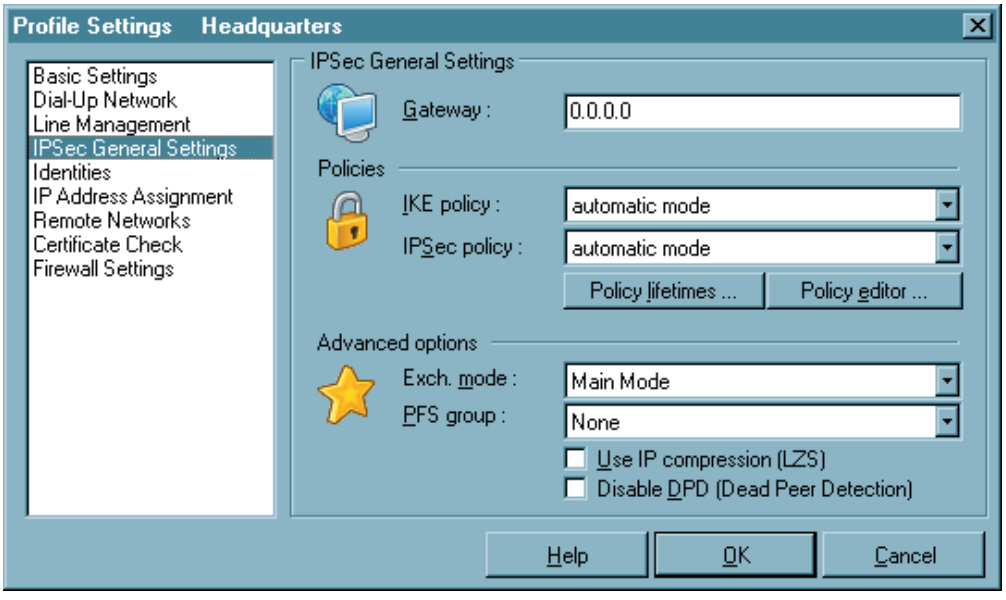
Multilink Threshold

This parameter tells the client the bit rate (as a percent of the current bit rate) at which a new link (B-Channel) is to be added. Possible settings are from 1 to 100. The default setting is “20". The Threshold setting is common to both transmitter and receiver.

In order for this value to be activated it is necessary to have Tx, Rx or TxRx under PPP Multilink selected.

Important: In order for PPP Multilink to work it must be supported by the destination’s Network Access System.+

4.1.5 IPSec General Settings



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.

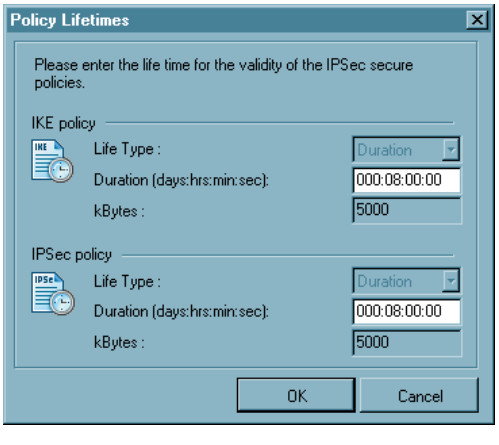
The same policies with their affiliated proposals should be valid for all users. This means that on the client side, as well as on the server side, the same proposals for the policies should be available.

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.

Policy lifetimes

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

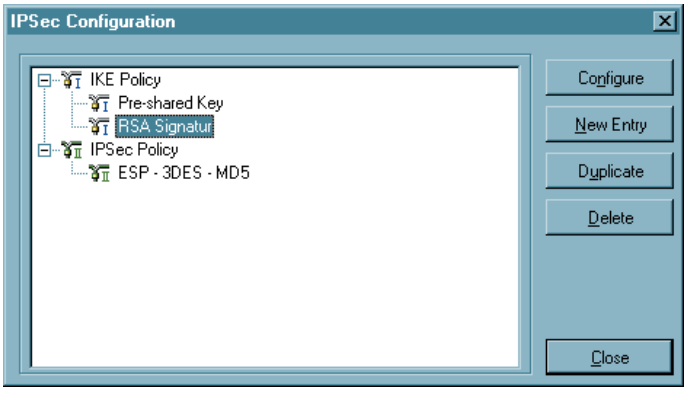


Duration

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

Policy editor

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.

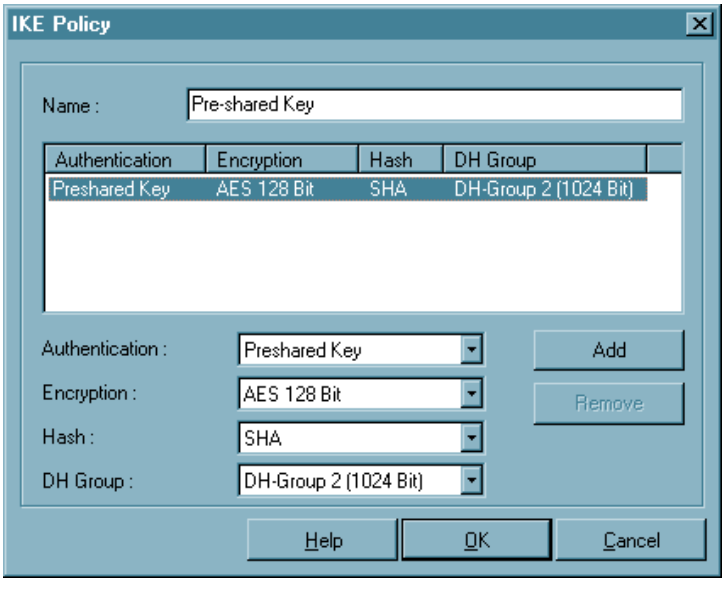
New Entry
In order to define a new Policy or SPD, select one of the Policies or the SPD and click on “New Entry”. The new Policy/SPD is entered. All parameters are assigned a default value except the Name.

