

## NCP Secure Entry Client (Windows 32/64 Bit)

New Features version 9.2 to 8.1

### **Disclaimer**

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

### **Trademarks**

All trademarks or registered trademarks appearing in this manual belong to their respective owners.

## Overview

New features in version 9.23 build 18 to version 9.20.....	2
New features in version 9.2 build 33 to version 9.10 build 55.....	3
New features of version 9.1 relative to version 9.0.....	6
New features of version 9.1 relative to 9.04.....	6
New features of version 9.04 relative to 9.03.....	6
New features of version 9.03 relative to 9.01.....	7
New features of version 9.01 relative to 9.0.....	8
New features of version 9.0 relative to Version 8.3.....	8
New features of version 8.3 relative to version 8.2/8.1.....	11

## New features in version 9.23 build 18 to version 9.20

### FIPS inside

The IPsec Client incorporates cryptographic algorithms conformant to the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1051).

Benefit: Official standards proof security level.

### Use a User Certificate stored in the Windows Certificate Store via CSP

For authentication purposes you can access (read only) user certificates, stored in the Windows Certificate Store, via CSP. You can only use this feature after successfully logging on to the windows system.

Since this function is only available after the user's logon to the windows system, it cannot be used for domain logon via VPN.

Benefit: The certificate may be loaded from the certificate store provided by your operating system.

### NCP's VPN Path Finder Icon

If you set up a connection via port 443 with the VPN Path Finder, the monitor displays this via an icon in its state display (below the HQ / Gateway to the right).

Benefit: For the convenience of the user, the client monitor displays any connection set up via NCP's VPN Path Finder Technology.

## **New features in version 9.2 build 33 to version 9.10 build 55**

### **Windows 7 Support (p)**

Full support is provided for the new Microsoft operating system Windows 7 starting with version 9.2. For this reason, the NCP Secure Entry Client runs under all 32/64 Bit Windows operating systems:

Windows XP, Windows Vista, and Windows 7

All current Windows desktop operating systems are supported by using the same graphical user interface.

*(Please note: The support for Windows 2000 has been discontinued, starting with version 9.2. In case of an update from Windows Vista to Windows 7, only the monitor of a Client version 9.1 can be started in order to enter a Client version 9.2 key.)*

### **NCP VPN Path Finder incl. proxy support (p)**

If default IPsec via port 500 or UDP Encapsulation via a freely configurable port is not possible, the NCP VPN Path Finder technology causes an automatic switchover to an alternative connection protocol - TCP encapsulation with SSL header via port 443. (In connection with NCP Secure Server 8.0)

The user has the possibility to connect to the corporate headquarters via IPsec tunneling, even with restricted internet access (to HTTPS port 443).

### **Wi-Fi roaming**

If the teleworker moves his laptop within the range of several access points with the same SSID, the system automatically switches to an access point with higher field strength in the case of low Wi-Fi reception. Applications communicating via this VPN tunnel do not "notice" this change.

The NCP Secure Entry Client can switchover to different access points within corporate networks (e.g. change of location with a laptop) without the need to set up a new connection and logging on to the VPN Gateway i.e. continuous remote access is possible despite changing IP address.

### **Improved data throughput on 64 bit Windows platforms**

For the use of the RWSNT service, data throughput has been augmented by about 20%.

### **Support of new Intel Wi-Fi driver versions 12.4.0.21 or above**

The new drivers are seen as Wi-Fi drivers instead of Ethernet drivers. For this fact it is necessary first to uninstall the NCP Secure Entry Client, reboot and then install the new NCP Secure Entry Client. In this process all settings made so far remain.

