

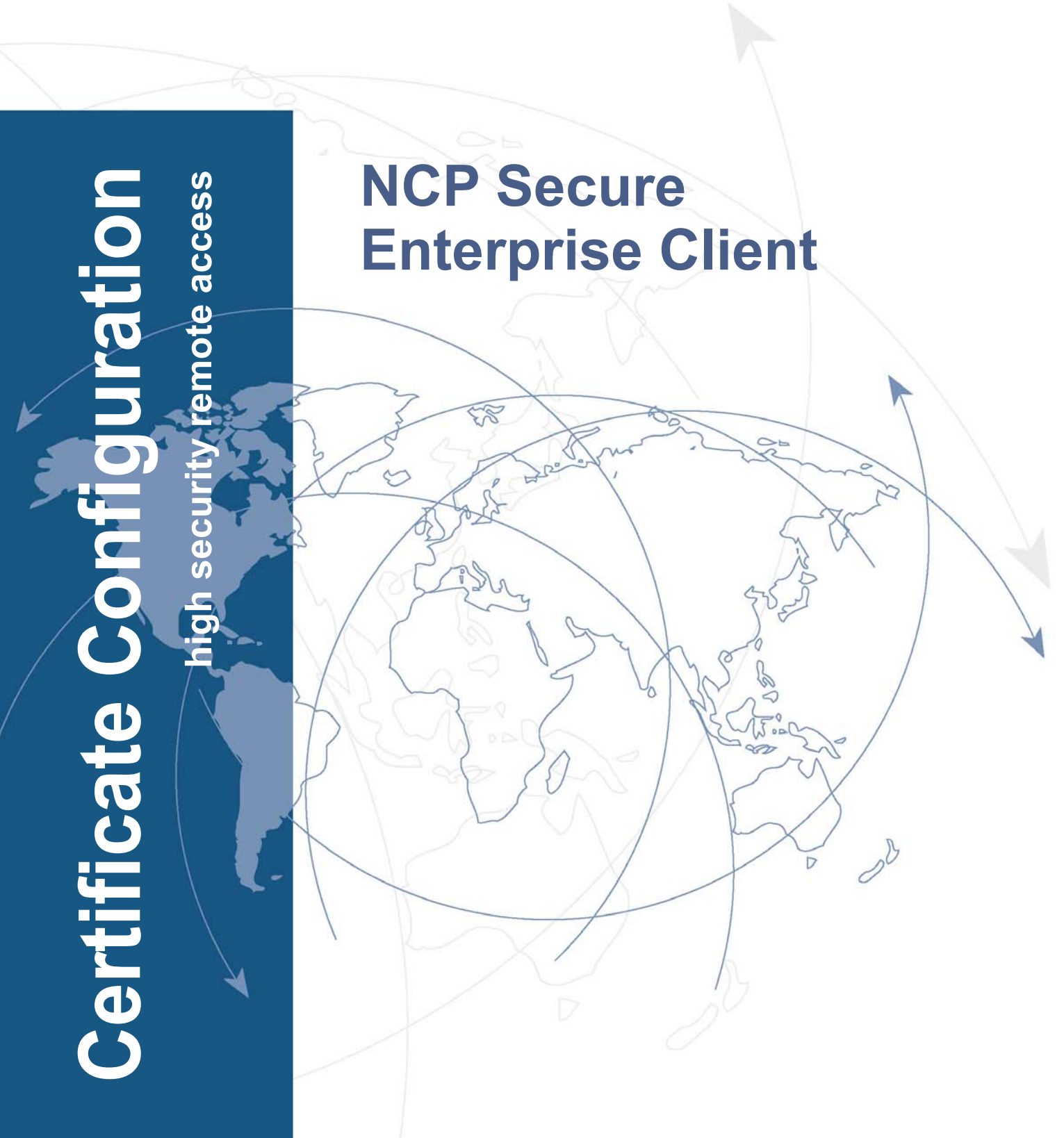


SECURE COMMUNICATIONS

# Certificate Configuration

high security remote access

## NCP Secure Enterprise Client





# **Certificates**

## **used by the Secure Enterprise Client**

## Support

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

### Fax Hotline Number

+49 (911) 99 68 458

### Internet Mail Address

support@ncp-e.com

When contacting NCP with your problems or queries please include the following information:

- exact product name
- serial number
- Version number
- Accurate description of your problem
- Any error message(s)

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



Network  
Communications  
Products engineering GmbH

USA:

NCP engineering, Inc.  
444 Castro Street, Suite 711  
Mountain View, CA 94041  
Tel.: +1 (650) 316-6273  
Fax: +1 (650) 251-4155

Germany:

NCP engineering GmbH  
Dombuehler Str. 2  
D-90449 Nuremberg  
Tel.: +49 (911) 9968-0  
Fax: +49 (911) 9968-299

## Copyright

*Considerable care has been taken in the preparation and publication of this manual, errors in content, typographical or otherwise may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP as desired.*

*NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or use for any particular purpose. Furthermore NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes.*

*This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH, Dombuehler Str. 2, D - 90449 Nuremberg, Germany.*

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

© NCP engineering, February 2013

<b>Certificates at the Secure Client</b>	<b>5</b>
Soft Certificates and Chipcards	6
Interfaces and Formats of the Client	6
Certificates for Authentication	6
Safeguarding PIN Use	6
CA Certificates	7
Use of a Revocation List (CRL)	7
Certificate Configuration	7
Certificate Distribution with the Secure Enterprise Management (SEM)	8
Usage of Certificates	8
<b>Manual Configuration</b>	<b>9</b>
Multi Certificate Configuration	9
<b>Certificate Configuration</b>	<b>10</b>
User Certificate	10
Certificate from Smartcard Reader	11
Certificate from PKCS#12 File	12
Certificate from CSP	13
Certificate from CSP User Certificate Store	13
Certificate from PKCS#11 Module	13
Entrust-Profile	13
PIN Policy	14
Certificate Renewal	14
Hardware Certificate	15
<b>View Certificates</b>	<b>16</b>
Display of Extensions for Incoming Certificates and CA Certificate	18
<b>PIN Entry</b>	<b>20</b>
Safeguarding PIN Use	20
<b>PC-Sharing (Using multiple Soft Certificates on one Client PC)</b>	<b>22</b>
Accounting on the VPN Gateway	23

# Certificates at the Enterprise Client

This document describes how to store issuer- and user certificates at the client, how to configure them according to their purposes with the client monitor and shows the analysis of certificates by the client.

---

## Overview of Contents

- Certificates at the Secure Client
- Manual Configuration
- Certificate Configuration
- User-Certificate
- Entrust Profile
- PIN Policy
- Certificate Renewal
- Hardware Certificate
- View Certificates
- PIN Entry
- PC Sharing  
(Using multiple Soft Certificates on one Client PC)



Further descriptions to a corporate network with public key infrastructure as well as certificate rollout and updating certificates you will find in the document **Secure Enterprise Management** (PKI Plug-in).