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)



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, in the Phonebook 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”.

Parameters:

- ☐ Policy Name | IKE Policy
- ☐ Authentication | IKE Policy
- ☐ Encryption | IKE Policy
- ☐ Hash | IKE Policy
- ☐ DH Group | IKE Policy

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.

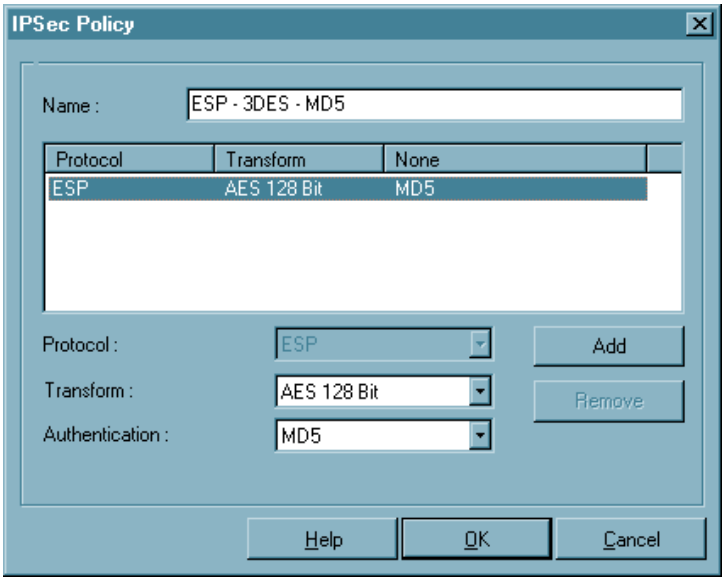
Hash | IKE Policy

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)



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”.

Parameter:

- ☐ Policy Name | IPSec Policy
- ☐ Protocol | IPSec Policy
- ☐ Transform | IPSec Policy
- ☐ Authentication | IPSec Policy

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.

Authentication | IPSec Policy

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

Advanced Options

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”.

Use IP compression (LZS)

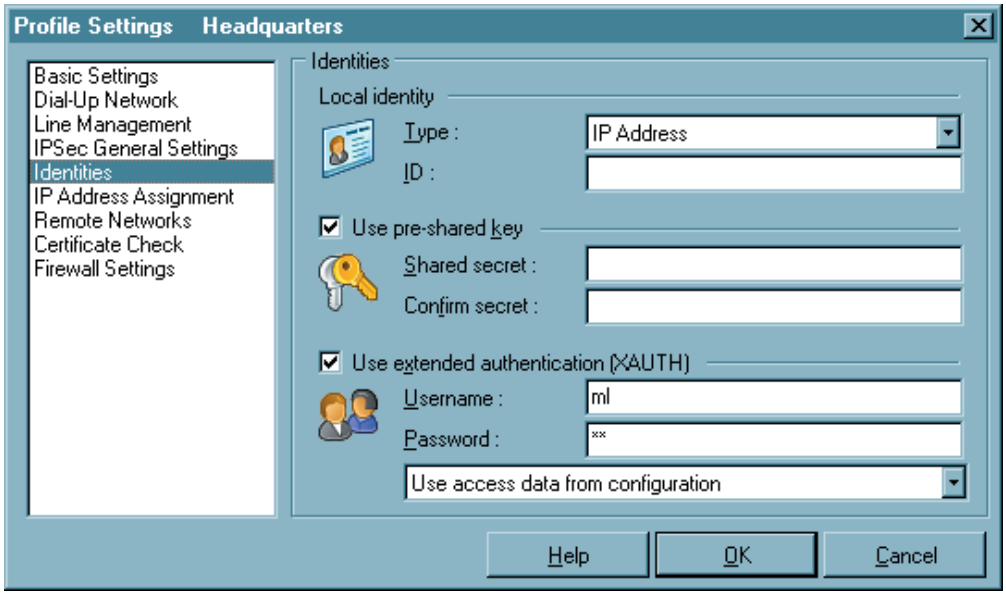
The data can be compressed in order to increase transmission rates. By enabeling compression the throughput can be increased to up 3 times that the regular transmissions without compression.

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.

4.1.6 Identities



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:

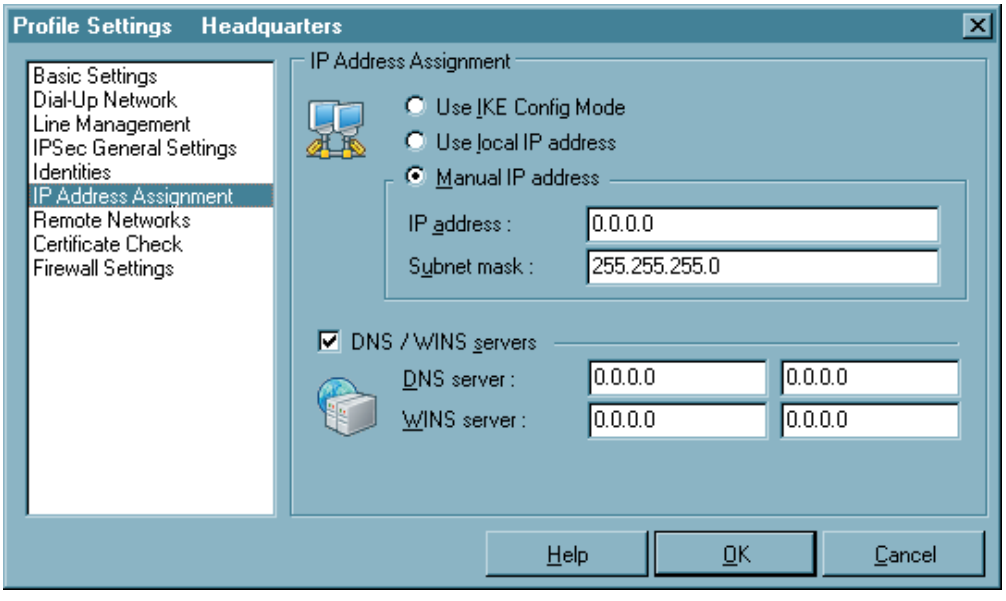
Use access data from configuration:
The VPN tunnel will be authenticated based on the User ID and Password entered in the respective fields above.