### **Support of Windows 7 mobile broadband driver (3G)**

## NCP Secure Entry Client (WIN 32/64)

### **Revised 3G configuration, provider list configurable via INI file (APN.ini)**

A new parameter folder GPRS / 3G has been introduced in the profile settings and with that the former 3G configuration has been revised. There are three modes now:

- a) Provider list (default setting): By selecting the provider, the Access Point Name (APN) and the dial-up number is being suggested.
- b) APN from SIM card: The APN is not handed over to the SIM card, this requires an APN configured on the SIM card.
- c) User-defined: The user is free to configure all dial-up parameters manually.

The use of GPRS/3G configuration has been facilitated even further.

### **Revised Wi-Fi GUI in regard to field strength measurement and tray icon**

If "Wi-Fi" has been activated, the affiliated tray icon appears in the taskbar. This icon shows the current connection state, the field strength and the mode of encryption. Clicking on the tray icon, all available Wi-Fi networks are displayed. Selecting one of the Wi-Fi networks either starts connection set up or the Wi-Fi profile wizard if no Wi-Fi profile has yet been configured. The Wi-Fi profile wizard facilitates connection set up to a new Wi-Fi network and automates connection set up to a new Wi-Fi network. The encryption mode (WEP, WPA, and WPA2) is now automatically detected during this process.

Wi-Fi handling has been facilitated for the user even further.

### **Status display for scanning Wi-Fi networks and connection set up (animated icon)**

If "Wi-Fi" is activated, a periodical scan is run for all Wi-Fi networks available. During scanning the respective icon is animated. Connection set up to an access point is displayed with a blinking yellow ball next to the selected SSID of the Wi-Fi network. A green ball indicates an established Wi-Fi connection. If several Wi-Fi access points use the same SSID, an additional small red triangle is displayed next to the SSID.

Wi-Fi handling has been facilitated for the user even further.

### **Tip of the day**

With each start of the monitor, a new "tip of the day" appears in the order in which the tips are stored in the INI file (in the directory tips). Clicking on the tip opens the affiliated HTML page in the default browser.

The user is being informed about the software potential of his remote workstation.

### **Profile export**

This feature exports the selected profile. Then it can be imported to another NCP Secure Entry Client. Certificates, however, have to be imported separately.

In the easiest of ways, the user can transfer his VPN profile to another computer.

## NCP Secure Entry Client (WIN 32/64)

### **Budget manager history for the previous twelve months**

The budget manager provides access to all relevant information about the data communication of the previous twelve months.

### **Vodafone web sessions support**

Easy-to-use for Vodafone users, too; after setting up a VPN tunnel by clicking on "connect" the user can log on to Vodafone web sessions.

### **Modernization of the graphical user interface**

The graphical user interface has been further optimized and adapted to the demands of the market.

The core changes are:

- A single connect/ disconnect switch
- World map depending on time zone;  
Depending on the time zone configured on the PC the corresponding section of the world map is displayed: Europe, America and Asia / Australia.
- Time dependant world map featuring the border between day and night;  
Depending on the time of day, the border between day and night is displayed. The position is being refreshed every ten minutes.

### **Improved log handling**

When highlighting a line in the monitor's "log", the log stops scrolling which allows for better log viewing and evaluation of the log entries.

### **Faster connection set up**

Faster connection set up can be achieved by optimization of the client in a disconnected state in the DHCP mode and by using manual connection set up.

### **Enhancement of encryption and hash options**

Diffie-Hellmann-Group 14, SHA-256, SHA-384 and SHA-512

### **Further changes:**

- "VPN IP Networks" has been renamed "Split-Tunneling"
- Optimized display of scanned Wi-Fi networks
- French and Polish have been added to the setup routine
- Number of configurable remote VPN networks raised to 250
- IPsec Optimization: Improved compatibility
- Improved processing of application related rules within the client's personal firewall
- Improved handling of language selection in the client's GUI

## New features of version 9.1 relative to version 9.0

### New features of version 9.1 relative to 9.04

#### **Budget Manager (p)**

The **Budget-Manager** serves to monitor the costs of all available connection types, focusing on UMTS, GPRS as well as WLAN connections. For this purpose, the administrators or users configure volume or time limits according to the basic provider rates. Should the user exceed his set limit, depending on the settings either a warning notice appears or further connection attempts are hindered. The Budget Manager also allows the restriction or disabling of roaming. Nasty surprises in the monthly provider invoice are avoided in this manner.