The easiest way to receive the desired information is via the **Secure Suite Navigation**. All available documents about your product are recorded in this pdf file.

Starting from navigator, you can jump directly into all relevant documents and download them from the NCP homepage in case they are not yet saved in your navigator directory.

## Soft Certificates and Chipcards

Certificates are created by a CA (Certification Authority) utilizing a PKI-based architecture. They may be created as soft certificate or implemented on a chipcard or USB Token. How to create certificates with the **Secure Enterprise Management** is described in the document about the PKI plug-in. In principle certificates with a private key up to a length of 4096 bits can be implemented with the Secure Client.

## Interfaces and Formats of the Client

The Secure Client can be used in public key infrastructures as of **X.509. V.3** standard. Additionally the Entrust Ready functionality has been granted for the Enterprise version. Thus the client supports all the important guidelines from Entrust relative to the implementation of certificates and their use. (See the description **Entrust Ready**).



The Secure Client supports the following interfaces/formats:

- Smartcards, USB-Tokens: PKCS#11, TCOS 1.2 and 2.0, CSP
- Soft Certificates: **PKCS#12-File**
- PC/SC conform **Chipcard Reader**: The client software supports all chip card readers which conform with PC/SC. The chip card readers are included in a list of the client once the reader is connected and the corresponding driver software has been installed.
- **Automatic Recognition of connected PC/SC Readers**: If the use of a PC/SC chip card reader is configured on the client for the PKI environment, the client recognizes and automatically uses the connected one.

This automatically simplifies profile creation within the Enterprise Management System, since no user specific chip card readers have to pre-configured in the central certificate configuration.

If a user receives a configuration without entry for the chip card reader from the Management System and if a certificate is pre-configured, then the client automatically reads the data of the PC/SC reader which is installed on the user PC and uses this reader.

This feature can only be used in connection with smartcards which can be addressed directly without interface software such as NetKey chip cards (Telesec).

- **PKCS#11 Module**: 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 relevant PKCS#11 module can be selected via an assistant.

Additionally the Secure Client supports the following features :

- Automatic Download of the Revocation List of a CA (Certification Authority): The client supports the **Certificate Extension CDP** (Certificate Distribution Point), which initiates an automatic download of the CRL. After the download the incoming certificates will be checked whether they are listed in the CRL.
- **PIN Policy**: The administrator can specify PIN guidelines that must be complied with during PIN entry or PIN modification. The guidelines selected here appear as a list of conditions that must be complied with when changing the PIN
- **Certificate Check**: You can specify per link profile which entries must exist in a certificate from the remote side before the connection will be established.
- **Certificate Renewal**: The administrator can specify whether a message is given out that warns of the expiration of validity, and he can specify how many days before the certificate validity expires this message should go out. Using the Enterprise Client the renewal of a certificate can be executed automatically with a **certificate update**.

## Certificates for Authentication

In order to use certificates for authentication with IPsec connections, no pre-shared key must be entered in the configuration of the IKE policy. Only in this way certificate based proposals with RSA signature can be sent to the remote side. (This setting can be configured at the Enterprise Client under **Security**, at the Entry Client under **IPsec Settings**.) Default setting for IPsec connections is **automatic Mode**, otherwise the encryption for IPsec connections is defined in the **IPsec Configuration**.

Using **L2Sec Connections** with the Enterprise Client the encryption method is defined in the configuration folder “Security” bestimmt.

## Safeguarding PIN Use

In order to use a certificate you must enter a PIN. For this **PIN Entry** and for the period of validity special security policies have been implemented. E.g. the **PIN State** is displayed in the monitor of the client. The PIN can be reset manually via the monitor menu or automatically after removing the chipcard. The system monitors whether the PKCS#12 file is present. If, for example, this file is stored on USB

stick or an SD card, then after pulling out the SD card the PIN is reset and an existing connection is disconnected. This process corresponds to the **Connection disconnect when smart card is removed**, which can be set when using a smart card, under “Configuration / Certificates” in the monitor menu. If the SD card is later reinserted the connection can be restored after another PIN entry.

## CA Certificates

The administrator of the corporate network specifies which certificate issuers can be trusted. This is done by copying the CA certificates of his choice into the installation directory under <CACERTS>. 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. Please note to this the description to the extended installation in the document **Enterprise Installation Description**.

Retrospectively, issuer certificates can be distributed automatically via the **Secure Management Server** (only to Enterprise Clients) or the user can save them himself as long as he has the relevant write permissions in the relevant directory.

Currently the formats \*.pem and \*.cert are supported for issuer certificates. They can be viewed in the monitor under the menu item “Connection / Certificates / **Display CA Certificates**”.

If the secure client receives the certificate of a remote station, then the NCP client will determine the issuer by searching the issuer certificate initially on smartcard or USB token or in the PKCS#12 file and finally in the installation directory under <CACERTS>. If the issuer certificate cannot be found then the connection will not be successful. If no issuer certificates are available, then no connection is allowed.

If soft certificates are created with the PKI plug-in of the Management Server then the issuer certificate is saved in the PKCS#12 file.

## Use of a Revocation List (CRL)

The secure client can have access to the corresponding CRL (certificate revocation list) for each issuer certificate. It is applied to the installation directory under <CRLS>. If a CRL is available, then the secure client checks incoming certificates against the CRL. The client downloads the corresponding CRL automatically if the incoming server user certificate includes the **Certificate Extension CDP**.

If revocation lists are used, then *usually there is no notification if the client has no saved CRL for incoming certificates*. If a notification is required in such cases then the file NCPPKI.CONF needs to be edited. It is saved in the installation directory. The standard entry in the section [General] is:

```
Enablecrlinfo = 0
```

This means that no notifications are displayed if, on the client at the remote station, no black list was found for the certificate. If a notification has to be displayed, then this setting has to be changed to:

```
Enablecrlinfo = 1
```

## Certificate Configuration

A number of individual certificate settings may be saved as **Multi Certificate Configuration** 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.

The certificate configuration of a client older than version 9.1 will, in case of an update to this version, automatically be converted to the **Standard Certificate Configuration**. The standard certificate configuration is set up after an initial installation of version 9.1.

A special function for **Certificate Selection** enables **PC-Sharing** for multiple users, who each use a separate certificate.

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



## Care of Certificates and the associated Private Keys

It is vital that each Certificate and the associated private key remain secret. The Certificate must not be copied from the device or file on which it was originally created.

If there is cause to believe that a Certificate or the associated private key has been compromised, the CA which issued the Certificate must be informed immediately. The Certificate in question must be revoked, its associated private key deleted and a new Certificate and private key generated.





