



Using the Minikey with Check Point™ VPN Networks

User Guide

Version: 1.0
20 February 2002

©2003 Algorithmic-Research LTD.
Commercial-in-con

Contents

1. DEFINITIONS	3
2. INTRODUCTION.....	4
3. CONNECTION TO CHECK POINT VPN	5
4. PRELIMINARY REQUIREMENTS.....	6
4.1 Client Hardware Requirements.....	6
4.2 Client Software Requirements	6
4.3 VPN-1 SecuRemote Server Requirements	6
5. INSTALLATION PROCEDURE.....	7
5.1 Establish a username/password based VPN	7
5.2 Configure VPN-1/FireWall-1 for PKI based authentication.....	8
5.3 Initialize the MiniKey	8
5.4 Generate RSA keys and obtain certificate for the client	9
6. CONNECT TO THE VPN WITH AR MINIKEY	14

1. Definitions

The following table prescribes a common understanding of the terms and abbreviations used throughout this document.

Term	Meaning
AR	Algorithmic Research Ltd.
API	Application Program Interface
VPN	Virtual Private Network
CA	Certificate Authority
CRL	Certificate Revocation List
LDAP	Lightweight Directory Access Protocol
IKE	Internet Key Exchange
USB	Universal Serial Bus
CAPI	Cryptographic Application Programming Interface
NG	Next Generation
PIN	Personal Identification Number
PKI	Public Key Infrastructure

2. Introduction

AR's MiniKey is a portable, personal USB token that allows users to conveniently manage their keys and authenticate their identity when connecting to enterprise, e-commerce or other secure applications.

When plugged in, the MiniKey enables strong identification, authentication and encryption for all Internet, Intranet, Extranet and Web-based applications. With a powerful Smartcard chip inside, MiniKey is really a Smartcard that eliminates the need for a reader. MiniKeys are ideal for storing signing and encryption keys, X509 certificates, for creating and verifying electronic signatures, facilitating e-commerce, e-shopping and more.

MiniKey is perfect for enabling public key technologies such as SSL, IKE and S/MIME. It is supplied with CAPI Software, allowing it easy integration with MS CAPI-based applications such as Check Point's VPN-1 SecuRemote/ SecureClient.

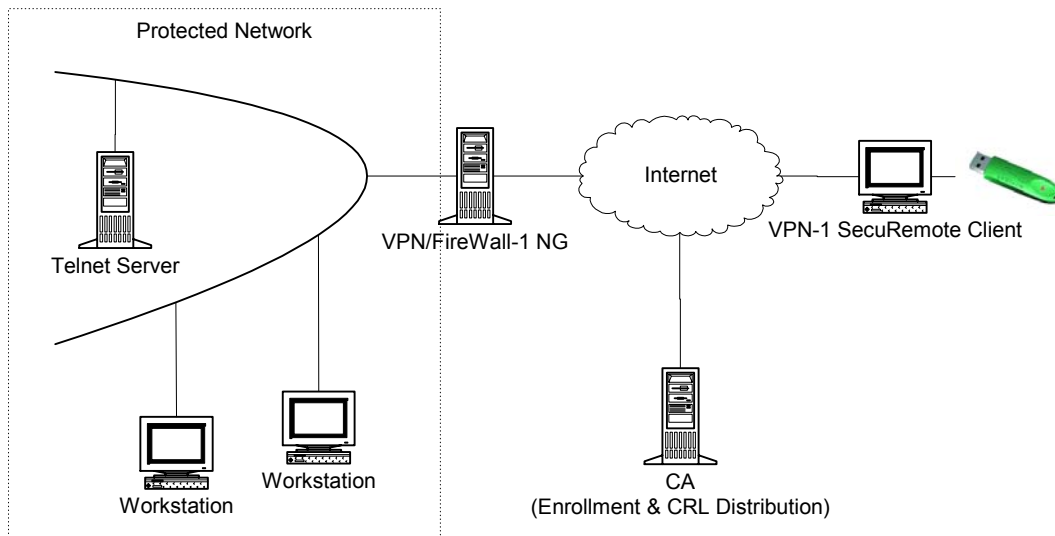


Check Point VPN-1 SecuRemote enables PC users to securely communicate sensitive and private information to networks and individual servers. Check Point VPN-1 SecuRemote extends the VPN to Windows workstations and desktops, using both dial-up and LAN connections.