#### **Extended Certificate Configuration (p)**

A number of individual certificate settings may be saved as multi certificate configurations in the client configuration. Per profile, one certificate configuration can be chosen from the selection. The different certificates enable authentication against different VPN remote stations e.g. to VPN gateway 1 with soft certificate and to gateway 2 with a certificate saved to smartcard.

#### **Profile Filter**

The configured profiles can be combined into groups, which can then be easily selected via the context menu of the client monitor. This can increase the clarity of existing

#### **Client Info Center**

Log and error messages were revised and their informative values were increased to optimize user help desk support. An overview with the following information is available:

- Client version (incl. build number)
- Current connection status (connected, broken, broken with error)
- Client service status
- Current certificate configuration (incl. validity)
- VPN user ID
- User for management server connection

### New features of version 9.04 relative to 9.03

#### **Importing PCF Data**

Via the Entry Client monitor menu "Configuration / Import Profile", configuration data for the profile can be read in with the help of a wizard. These profile settings can be created from the prevailing destination system as differential data types. If individual configurations are not present in these profile settings (e.g. password), these are called by wizard upon import. The NCP Entry Client supports the following data types:

\*.ini, \*.pcf, \*.wgx and \*.spd.

#### **Roaming with IPSec Connections**

If a new IP address is assigned to the client during a session with wireless LAN or LAN connection via DHCP, the client assumes the new IP address and sends an

## NCP Secure Entry Client (WIN 32/64)

IKE notify report (NCP-specific) to the gateway in order to inform the address change. Meanwhile, the IPSec connection is not interrupted and need not be reestablished.  
Prerequisite: NCP Secure Server >= 7.02 Build 25.

### **WISPRr for comfortable Login on T-Mobile Hostspots**

The NCP Secure Entry Client 9.04 Build 60 supports the new logon technology via WISPr protocol (Wireless Internet Service Provider roaming). This ensures compatibility to T-Mobile hotspots in Germany, Austria, Netherlands, Czechia and Great Britain, and also in some Lufthansa lounges of international airports. The configuration can be made by entering the access data into a script of a WLAN profile.

### **Improved UMTS card handling**

#### **Store SIM PIN in the Configuration**

The option "Store SIM PIN in Configuration" has been added in the dialog for entry of the SIM PIN for GPRS/UMTS cards. If this function is used, the formerly registered SIM PIN is employed for each destination system with the connection medium GPRS/UMTS, and need no longer be entered specially.

This function is not visible in the Entry Client default setting. It becomes visible and configurable for the user when the privilege is granted to him in the configuration locks under "GPRS/UMTS", i.e. "Allow user to save the SIM PIN in the configuration" has been activated.

### New features of version 9.03 relative to 9.01

#### **64-Bit operating system (p)**

The new client supports Microsoft Windows XP for 64 bit.

#### **License Key for Windows Operating Systems**

To use the client software on Windows XP 64 bits and Vista 64 bits and Vista 32 bits a version 9.0 license key is required.

#### **Driver Signature for Windows XP**

The intermediate driver for the Windows operating systems XP 32 bits and XP 64 bits is now signed. The security detection therefore will no longer prompt the user about installing an unsigned driver. Problems with third party firewalls should no longer occur due to the adaptation of the signed intermediate driver.

#### **2-factor authentication OTP Mobile**

OTP Mobile by T-Systems and T-Mobile uses the existing mobile phone for 2-factor authentication. It calculates at the press of a button – completely without mobile radio connection – a one-time password, that the user enters in the login mask of the application.

## NCP Secure Entry Client (WIN 32/64)

### **Support for certificates with a key length of 4096 bit**

Certificates with a key length of 4096 bit can be deployed on the server and client side for user authentication.