## Certificate Distribution with the Secure Enterprise Management (SEM)

User certificates and hardware certificates can be distributed via the CMP protocol (Certificate Management). This type of certificate distribution is only possible with Secure Enterprise Management. In addition, Port 829 (TCP) is required between Update Client and Management Server. The PIN for the VPN certificate is requested before saving the PKCS#12 file. With the hardware certificate this is automatically determined by the hardware.

Hardware certificates can be distributed automatically by the Secure Enterprise Management via the CMP (Certificate Management Protocol). The first-time download is only possible for the first dial-in with an **Init User**. In the certificate configuration of the Init user, a name for the PKCS#12 file must be specified prior to downloading a file, even if this file is not yet present. If no certificate configuration is defined, then no certificate will be downloaded.

After establishing the connection to the Management Server and after entering user name and authentication code the hardware certificate will be downloaded and stored in the defined folder. After the download the certificate can be displayed in the client monitor under the menu item “Connection / Certificates / **Hardware Certificate**”.

## Usage of Certificates

The usage of a certificate can be defined when creating it at the SEM as **VPN Certificate** (user certificate) or **Hardware Certificate**. The created certificates can be stored directly in the Management Server’s database.

Assignment of the certificate to the respective user is unique with the **VPN User ID** from certificate. For example this ID can be comprised of the common name or the e-mail name of the certificate and a suffix. The suffix can be used if there are names that are the same, or to distinguish group membership.

This VPN User ID must agree with the entry in the client software (see **VPN Tunneling**). This entry is entered in the client configuration of the SEM under configuration update as “ID for personalized phonebook” (**RSU-ID**), and it is transmitted with the PIN letter to the initial user.



## Multi Certificate Configuration



The default path of soft certificates is the installation directory of the client software. This is also the default path of soft certificates which are will be downloaded from the Management Server during a rollout or a certificate update. In the installation directory always exist test certificates for users (Client1.p12 up to Client4.p12) as well as a CA certificate for test purposes (NCPSupportCA.pem).

The default path for certificates, specially for certificates stored on tokens or smartcards, can be modified by using the system variables (of the SEM) or by entering path and filename manually.

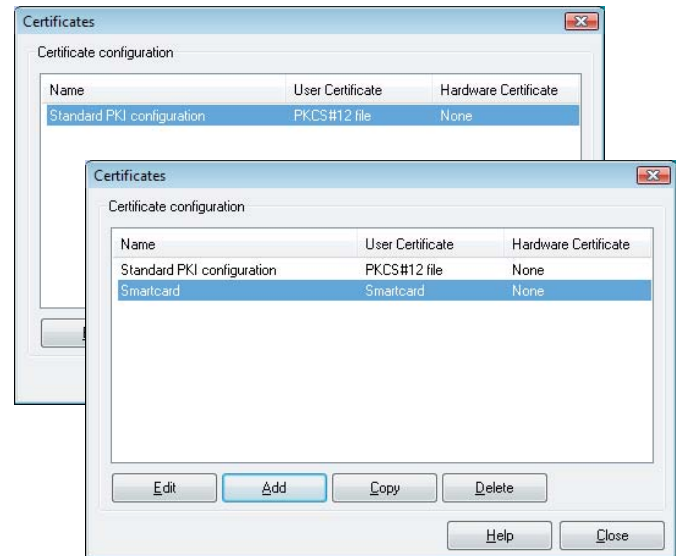
## Manual Configuration



At the Secure Client the manual certificate configuration takes place basically in the same way as in the configuration plug-in of the Enterprise Management under “PKI Configuration” in the client template. In this template multiple different certificate configurations can be stored. (Requirement: SEM versions  $\geq$  2.02 and Client versions  $\geq$  9.10.)

After selecting the menu item “Certificates” in the configuration menu of the client monitor you can store multiple different certificate configurations in the same way (illustration above). In principle multiple certificate configurations can be stored which are each identified by their own name

After selecting “Certificates” a standard PKI configuration will be displayed (illustration below). Pressing one of the buttons “Add” or “Edit” you can add a new certificate configuration under a new name (below “Smartcard”) or modify an existing entry (see next



page).

### Name and “Standard PKI Configuration”

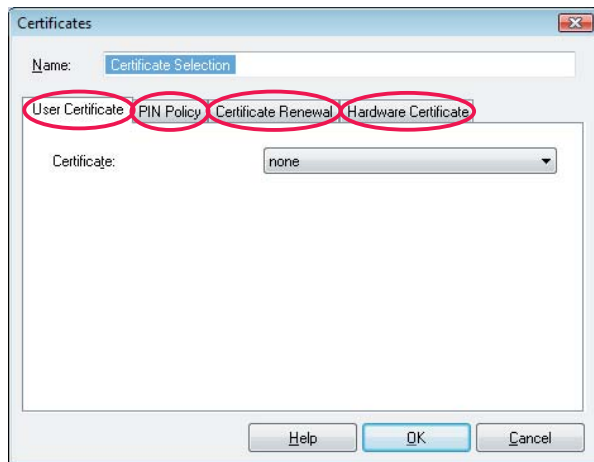
The certificate configuration of a client older than version 9.1 will, in case of an update to this version, automatically be converted to the standard PKI configuration. The standard PKI configuration is set up after an initial installation of version 9.1.

Per profile you can select one of the different certificate configurations. 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.



In the configuration folder **Security** a certificate of this certificate configuration can be selected for the encryption and the authentication in the **Security Mode L2Sec** or in the **Security Mode IPsec** for the **extended Authentication** (XAUTH).

## Certificate Configuration



After pressing the “Edit” button or the “Add” button you can modify the Standard PKI Configuration and store the certificate configuration with a new name.

This is where it is specified if certificates are to be used to authenticate the client and where the **User Certificates** are saved.

In other configuration fields, the **PIN Policy** for entering PINs is specified and the time interval is set within which the certificate will expire or a certificate extension needs to be requested (**Certificate Renewal**.)

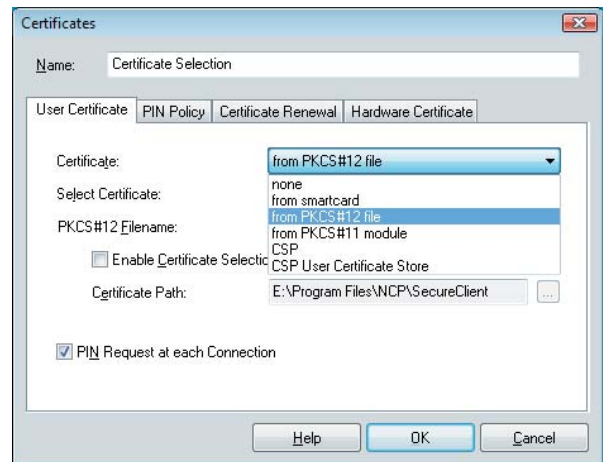
Additionally a **Hardware Certificate** can be configured.