VPN-1 SecuRemote encrypts data before it leaves the laptop and thus offers secure solution for remote connections. VPN-1 SecuRemote can transparently encrypt any TCP/IP communication.

3. Connection to Check Point VPN

Figure 1 shows a simple VPN network.



The client uses VPN-1 SecuRemote to securely connect to a telnet server. AR MiniKey is used to store the client's certificate and a pair of RSA private / public keys. The certificate was obtained from the CA of the organization.

The following process is triggered when the client tries to connect to the Telnet server:

- The VPN-1 SecuRemote automatically opens the authentication window.
- The client selects his authentication certificate. This certificate is sent to the server.
- A key exchange process (IKE) with the server starts.
- The client is requested to enter the PIN of the MiniKey to allow access to the private key that is stored on the MiniKey.
- The MiniKey signs an authentication message with the client's private key.
- The server checks the validity of the client's certificate by connecting to LDAP or HTTP servers.
- The server verifies the message signature with the client public key.
- The server sends his certificate to the client for verification.
- Once the authentication is verified, a secure and encrypted connection between the client and the Telnet server is established.

4. Preliminary Requirements

Following is a list of preliminary requirements that the VPN-1 SecRemote client and server computers should meet in order to be able to connect to the VPN using AR MiniKey.

4.1 Client Hardware Requirements

- Standard USB Port
- AR MiniKey token

4.2 Client Software Requirements

- Operating system: Windows 98, ME, NT Service Pack 6, 2000 or XP
- VPN-1 SecuRemote/ SecureClient, build 51057 or higher
- AR Cryptokit version 3.1 or higher.
During installation, MiniKey and CAPI components must be selected.

4.3 VPN-1 SecuRemote Server Requirements

- Check Point VPN-1/FireWall-1, Next Generation (NG)

5. Installation Procedure

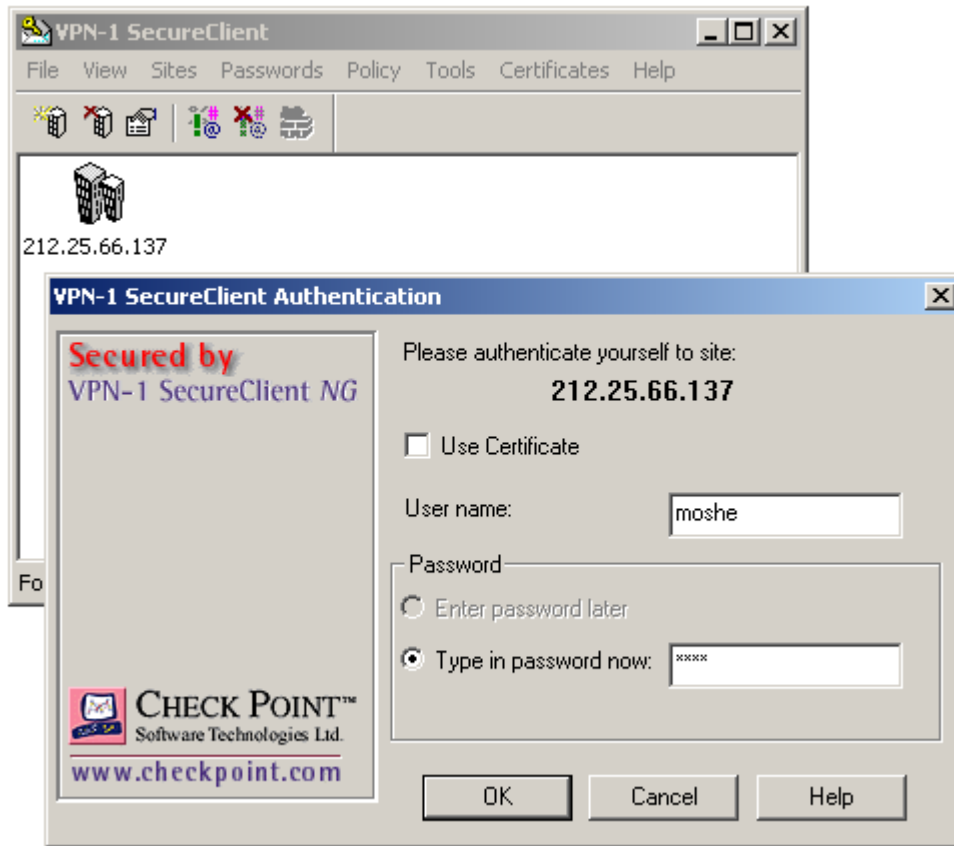
In order to configure your VPN-1 SecuRemote clients to work with AR MiniKey, you should configure both VPN-1 SecuRemote client and the VPN-1/FireWall-1 NG computers.