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.

4.1.7 IP Address Assignment



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.

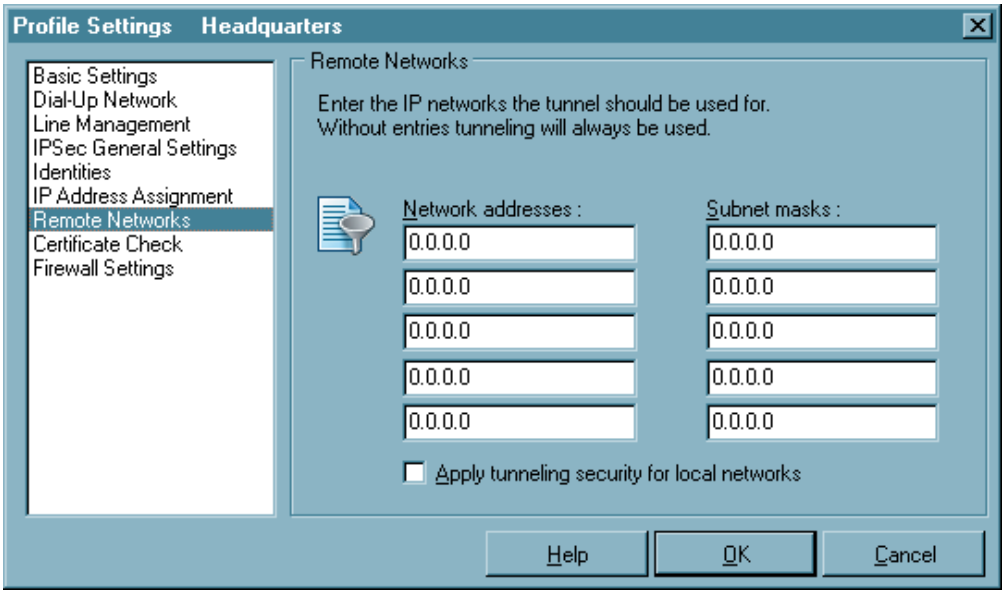
DNS server

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.

4.1.8 Remote 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

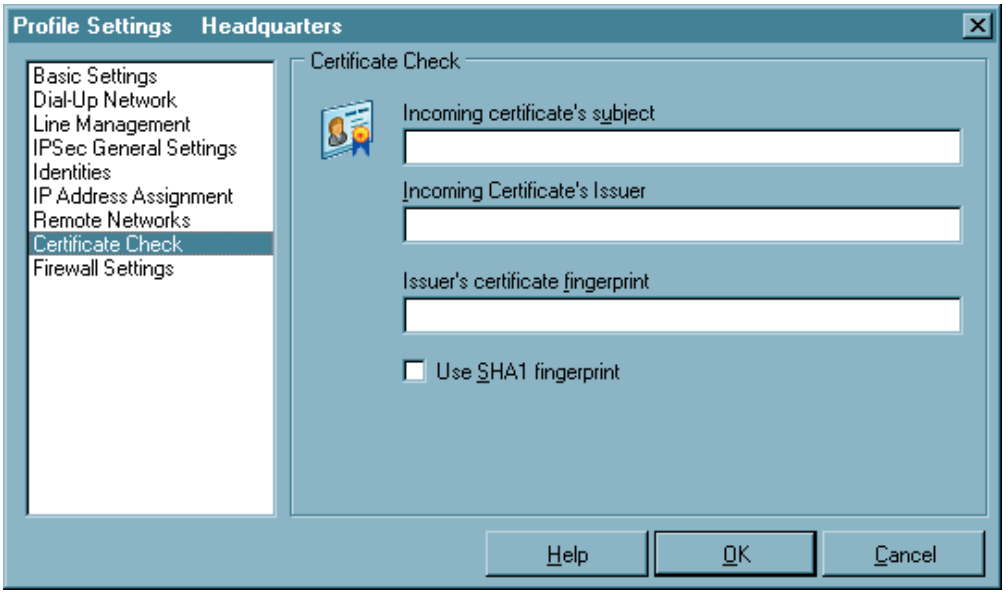
In this window enter the address(es) and netmask(s) of IP Network(s) that you want to reach via the gateway. These addresses are available from your administrator.

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.

4.1.9 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\ca-certs\ 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.