### Entrust Profile



Please note the document **Entrust Ready Functionality** and “Load Entrust Profile” below.

## User Certificate



### none

The default value is “None”, indicating that no certificates will be used.

### from smartcard

In order to use smartcard based certificates select “from smartcard” and then select the smartcard reader from the list of supported smartcard readers.

### from PKCS#12 file

Select “from PKCS#12 file” from the listbox in order to use a soft certificate which is stored on the harddisk of your PC.

### from PKCS#11 module

Select “PKCS#11 module” from the list in order for the respective certificate to be read via a PKCS#11 module from a smartcard in a smartcard reader or from a Token.

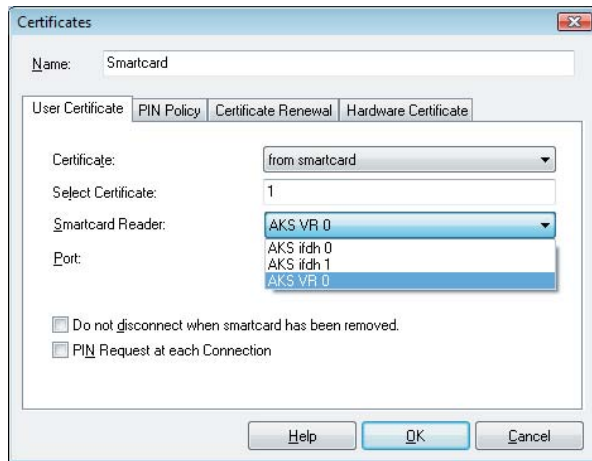
### CSP

By choosing this as the certificate as source, the certificate of a smartcard or a token will be accessed by the Windows CSP (Certificate Service Provider), if the respective interface has been installed and registered.

### CSP User Certificate Store

If you select the “CSP user certificate store” from the listbox, the certificate from the CSP user certificate store is used for extended authentication. Please enter the certificates “Subject CN” and “Issuer CN” in the respective fields.

## Certificate from Smartcard Reader



In order to use certificates from the smartcard select the appropriate Smart Card reader from the list of supported smartcard readers. (See also: Enter PIN).

### Certificate from Smartcard Reader

The client software supports all smartcard readers that adhere to the PC/SC standard and detects the smartcard reader automatically after the PC has been booted.

The PC/SC interface is only opened for a connection setup in which a smart card access occurs. This means that now other applications can also open the PC/SC interface in “exclusive” mode.

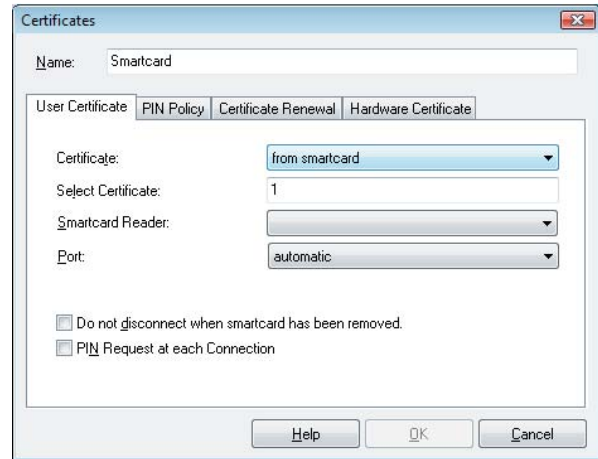


Note: If use of a certificate is configured on the client for the PKI environment, then the client automatically detects and uses the connected PC/SC card reader. Thanks to this automated mechanism creation of profiles with the Enterprise Management is facilitated, because it is no longer necessary to pre-configure user-specific smartcard readers in the central certificate configuration, rather this entry can remain empty on the Management Console if the users implement different PC/SC card readers.

*If the user receives a profile setting from the Management System without entry for a smartcard reader, and if a certificate is preconfigured, then the client will automatically read the data of the PC/SC reader that is installed on the user PC, and it will use this reader.*

*This feature can only be used in conjunction with smartcards that can be addressed directly without interface software (e.g. TCOS, NetKey from Telesec, and TC Trust).*

## Smartcard Reader



If the chipcard reader is to be installed after the client, the client detects the chipcard reader only after booting (illustration above). After that the installed reader can be selected.

### Certificate Selection

#### 1. Certificate ...4.

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

On the Smart Cards of Signtrust and NetKey 2000 there are located three certificates:

- (1) for signification
- (2) for encryption and decryption
- (3) for authentication (NetKey 2000 option)

### Port

If you have selected above “from smartcard” then the port for the smartcard reader must be entered here.

#### automatic

If the card reader has been correctly installed then the port will be determined automatically.

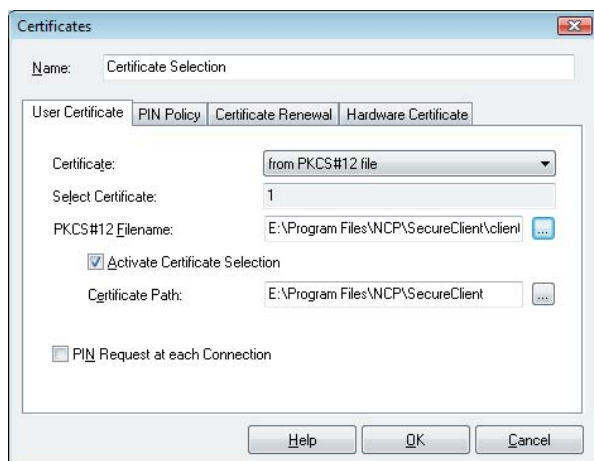
#### COM1 ... COM4 :

If there is no agreement then COM ports 1-4 can be directly allocated.

### Disconnect when Smartcard is removed

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

## Certificate from PKCS#12 File



### PKCS#12 Filename

If you are using the PKCS#12 format, then you will receive a DLL from your smartcard 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, you can choose the file after pushing the [...] button (select button).

Important: The strings of the filename can be entered with variables. This simplifies the handling of the configuration files by the client plug-in of the SEM, because the same strings with environment variables can be entered for all users. Example:

```
%SYSTEMROOT% > Windows Directory (c:\Windows)
%INSTALLDIR% > NCP Installation Directory (c:\Programs\NCP\SecureClient)
%PROGDIR% > Windows Programs (c:\Programs)
%windir% > C:\Windows
%NCPUSERDIR% > This variable for the configuration of the P12 file substitutes the user directory
(e. g. C:\Documents and Settings\UserXY). In this way the current Windows user can logon with his certificate data at the VPN gateway with this certificate configuration. (This function is not supported by the NCP GINA).
```

### Aktiviere Certificate Selection



This function is needed only for PC-sharing, when multiple users of the PC work with different soft certificates. Please note the section **Using multiple Soft Certificates on one Client PC** in this document.