For a detailed explanation how to install and configure the VPN-1 SecuRemote and VPN-1/FireWall-1 NG, please refer to the book “Check Point Virtual Private Networks”.

5.1 Establish a username/password based VPN

To set up your VPN, please do the following steps:

1. Connect the gateway computer to the network and configure the routing tables.
2. Install and configure the VPN-1/FireWall-1 NG software on the gateway computer.
 - ◆ Configure the VPN-1/FireWall-1 NG software
 - ◆ Define users and groups of users
 - ◆ Define the firewall rules, including the VPN.
3. Install the VPN-1 SecuRemote software on the client computer.
4. Select “Add a new site” from VPN-1 Secureremote menu and enter the IP address of the server.
5. Enter username and password and connect to the VPN.



Once a secure VPN connection has been established by using a username and password we can proceed to the next step and configure the client and server to work with AR MiniKey. This configuration is based on PKI technology and the organization needs access to a CA for certificate generation and CRL distribution.

5.2 Configure VPN-1/FireWall-1 for PKI based authentication

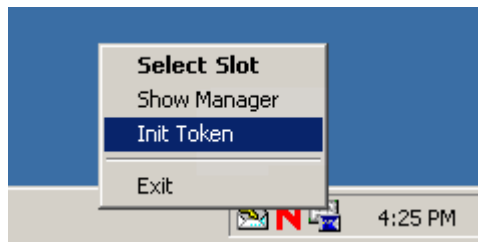
Please do the following steps on the VPN-1/FireWall-1 NG computer:

1. Add definition of the CA.
2. Obtain a certificate for the VPN-1/FireWall-1 server from the CA by generating a PKCS10 certificate request.
3. Add definition of LDAP or HTTP server that distributes the CRL's.
4. Specify in the user's definition IKE encryption method.

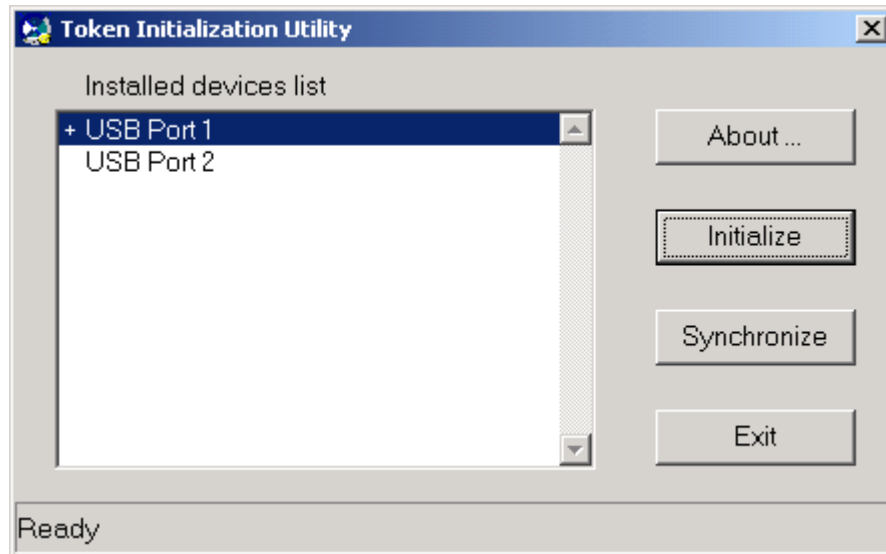
5.3 Initialize the MiniKey

Before using the MiniKey for the first time it has to be initialized with the "Token Initialization Utility".