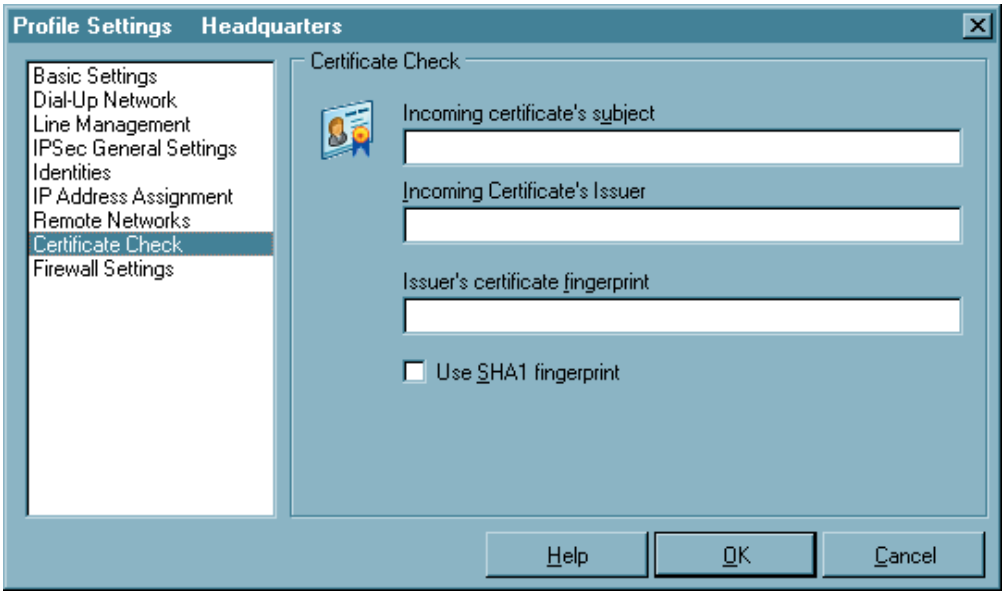
3. Checking Revocation Lists

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.

4.1.10 Firewall Settings



The “Firewall settings” 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 highest 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
- ☐ 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.

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.

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.

5. Establishing a Connection

In order to guarantee the proper functionality of your IPSec client Bintec offers a public VPN test access. A detailed step-by-step guidance how to use this test access and how to set the needed configurations correctly can be found on the Bintec websites at www.bintec.de.

■ Establishing a Connection to the destination system

Provided the software is installed properly and the profile parameters are configured correctly a dial-up to the destination system can take place. Part of the configuration is to define the mode with which this connection is to be established. There are three modes to select from: automatic, manual and variable. You define the connection mode of the destination system in the Phonebook under “Line Management – Connection Mode”.

Automatic (default):

The Client works on the principle of LAN emulation, whereas with Microsoft RAS, every connection has to be established manually. This means that the Secure Client will automatically activate a connection in accordance with your application program requirements to the destination selected in the Phonebook.

Manual:

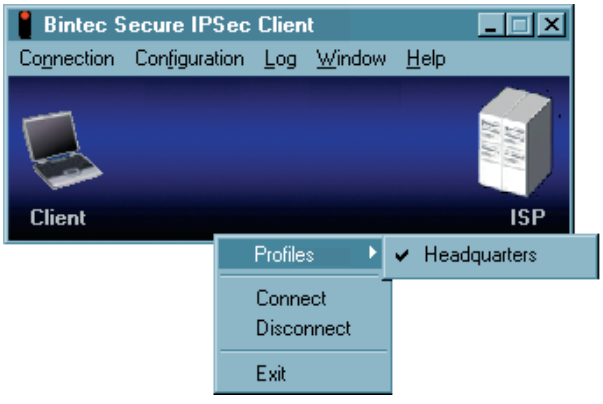
This means that you must manually activate a Connect. This is done by clicking on “Connection” in the Monitor and than selecting “Connect”.

Variable:

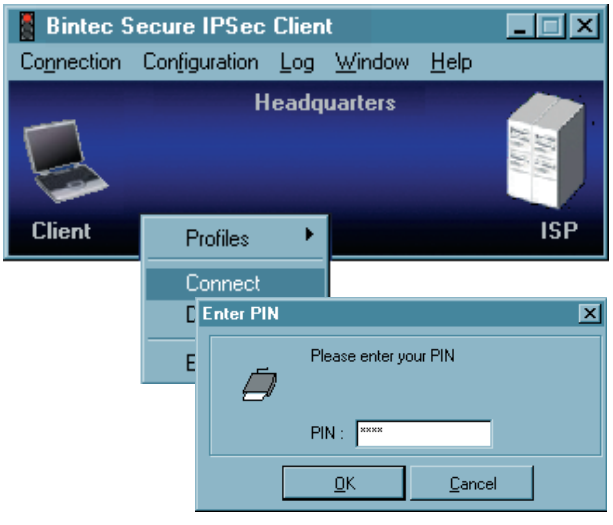
When this mode is selected, the connection must be established “manually”. Subsequently, the mode adapts according to the manner in which the connection was terminated:
– If the connection was terminated as a result of a timeout, then the following connection will be automatically initiated as required.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

■ Connect

Independent of the connection mode, the monitor always displays the connection status as explained in the following example:

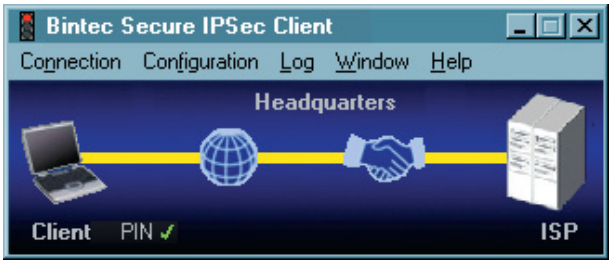


First step is to select a destination system to connect to – click the right mouse button to display the menu.



To then manually establish a connection click the right mouse button to display the menu and then select “Connect”.