When using soft certificates the certificate path for the PKCS# 12 files can be specified after "Certificate Selection" has been activated. Under the graphic field of the monitor the system will display a selection field with all soft certificates under the specified directory (see **Client Monitor**). If a soft certificate is selected, then the configuration that belongs to this certificate becomes active, and accordingly the connection is disconnected and the PIN is reset. In addition the PIN can be reset via



the "Logout" button and via the "Reset PIN" menu item, for example, when the user leaves the workplace.

### Certificate Path

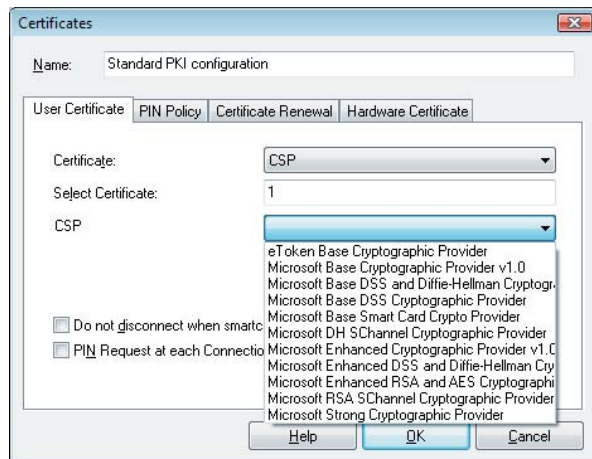
The Certificate Path is needed only for PC-sharing.

### PIN Request at each Connection

Here you can specify that the PIN must be entered correctly, not only after each initial connection establishment after booting the PC, but rather before any connection establishment. This functionality, which can be used for all connection modes, (manual, automatic, alternating), requires the monitor to be started. However the monitor may be minimized.

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.

## Certificate from CSP



By choosing this as the certificate as source, the certificate of a smart card or a token will be accessed by the Windows CSP (Certificate Service Provider), if the respective interface has been installed and registered.

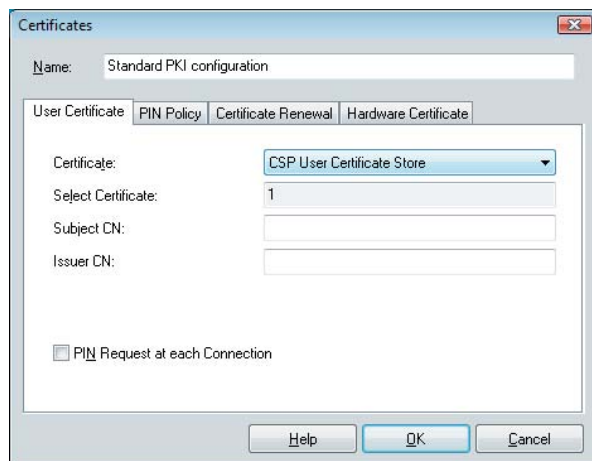


If the certificate number “0” is configured, the first certificate with the extension “SSL Client Authentication” which will be found is to be used.



Note: Access to the Windows User Certificate Store is currently not supported.

## Certificate from CSP User Certificate Store

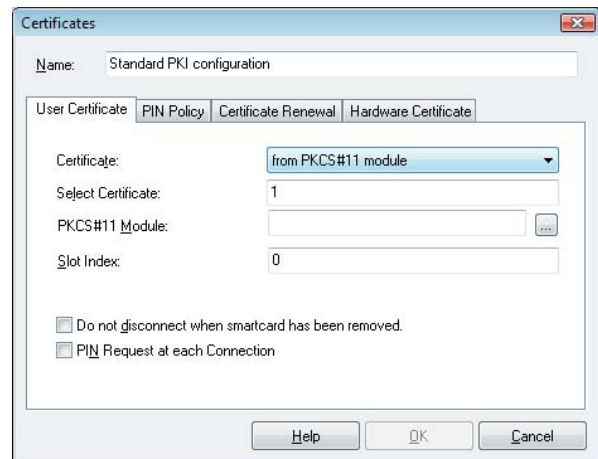


If you select the “CSP user certificate store” from the listbox, the certificate from the CSP user certificate store is used for extended authentication. Please enter the certificates “Subject CN” and “Issuer CN” in the respective fields.



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

## Certificate from 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.

You can use an assistant to search for installed PKCS#11 modules and then select the desired module with the associated slot. For this click the button “PKCS#11-Module”. Click on the search button (illustration above) in the line of the PKCS#11 module.

## Entrust Profile



Please note the document **Entrust Ready Functionality** and “Load Entrust Profile” below.

The NCP Entrust Ready certification has been granted for the NCP Secure Client versions 7.03 and version 7.22.

Select “Entrust Profile” from the listbox and the according certificate will be loaded.

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

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

Please note that the input fields in the Entrust assistant for the profile path and profile name can be preconfigured and blocked via SEM.



## PIN Policy

The administrator (or user) can specify PIN guidelines that must be complied with during PIN entry or PIN modification. The guidelines selected here appear as a list of conditions that must be complied with when changing the PIN (illustration below).

## Certificate Renewal

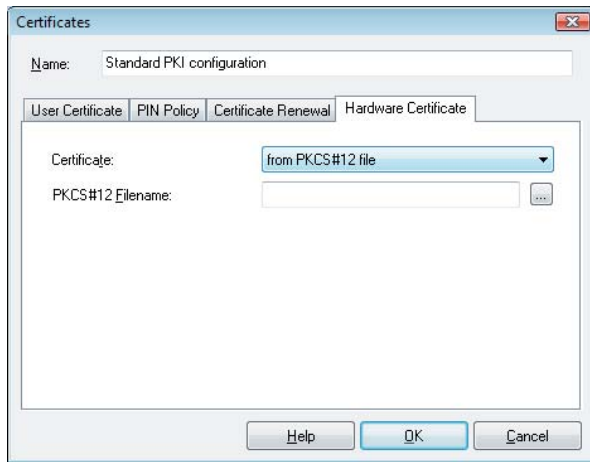
Here you can specify whether a message is given out that warns of the expiration of validity, and you can specify how many days before the certificate validity expires this message should go out. As soon as the set time frame before expiration goes into effect, a message will appear each time a certificate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



### Validity Extension of Soft Certificates via the Enterprise Management

First, in the Client, the PKCS#7 file is saved in the RSUDATA directory. After clearing the connection the system checks whether a PKCS#7 is available for this user. If this is the case, then the old certificate is saved under a new file name, and the new certificate with the new private key is saved in the configured PKCS#12 file, with the entered PIN. The user receives a message that his certificate has been extended. The prerequisite in this case is the PKI Plug-in with the Enterprise Management.