### New features of version 9.01 relative to 9.0

#### **64-Bit Operation System**

The current version of the client software supports the 64-Bit operation system of Microsoft Windows Vista.

### **New features of version 9.0 relative to Version 8.3**

#### **Support of Windows Vista (p)**

With version 9.0 of the NCP Secure Entry Client in addition to the operating systems Windows 2000 and Windows XP, Windows Vista is also supported.

The Client user interface has been visually adapted to the Windows Vista operating system without changing the relationship between the icons and the functional sequence of connection set-up and authentication.

Installation of the Client software 9.0 under Microsoft Vista requires a license key for this version. This software cannot be operated under an older license key.

#### **Multi-function card**

In the "Connection" monitor menu, the menu item "Multi-function Card" is displayed if a multifunction card is inserted, and if it has been detected by the Client. (New additions to the set of supported multifunction cards are: The integrated card of the Lenova notebook (Sierra chipset) starting with version 8.31 and Vodafone Easybox USB adapter for UMTS/GPRS.)

The following functions are executed via the "Multifunction card" menu item:

- Network search
- Activate UMTS or GPRS
- Enter or change SIM PIN

A PIN dialog for entering the SIM PIN is always displayed if the media type "UMTS/GPRS" has been configured in a profile, and if a multifunction card that the Client detects has been inserted.

In addition, the functions "Network search", and "Activate UMTS or GPRS", can also be triggered via the field for graphic display of the signal strength. This field is opened automatically if you select a profile with the connection type "UMTS/GPRS" from the profile settings.

## NCP Secure Entry Client (WIN 32/64)

### WLAN panel

Depending on the connection medium of the current link profile, in the Monitor menu "window" under "Show WLAN status", you can open or close a separate field for graphic display of WLAN field strength, if a WLAN configuration has been activated in the the Monitor menu, "Configuration", under "WLAN settings". A button [...] in this panel takes you directly to the configuration field of the "WLAN settings". If a multifunction card has been configured, then the menu item "WLAN panel" is not active.

### EAP Authentication

You can specify whether EAP authentication will only be executed via WLAN cards, LAN cards, or via all network cards, in the "EAP Options" of the Monitor menu. The setting made here applies globally for all phonebook entries. In an activation box the EAP authentication can be set as follows.

- Deactivated
- For all network cards
- Only for WLAN cards
- Only for LAN cards

### EAP Authentication before Destination Selection when using Gina

Under the "Logon Options" in the Monitor menu the parameter "Execute EAP authentication before destination selection" has been added. If this parameter is activated then EAP authentication will be executed prior to the destination dialog in Gina and the system will ask for the necessary PIN, regardless of whether EAP will be required for subsequent dial-in. This parameter can be used, for example, if the NCP Gina will only be used for EAP authentication, without setting up a connection to destination system (use as a pure EAP client).

### EAP for WPA Encryption (p)

In the Monitor menu under "Configuration / WLAN Profiles", the option "EAP" can be added under "Key Management" for WPA encryption. The prerequisite in this case is that a certificate must have been configured. Regardless of the EAP configuration, EAP with certificate is always used here.

### Certificate Verification for HTTP Authentication with Script

From this point on incoming certificates can be also be verified with HTTP authentication. For this the variable CACERTDIR must have been set in the script. In addition WEB server certificate content can also be verified. Additional variables are available in this regard:  
CACERTVERIFY\_SUBJECT : Checks the content of the subject (e.g. cn=WEB Server 1)  
CACERTVERIFY\_ISSUER : Checks the content of the issuer  
CACERTVERIFY\_FINGERPRINT : Checks the MD5 fingerprint of the issuer certificate

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

## NCP Secure Entry Client (WIN 32/64)

### Extension of IPSec Hash Algorithms

The algorithms SHA 256, SHA 384, and SHA 512 bit can be used for authentication for both the IKE policies as well as for the IPSec policies. You can make this setting in the Monitor menu under:

IPSec / ...Policies / Recommendations / Authentication

### Application Execution for specific Phonebook Entry

Programs can be entered in the configuration menu of the monitor under "Connection control / Ext. Applications" that will be started automatically after the connection is setup. In addition these applications that will be executed can also be linked to a specific phonebook entry. The dialog from which the available destinations can be selected has a combo box.