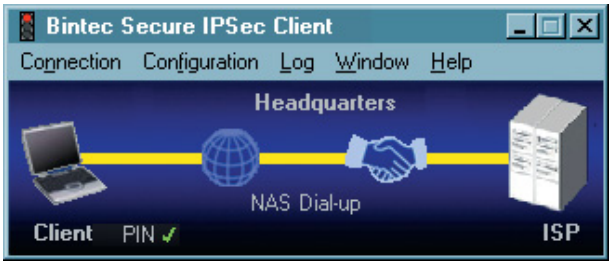
If the use of a (Soft-) Certificate was configured you first have to enter the PIN.

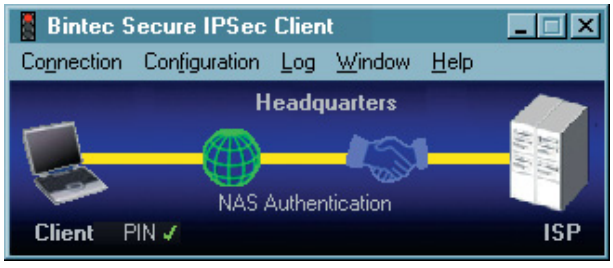


Then a link to the Internet Service Provider (ISP) is built indicated by a yellow line. The dial-up negotiation is displayed with a symbol representing a globe and the authentication status with a handshake. Upon doing so the symbols change according to the current status.

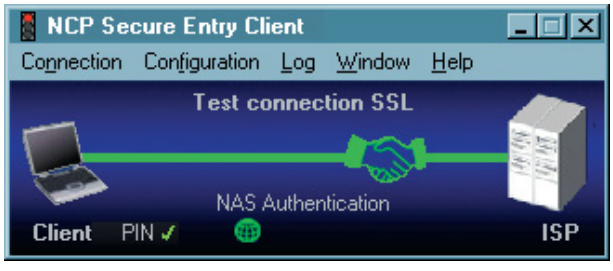
light blue = Link building stage

dark blue = Stage passed



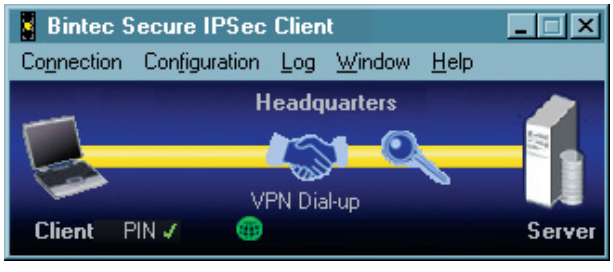


green = sucessfully negociated stage.

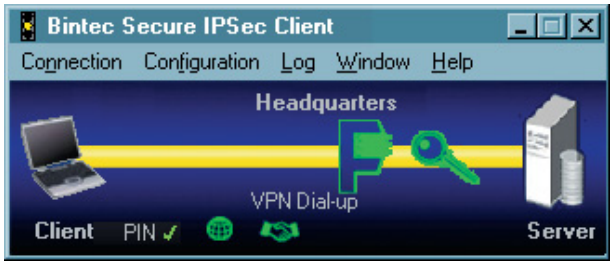


The sucessfully passed stages are displayed by minimized symbols.

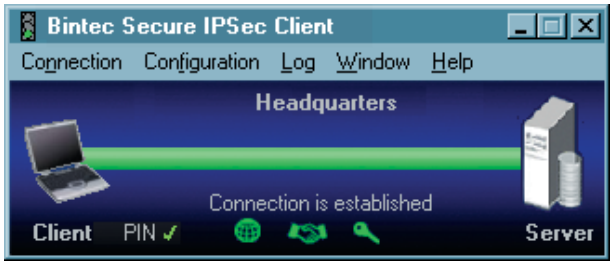
Upon a successful authenticated connection with the ISP/Network Access Server (green line and green handshake symbol) ...



... a tunnel is built indicated by a new yellow bar and the second dial-up to the VPN Gateway starts. Here authentication is necessary as well. In addition under the use of Test connection SSL an encryption (key) is configured.



If the configuration of the destination system is set to utilize compression, you can configure compression as well.



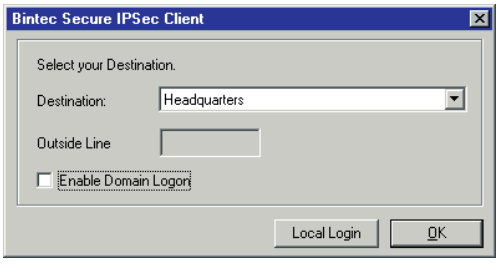
If the last stage of the link built (here encryption resp. descryption) is successfully passed, the traffic light swiches to green...

... as well as the tunneling. Now a connection is established.

Please note that green traffic lights indicates that a link is built and that communication costs are beeing incurred!

Client Logon

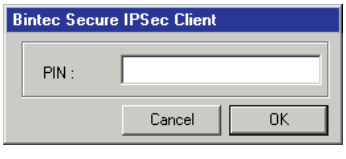
If the Client Logon to the Network Access Server occurs before the Windows Logon to the remote domain, ("Logon Options" (see → Monitor, Logon Options), the connection is established in the same way as described under "Connect" (see above).



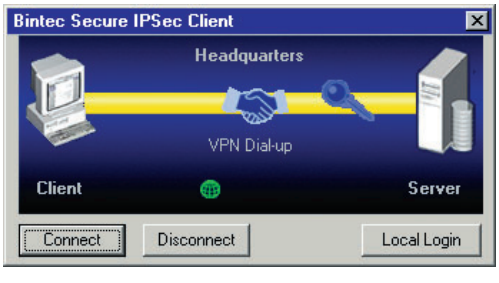
To initiate a link to be built, select the destination system to connect to and then click on the OK button.