## Hardware Certificate



Additional authentication with a hardware certificate can only be used with IPsec. To activate the function, the option “Hardware Certificate CN” must be switched on under Link Profiles on the Gateway (version 6.02 build 14 or greater). The computer authenticates itself relative to the gateway with a hardware certificate. If the hardware certificate is used in addition to a user certificate, then you can be sure that the user always dials in from the same computer.

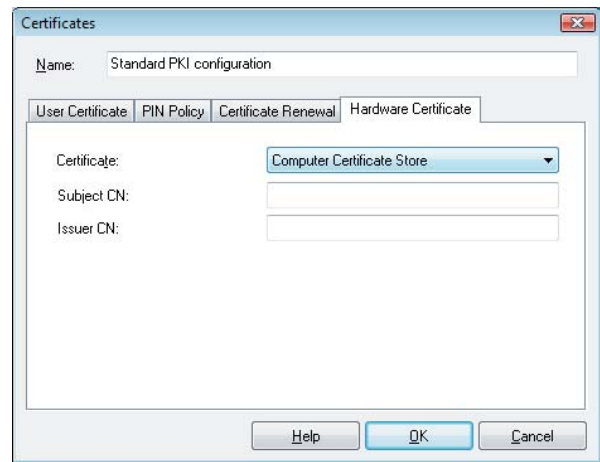
### Certificate from PKCS#12 File

A hardware certificate can be configured as “PKCS#12 file” or “Entrust Profile”, the corresponding name must be entered. The PIN for the hardware certificate is entered automatically in the background, without user intervention. The serial number of the computer or of the hard disk is used as PIN for the certificate.

If an Entrust profile is loaded, then the common name of the certificate must agree with the value of the “WS NAME” system environment variable. Otherwise the Entrust profile will not be loaded. The PIN is assigned automatically when loading the entrust profile.

Listings for the PIN and the environment variables are specified in the “NCPHWINF0.DLL” file. If other specifications are required then this DLL must be modified and replaced. The PIN must be manually assigned for producing a hardware certificate as a PKCS#12 file. The serial number of the computer that is used as PIN, can be read out with the program “HWINF0.EXE”. The PIN must be at least 8 characters and a maximum of 20 characters in length.

## Computer Certificate Store



With this setting, the local Windows Computer Certificate Store can be used for storing certificates. If a certificate has been stored here, which entails that it has been imported into the local Computer Certificate store, it can be used by the client for authentication.



**Note:** Access to the Windows User Certificate Store is currently not supported.



Contrary to the user specific certificates found within the Windows User Certificate Store, which can only be accessed and used after the Windows user login, hardware certificates stored in the Computer Certificate Store can be used immediately after the boot phase (e. g. for domain login).



Once a certificate has been imported, it can not be exported. For this reason one can forgo the necessity of a PIN for this certificate as it can only be accessed in accordance to the security policy. These certificates will also be accessed by services that cannot input PINs.

If a hardware certificate (without PIN) based authentication has been configured correctly, the PIN symbol will show up green on the monitor (see **Client Monitor**).

### Subject CN / Issuer CN

The correct user certificate can be selected from the User Certificate Store by its Common Name and Issuer (Subject CN and Issuer CN).



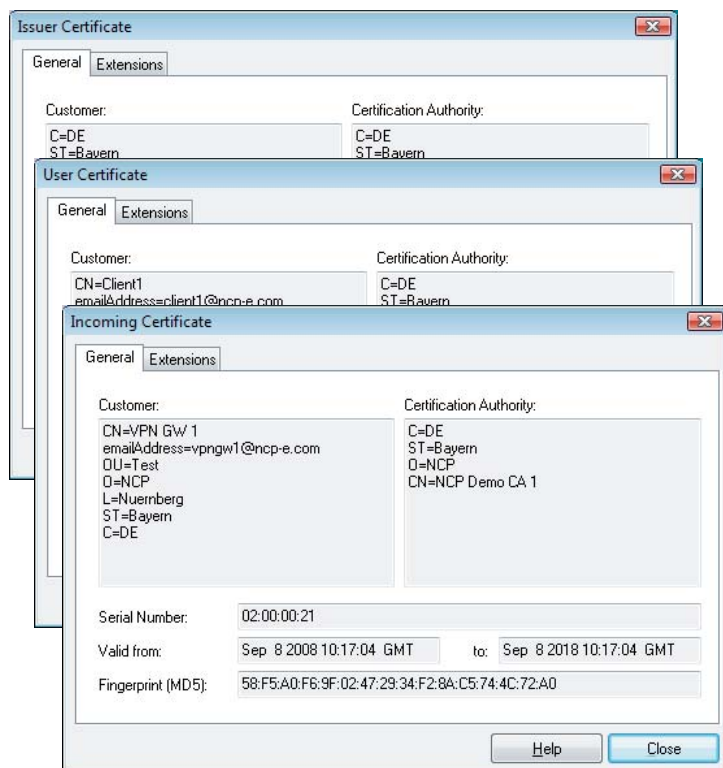
## View Certificates



Viewing an issuer-, user- or hardware certificate, the attributes will be displayed used by creating the certificates, e.g. the distinct e-mail address.

The incoming certificate is transferred with the SSL negotiation from remote site. You can check e.g. whether the displayed issuer is included in your list of CA certificates.

Depending on the certificates which are configured and whether after a established connection a certificate of the remote site has been received already the certificates can be considered via the connection menu of the monitor (illustrations above and below).



### Issuer (CA)

The user and the issuer of a Issuer Certificate are normally identical (self-signed certificate).

The issuer of User Certificate has to be identical with the issuer of the Issuer 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

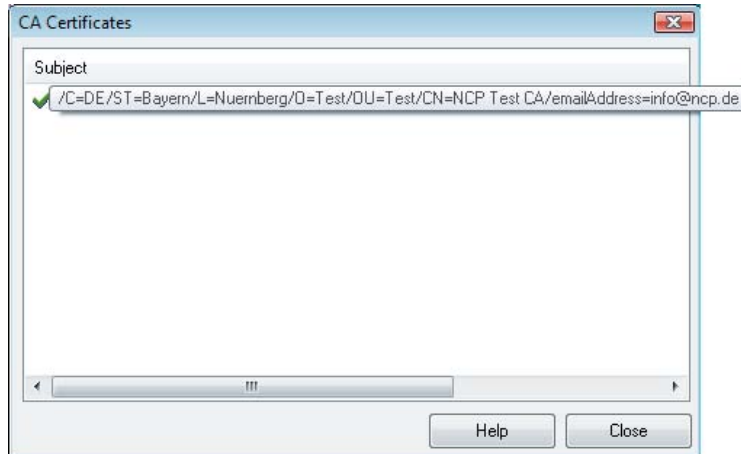
The fingerprint is a hash value. The hash value is the signature of the certificate. The hash value is encrypted with the private key of the CA.