### Hotspot Logon

Hotspot logon is executed via the Monitor menu "Connection / Hotspot Logon". After this menu option has been selected different connection messages will be displayed on the screen:

- If the user is already connected to the Internet he will be connected with the start page <http://www.ncp-e.com>. A window with the following message will appear: "You are already connected to the Internet. Hotspot logon is not necessary or has already been executed." This text can be changed by the administrator by entering the address of a different HTML start page in the form "<http://www.mycompagnie.de/error.html>". And the text of error.html is changed accordingly.
- If the user is not yet logged on, then a window will be displayed requesting the user to enter user ID and password for logon to the hotspot operator.
- If the user has not reached a website, then the Microsoft error message "...not found" will be displayed.

### A Project Logo can be added in the Client

The logo is displayed in a panel of the Client over the entire width of the

Monitor at the very bottom. An ini file (ProjectLogo.ini) must be created for

the logo, where the following can be entered:

- Project logo for small fonts
- Project logo for large fonts
- Info text (ToolTip) if the cursor is positioned on the logo
- HTML file if there is mouse click on the logo.

For the installation a "ProjectLogo.ini" is copied into the installation directory that contains further explanations for creating the logo.



### Available Connection Types

In the monitor menu under "Connection" an information window can be opened for the available connection types. This window is used exclusively for user information about available connection types and the connection type that is currently being used.

## NCP Secure Entry Client (WIN 32/64)

If different connection types are used in alternation, then the Client automatically detects which connection types are currently available and selects the fastest of these. The available connection types are indicated by a yellow traffic light, the selected connection type is indicated by a green traffic light.

Use the checkbox to specify that this window will be automatically displayed if the connection setup fails. The window will then also be displayed on the screen, if the Client Monitor is minimized. The error will be identified after the media type used. Note the "Destination System" parameter field in the phonebook for the configuration.

### **New features of version 8.3 relative to version 8.2/8.1**

---

#### **Integrated WLAN Configuration**

Under Windows 2000/XP the WLAN adapter can be operated with the connection type "WLAN". In the monitor menu the special "WLAN settings" menu item is displayed where the access data for the wireless network can be saved in a profile. Installation of the management software is not necessary.

#### **Automatic Media Detection (p)**

On the basis of a pre-configured destination system, those connection types that are currently available for the Client PC are detected and implemented, and if multiple alternative transmission paths are available, the fastest will be selected automatically. The connection type priority is specified in the following sequence in a search routine: 1. LAN, 2. WLAN, 3. DSL, 4. UMTS/GPRS, 5. ISDN, 6. MODEM.

The configuration is executed in the Phonebook with the connection type "Automatic media detection" under "Destination system". If desired, all destination systems for the VPN gateway that are pre-configured for this Client PC can be assigned to this automatic media detection. This renders manual selection of a medium (UMTS, DSL, ISDN, MODEM) from the Phonebook entries superfluous. Input data for the connection to the ISP are transferred from the available Phonebook entries in a manner that is transparent for the user.

#### **Friendly Net Detection (FND)**

FND enables the NCP Client to automatically detect whether it is in a Friendly Net (FN) or not.

Integrated intelligent automation mechanisms in the Personal Firewall automatically replace manual interventions. The administrator can define what constitutes an FN in the Firewall settings of the Monitor. The monitor indicates the presence of a FN by displaying the Firewall Icon in green.