Local logoff:
With a click on this button the link build is stopped.

Activate Domain Logon: With this option a safe WAN domain logon is possible, even if the logoff was not executed correctly. The logon takes some seconds. This function is not necessary if the shut down of the PC was made correctly and mapped drivers were disconnected properly.



If the use of a (Soft-) Certificate was configured – like example destination Test connection SSL – you first have to enter the PIN.



The following stations of the link built in the same procerure as described above under "Connect"...

... until the connection is established.

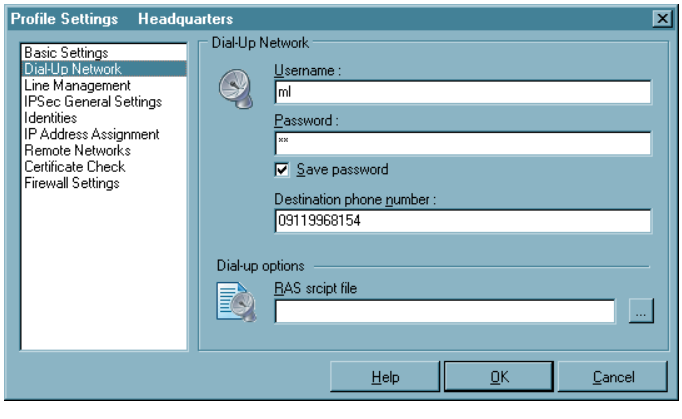
Passwords and User Names

The password (see → Dial-Up Network, Password) is used for identifying 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 password ID can include up to 256 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, for authentication purposes. Upon entering your password all characters will be displayed as an asterisk (*) in order to keep them from being overlooked by someone else. Therefore it is necessary to be very careful that you enter your password exactly the way in which it was assigned to you (pay attention to upper case and lower case characters).

Even if you selected “automatically” as connection mode (see → “Establishing a Connection to the destination system”), you have to establish the first connection manually and enter the password. For every additional automatically established connection the password is adopted automatically, until you reboot your PC or you select a different destination system. This means that even though the function “Save Password”(see → Dial-Up Network) was not activated, automatic connections can still be made where this cached password is used to authenticate. When (re)booting your PC the once entered password is then deleted (Please notice → Logon Options).

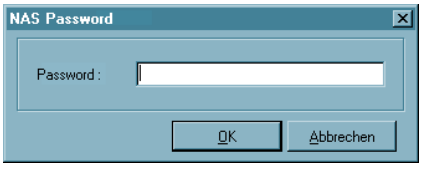
If you do not want to delete the password when (re)booting your PC you have to activate the function “Save Password” (see → Dial-Up Network). Please notice that for security reasons you must be aware that should some unauthorized person use your PC, they will be able to use your password. Therefore caution should be used when your PC is unattended.

User ID for NAS Dial-Up

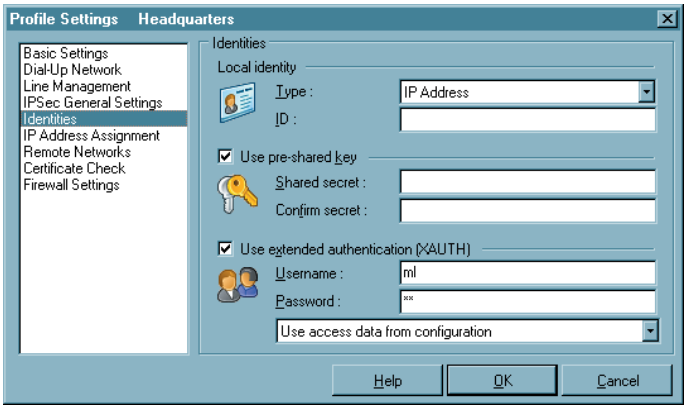


If the Password has not been entered or saved it will be requested in a seperate window.

The “User Name”of the Dial-Up Network must always be entered in the configuration of the profile. Without this User ID a dial-up to the NAS is impossible (see → Dial-Up Network)



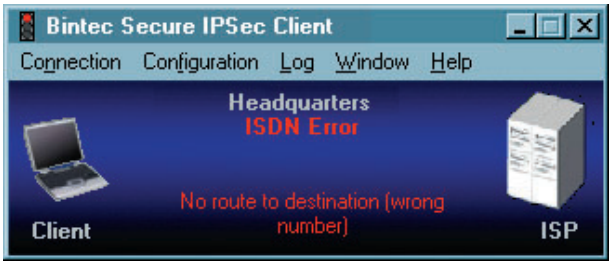
User Name and Password for Extended Authentication



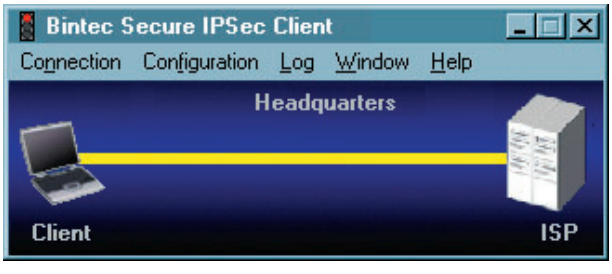
If you use Extended Authentication, User Name and Password must be entered in the configuration folder of the profile. Otherwise the establishing of a connection will not be successful (see → Profile Settings, Identities, Use extended authentication (XAUTH)).