The display fields under "General" are identical for all certificates exceptionally the CA certificate. Therefore these fields are only described at one time.

## Display CA Certificates

Multiple issuer certificates are supported with the client software (multiple CA support). The issuer certificates must be collected in the installation directory under <CACERTS> for this. This is useful when the user certificate of the remote site has been issued by another CA as the user certificate of the client.



Valid CA certificates are marked with a green hook, invalid CA certificates are marked with a red cross (illustration above). By double clicking on a CA certificate all display fields are shown as described on the previous page.

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 installation directory under <CACERTS>. If the issuer certificate is not known, then the connection will not be established (No Root Certificate found, see above **CA Certificates**).



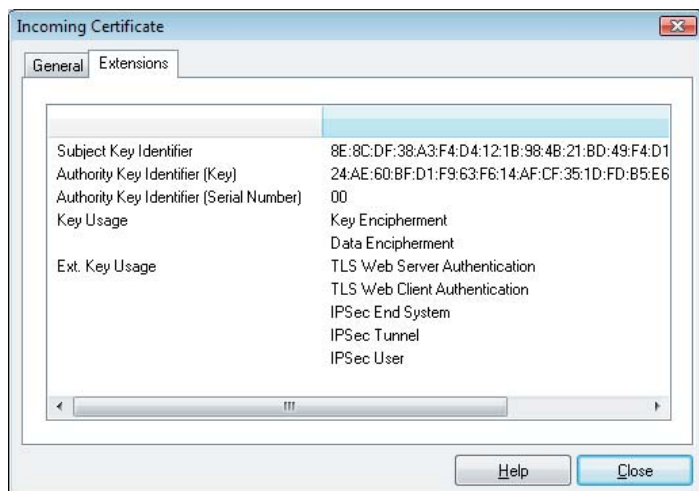
If you want to copy CA certificates to the client please note the description about the extended installation in the documents **Enterprise Client Installation**.

## Display of Extensions for Incoming Certificates and CA Certificate

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. Following extensions are significant for the Secure Client and the Secure Server:

- KeyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- CDP (Certificate Distribution Point)

The CA certificate whose extensions are displayed, has to be opened by a double click in the window of CA certificates (see above). Upon doing so the left window with general information is opened. The window “Extensions” displays the certificate extensions if available. (see illustration below)



### KeyUsage

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted:

- Digital Signature
- Key Encipherment (key transport, key management)
- Key Agreement (key exchange process)

If one of the bits is not set, then the connection will be cleared.

### 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 callback 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 certifica-

tes that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

### CDP (Certificate Distribution Point)

The URL for downloading an CRL is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is setup, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid then, the connection is disconnected. In this process the CRL is stored in the installation directory under <CRLS>, under the common name of the CA.

### CRL and ARL Checks

The Secure Client is capable of checking the following revocation lists:

- Certificate Revocation List (CRL)
- Authority Revocation List (ARL)

CRLs respectively ARLs must be copied in the according subdirectories of the installation directory under <CRLS> and <ARLS>.

The Secure Client can be provided with the associated CRL (Certificate Revocation List) for each issuer certificate. 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).

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.

### HTTP Proxy for CRL Download

A proxy for the CRL download can be configured via HTTP in the NCPPKI.CONF file in the “HttpProxy” group:

```
[HttpProxy]
#ProxyHost = xxx.xxx.xxx.xxx
#IP address of the proxy server for CRL download via
#HTTP ProxyPort = 80
#Port of the proxy server for CRL download via
#HTTP ProxyUser = xyz
#Username of the proxy server for CRL download via
#HTTP ProxyPw = xxxx
#Password of the proxy server for CRL download via HTTP
```

## PIN Entry



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 **PIN Request at each Connection**).

If you have configured the client for the use of a Smart Card or of a PKCS#11 module, 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 (see **Client-Monitor**).

As soon as you wish to establish a connection that requires certificate support, the “Enter PIN” prompt appears – if you have not yet entered the PIN (illustration below).



Using a soft certificate the PIN can have 4 digits. Using a smartcard the PIN must have minimum 6 digits.



Entering an incorrect PIN causes an error message to be displayed after 3 seconds. A connection to the Destination will not be possible. After 3 incorrect entries the PIN will be locked! (This concerns not to soft certificates!) In this case please contact your administrator.



If you remove the smartcard or USB stick with token during a communication session the link will be immediately disconnected when configured (see above **Disconnect when Smartcard is removed**).

## Safeguarding PIN Use

If you activate the function, “PIN request at each connection”, in the certificate configuration, then the PIN can no longer be entered via the “Enter PIN” Monitor menu option. The menu option “Enter PIN” is thus switched to inactive automatically. This ensures that the PIN will only be queried and can only be entered directly before the connection is set-up.

Activate this function to prevent an unauthorized user from setting up an undesired connection if the PIN has already been entered.

Likewise, if the “Change PIN” function has been switched active, then the PIN that has already been requested in other function contexts is no longer used – i.e. when setting up a connection, or in the “Enter PIN” connection menu. Instead you can always select the menu option “Change PIN” and the new PIN will be automatically reset immediately after the change.

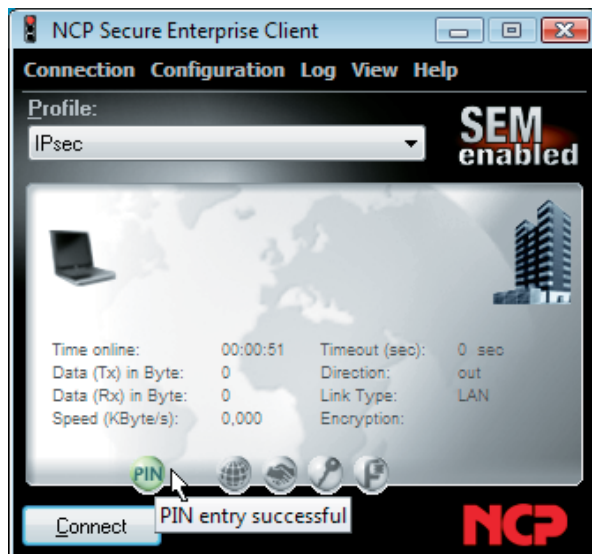
This ensures that when configuring “PIN Request at each Connection” on an unauthorized Client Monitor, a PIN entered previously by an unauthorized user cannot be used at anytime to set-up a connection.

## Reset PIN

This menu item can be selected for deleting the PIN, for making the valid PIN useless to other users. It can be helpful for example if you leave your client temporary or if the user changes. Afterwards a valid PIN must be reentered again for authentication.