A Friendly Net Detection Server (FNDS) is required; this is an NCP software component that must be installed in a network that is defined as "Friendly Net". The FNDS is authenticated via EAP or EAP-TLS.

The user does not have to worry about setting the Personal Firewall. The NCP Client dynamically accesses a suitable firewall policy depending on the communication

## NCP Secure Entry Client (WIN 32/64)

environment. Unintentional use of incorrect firewall configurations, and thus attacks on the corporate network are prevented. To increase redundancy the IP address of a second FND server can be entered after the first IP address, after a comma.

The IP address of the first available FND server will be selected automatically for friendly net detection.

### **The Range of supported Smart Cards has been extended**

The following smart cards are supported directly via the PC/SC or CT-API interface:

- Signtrust
- NetKey 2000
- TC Trust (CardOS M4)
- Telesec PKS SigG

### **External Applications**

Use this connection management configuration field in the monitor menu to start applications or batch files, depending on the Client Monitor.

In a more extensive configuration you can determine when the application will be started:

- Prior to starting the connection setup (precon)
- After starting the connection setup (postcon)
- After starting the connection disconnect(discon)

The wait function "Wait until application has been executed and ended" can be relevant if a series of batch files will be executed one after the other.

### **New Parameter Field in the Phonebook "Authentication before VPN"**

This parameter field only appears if the connection type "LAN" or "WLAN" has been configured for the destination system, or if an external dialer is used, or if the destination system has been configured for automatic media detection. Please read the description of the "Destination / connection type" parameter field, for more information in this regard.

### **New Parameter Field in the Phonebook "HTTP Authentication" (p)**

HTTP authentication allows automatic, script-driven logon for mobile users at hotspots (DSL as well).

For a link with the connection type WLAN the HTTP logon is not switched on in the phonebook! Instead, activation of this function causes the authentication data from the WLAN settings in the Monitor menu to be used for this destination system. If the access point executes an HTTP redirect, then user name and password entry is not necessary in a browser window. Instead the authentication data are entered here.

Authentication is executed via an appropriate script. Examples are in the installation directory <system root> ncp\scripts\sample.

## NCP Secure Entry Client (WIN 32/64)

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

The user sets up the connection to the hotspot automatically if the HTTP application is activated. A message box informs the user that there are charges for this connection and that he accepts the contract conditions of the hotspot operator.

### **Support for UDP Encapsulation (Port 4500)**

If UDP encapsulation is used then the port can be freely selected. Standard for IPsec with UDP is port 4500, for IPsec without UDP port 500. The NCP Gateway detects the UDP encapsulation automatically.

### **Voice over IP (VoIP) setting priorities**

If the Client is used for communication with Voice over IP, then this function "Voice over IP (VoIP) setting priorities" (in the phonebook under "Line Management") should be activated in order to send and receive the voice data without delay and without distortion.

### **Support of multi-function cards for UMTS/GPRS**

If a multi-function card for UMTS/GPRS is installed, then an additional field appears with the connection type "GPRS/UMTS". This field shows field strength, connection type (UMTS or GPRS), and the network. In addition, the current connection type can be switched and the network can be changed.

### **Log file for a multi-function card**

If a multi-function card for UMTS/GPRS is installed, then a log file is written in the log directory of the Secure Client, with the following columns.

- 1st Column: Time
- 2nd Column: Current field strength
- 3rd Column: Average field strength of the last minute
- 4th Column: Average field strength of the last 5 minutes
- 5th Column: Average field strength of the last 10 minutes
- 6th Column: Current network type (UMTS or GPRS)
- 7th Column: Current network

An entry is created every 10 seconds; however the entries are only written to the file every 5 minutes. A log file is created with the name "mfc<DATE>.log" for each day. The log files for the last 7 days are saved.

### **Log entry when setting up a connection (reason for the set-up)**

If an existing connection is disconnected, then the system writes a log entry in the Client's logbook citing the reason why the connection was disconnected.