Disconnection and error

If an error occurs, a connection will not be established and the reason is displayed in the monitor (please notice the passage “ISDN CAPI Error Codes“)



Disconnect

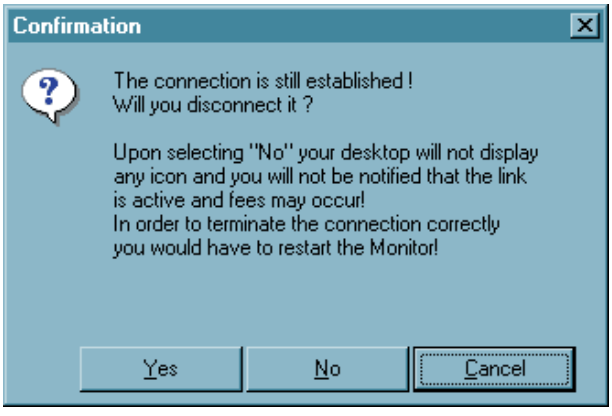


With the function “Disconnect” a connection can be manually terminated. If you want to keep the possibility to disconnect manually you have to set the connection mode to “manually” and deactivate the active Timeout by setting it to zero (0) (→ Connection Mode).

If the connection is terminated, the color of connection line changes until it disappears and the lamps of the traffic light changes from green to red during the period of offline.

Disconnect (the Monitor)

If the connection is still established, with a click on this menu item or on the “Disconnect” button, the monitor can be closed as well. Please note that the connection is not automatically terminated by closing the Monitor. If the link should be established although the monitor is closed and fees may occur , the software asks you explicitelly for a prompt (see picture)



Upon selecting “No” your desktop will not display any icon and you will not be notified that the link is active and fees may occur! In order to terminate the connection correctly you would have to restart the Monitor!

6. Examples and Explanations

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

6.1 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.

6.1.1 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.

6.1.2 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.

Class 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.

6.1.3 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.

6.1.4 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.

6.2 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.

6.2.1 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.

6.2.2 Extended Firewall Settings

The extended 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 [...].

6.2.3 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)**

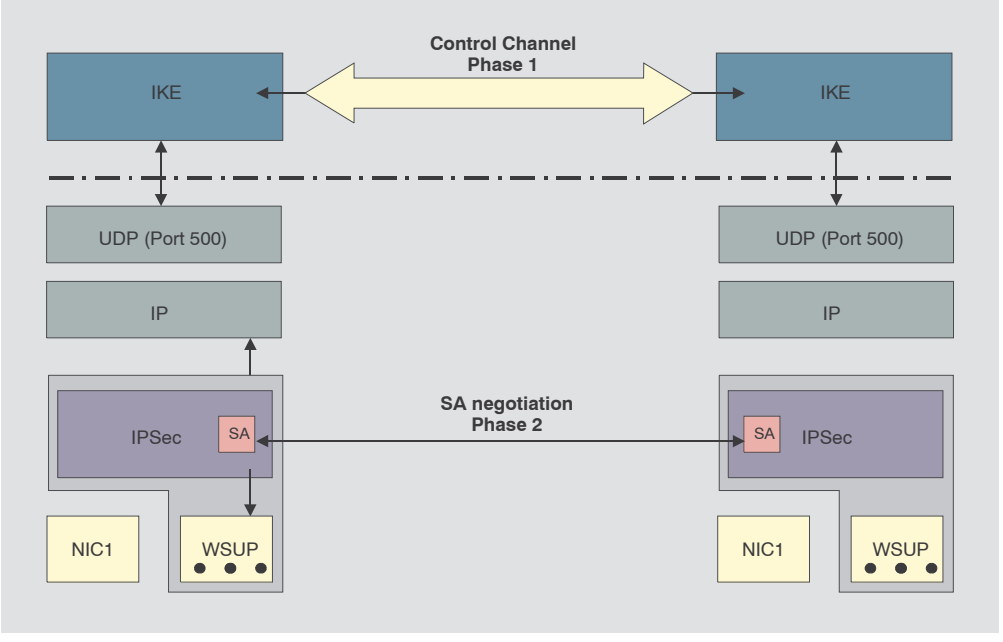
IPSec establishes the control channel in tunnel mode over the IKE protocol to the IP address of the secure gateway. In Transport mode it is established directly to the IP Address of the other side.

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.

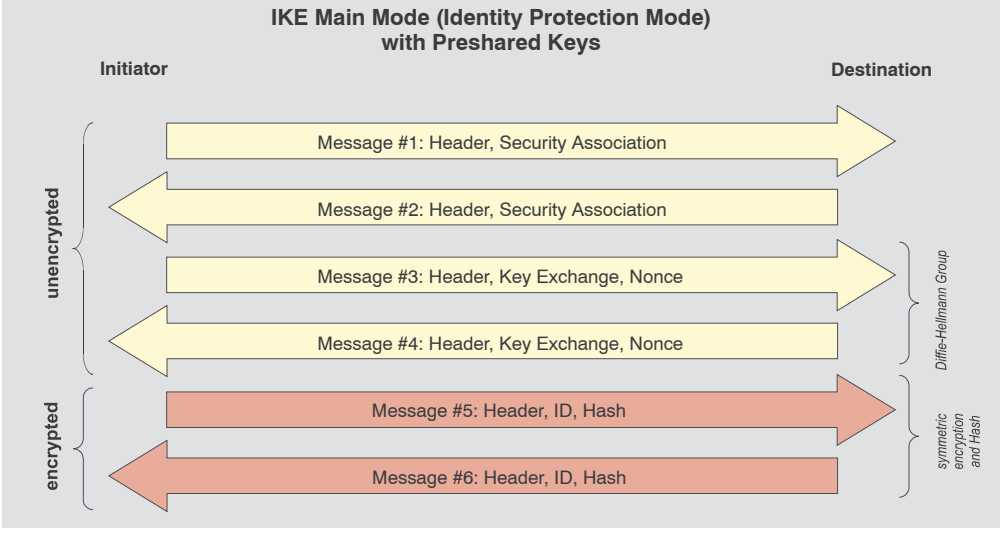
IKE Modes

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.