## PIN State Symbol in the Client Monitor

If a valid PIN is entered this is symbolized by a green icon display in the client monitor. If the PIN has not yet been entered correctly the symbol will be grey (illustration below).



## PIN Handling after Logoff or Sleep Mode

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

## Display ACE Server Messages for RSA-Token

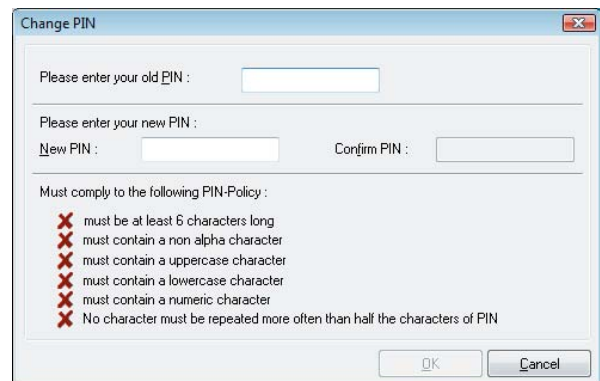
If messages are sent by the ACE server because of the RSA token they will be displayed on the monitor in an input field (for example "Expiration of valid PIN").

## 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 with a red cross (illustration above). They can be set in the main menu under "Certificate / PIN Policy".



## PC-Sharing (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 “User Certificate” the menu item “Certificate Selection” must be activated and a “Certificate Path” must be entered. If this path has been created previously, then you can select this path via the select button (e. g. INSTALLDIR\usercert). The various user certificates must then be stored 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 client1 to client4).



If the user has selected his soft certificate (client2 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. (Illustration above)



If the user leaves the workstation, then he should activate the “Logout” button. This completely dismantles the connection and resets the PIN (this also occurs if another connection is selected during an existing connection). If there is no logout, then nonauthorized users can obtain access to the VPN Gateway via the existing connection.

A subsequent user proceeds in precisely the same manner. First he selects his certificate, then clicks on the “Connect” function and enters his PIN. Only then can the connection be established correctly. If the user leaves the workstation, then he clicks on the “Logout” button.



**For Accounting on the VPN gateway when using PC sharing see next page.**



## Accounting on the VPN Gateway

The type of accounting on the VPN gateway is defined via the profile settings of the client. What is important here is the “VPN User Name” parameter in the “VPN-Tunneling” parameters.

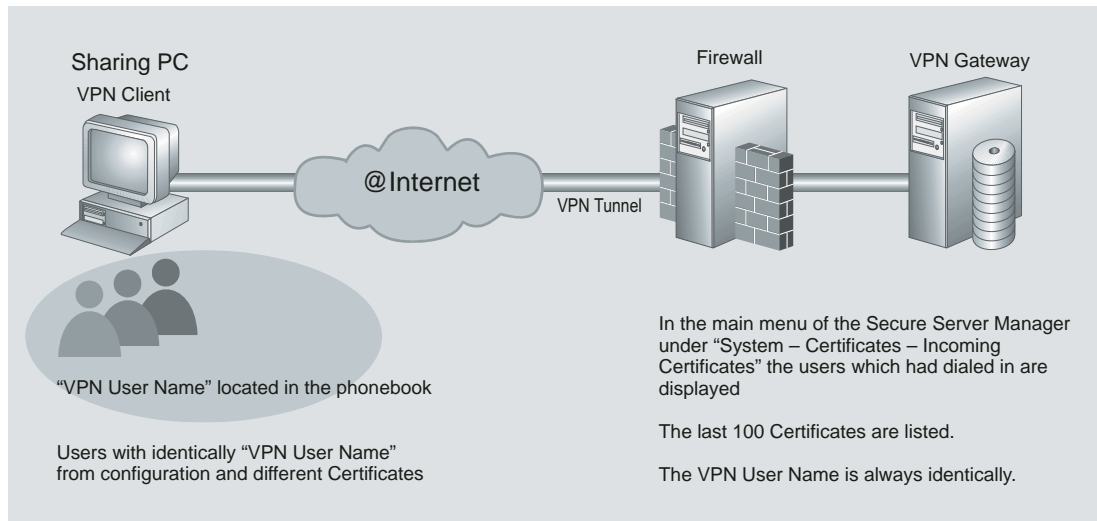


Illustration above: If “VPN User Name” is selected from the configuration (Sharing-PC1, for instance) then accounting is handled for all users, who dial in to this destination system, under the same user name, each with different certificates. Only one link must be created on the VPN gateway for this. The certificate last used for the general user name for the workstation PC can be read on the server under “Incoming Certificates”.

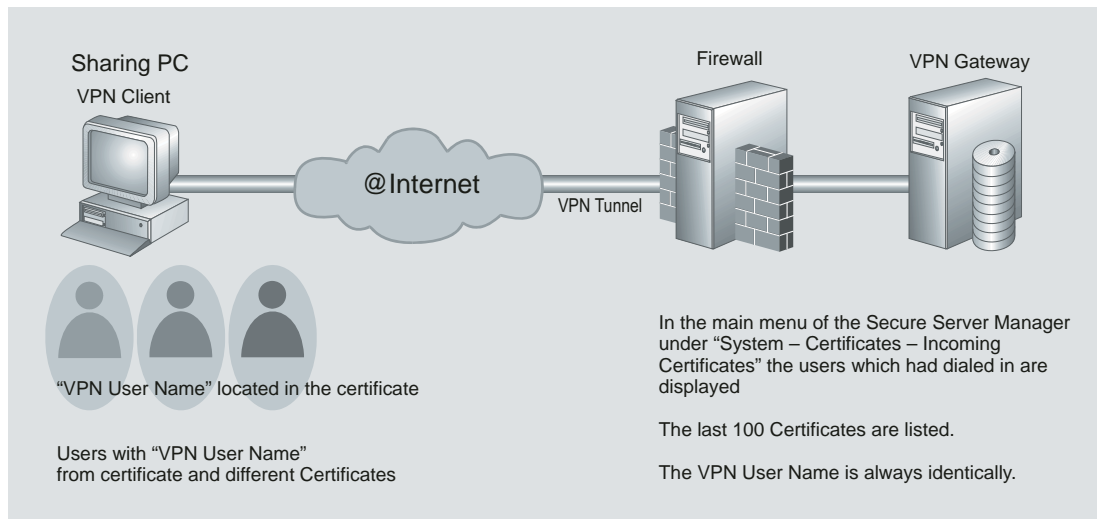


Illustration above: If the “VPN User Name” and the “VPN Password” are used from the soft certificate, then there is personalized accounting on the VPN Gateway, as with each newly selected certificate “VPN User Name and ”Password” change accordingly. In order to use this type of accounting, a separate link must be created on the VPN Gateway for each user.