### **Log entry when disconnecting a connection (field strength status)**

If an existing connection is disconnected, then the system writes a log entry in the Client's logbook citing the last field strength status values for UMTS/GPRS.

## NCP Secure Entry Client (WIN 32/64)

### Firewall

The Personal Firewall can be set in the "Configuration" monitor menu, and it is a fixed component of the Secure Client. All firewall mechanisms are optimized for Remote Access applications and are activated when the computer is started. This means that in contrast to VPN solutions with autonomous firewall, the teleworkstation is already protected against attacks before actual VPN utilization. The Personal Firewall also offers complete protection of the end device, even if the client software is deactivated. All firewall rules can be centrally specified by the administrator, and compliance with these rules can be forced. The prerequisite in this case is the central NCP Secure Enterprise Management system, which is used to configure the Client, which can be permanently specified as unchangeable for the user.

### Automatic hotspot logon

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

Functional description:

If a user with his end device is in receiving range of a public WLAN, then he selects the menu option "Hotspot Logon". The Client then searches the hotspot automatically and opens the website for the logon procedure in the standard browser. After successfully entering the access data and release by the operator, the VPN connection can be established to corporate headquarters, for instance, and the user can securely communicate, as he would on an office workstation. To keep the PC invulnerable at all times when logging onto the WLAN, the firewall dynamically releases the ports for http or https for logon or logoff. Logoff at the hot spot free. In this process data traffic is only possible with the hotspot server of the operator. Non-requested data packets are rejected. In this manner the system guarantees that a public WLAN will only be used for the VPN connection to the central data network and that there is no direct Internet access.

Direct communication to the Internet bypassing the VPN tunnel is impossible due to the previously described dynamic firewall rules that are set automatically by the integrated Personal Firewall of the NCP Secure Client. Please note: proxy settings that may have been entered must be adapted or deactivated for logon via the standard browser at the hotspot.

If hotspot logon has not been executed by the NCP Secure Client then this fact is communicated to the user through the message "Hotspot could not be found". In such a case you must determine whether a general problem exists in conjunction with the mechanisms implemented by NCP relative to this hotspot operator.

### Compression type Deflate

The compression type Deflate is now supported. In the phonebook the parameter "Use IP compression" under "IPSec Settings" is displayed. Using this function both methods, LZS and Deflate, are negotiated.

**In the phonebook under "IP Address assignment" you enter the domain name.**

## NCP Secure Entry Client (WIN 32/64)

### **Using multiple Soft Certificates on one Client PC**

If you want to set up PC-sharing for multiple users, who each use a separate certificate, then you can configure this in the main menu of the Client Monitor under "Configuration - Certificates - User Certificate".

Under "User Certificate" you must switch on the "Activate Soft Certificate Selection" menu item, and you must select a "Certificate Path". If this path has been created previously, then you can select this path via the Select button. (C:\WINNT\ncple\usercert, for example). The various user certificates must then be created under this path. If these settings are saved with "OK", then the certificate list will appear under the graphic field of the monitor, with the list of all user certificates saved under the certificate path (for instance user1 to user4). If the user has selected his soft certificate (user2 for instance) and has established a connection to the central VPN gateway, then he must first enter his PIN. Then the connection to the destination system will be established.

### **Using EAP 802.1x**

For WLAN and switches supporting port authentication the client supports EAP-MD5/TLS. This makes it unnecessary to install a separate EAP client. EAP-MD5: UserId/Password authentication is supported and the possibility exists to get the UserId/Password from the certificate used for the VPN connections. EAP-TLS: Certificates are used and are taken from the NCP certificate configuration. EAPOL KEY (Dynamic WEP key ) is supported.

### **Statefull Packet Inspection**

Stateful Packet Inspection is always activated. This means, for non-VPN connections to provider SPI (Statefull Packet Inspection) is now always enabled.

### **XAUTH protocol**

Changed the XAUTH protocol for use with NETSCREEN and OTP.

(p) = to be purchased