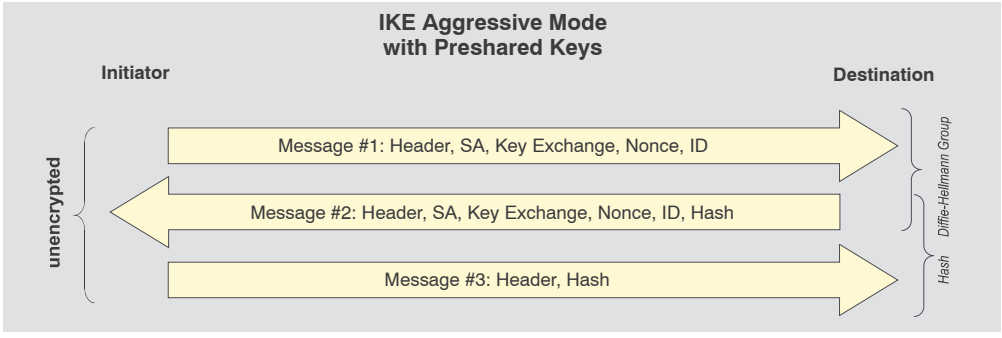
In Main Mode (standard setting) six messages are sent over the Control Channel and the last two messages are encrypted. The last two messages contain the user ID, the signature, the certificate and, if required, a hash value. This is why it is also known as Identity Protection Mode.

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

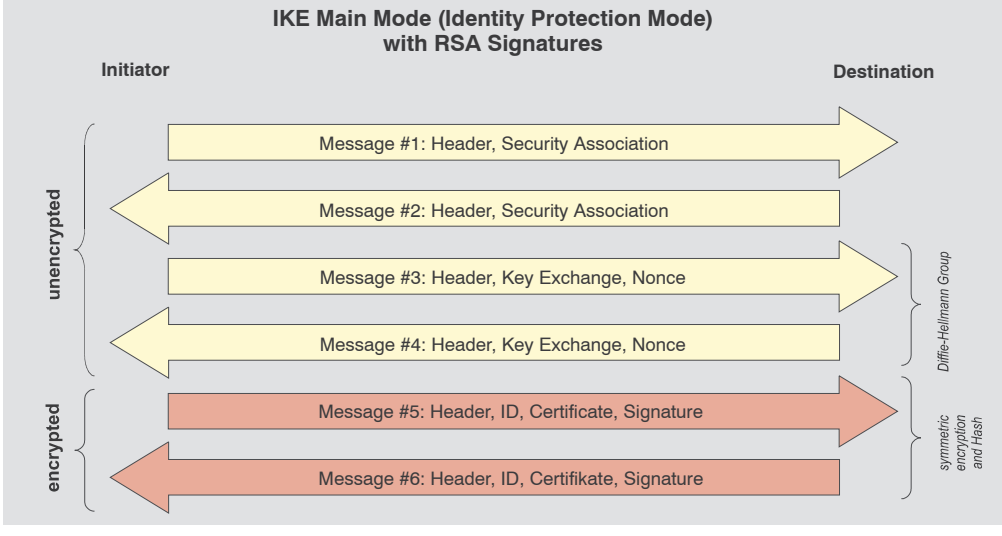
You determine the IKE mode (Exchange Mode), Main Mode or Aggressive Mode "Security" parameter fields under "Link Profiles" (for a dynamic SPD) and under "IPSec, Secure Policy Database" (for a static SPD). (See also → Exchange Mode).



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.



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.

6.2.4 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

6.2.5 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.

6.2.6 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:

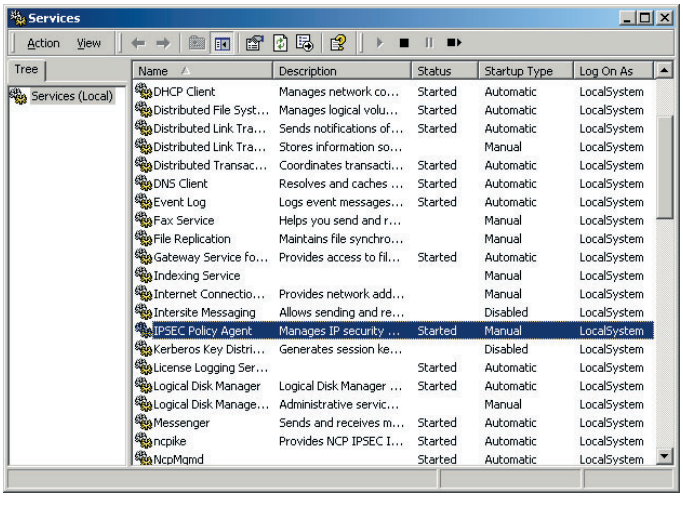
1. To determine which ports are currently being used by your system, you can enter the following command under the Command Prompt:
   `netstat -n -a`
   to display current network status.

```
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”.



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.

6.3 Certificate Checks

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

6.3.1 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\ca-certs\ 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.

6.3.2 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.

6.8.3 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.

6.4 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 seg-

ments. 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 implementation 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 directo-

	ry. 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. Certifica-

tes 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 cer-

	tificates 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

D

E

F

G

H

I

R

S

T

U

V

W

X