To run this utility, select it from the cryptokit menu or by pressing right click on the icon of "AR Certificate Manager" at the system tray and selecting "Init Token".



The “Token Initialization Utility” screen displays a list of all the tokens currently installed on the computer. A plus sign [+] indicates that the token is present.




To initialize the MiniKey:


- Insert the MiniKey into the USB port.
- Click in the installed devices list, the USB port with MiniKey inserted.
- Click the Initialize button.
- Enter the password for the MiniKey (minimum 6, maximum 55 alphanumeric characters) and confirm it.
- Wait until the initialization process is finished.

5.4 Generate RSA keys and obtain certificate for the client

The client has to generate on the MiniKey a pair of RSA private / public keys and obtain a certificate from the CA by:

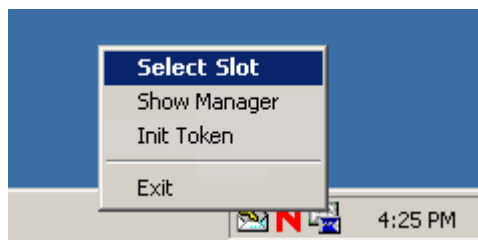
- Filling an enrollment form using a Web browser.
- Generating a PKCS10 certificate request and sending it to the CA. The CA generates the certificate and sends it back to the client.

 **Note:** The client must obtain the certificate from the same CA that certified the VPN-1/FireWall-1 server. When the SecuRemote user and the site authenticate each other using certificates, the SecuRemote client trusts only the CA that signed the user's certificate. If a different CA signed the server's certificate, the authentication will fail.

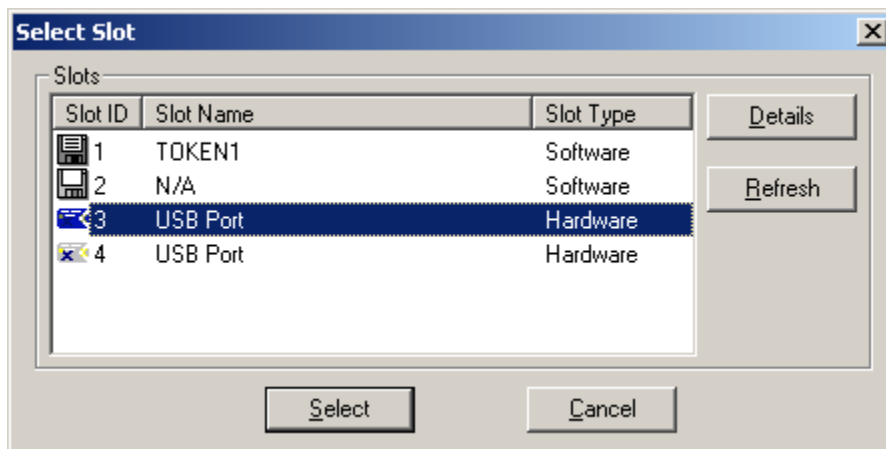
 **Note:** AR Minikey may hold up to 6 sets of private/public/certificate objects. Each set, may be used to authenticate to a different server or application.

Please follow the instructions below to generate the keys and certificate by using a Web form:


- Open AR “Certificate Manager” by selecting it from the cryptokit menu or by pressing right click on the icon of “AR Certificate Manager” at the system tray and selecting “**Select Slot**”.



- The “Select Slot” Window should open and display all the slots that are installed on the computer. Verify that the selected slot (default slot) is the USB port with the MiniKey inserted and press the select button.




- Open a Web browser and enter the enrollment page of the CA of the organization.
- Fill in the enrollment form. Make sure that the CN (Common Name) is exactly the same as was defined in the users table of the VPN-1/FireWall-1 server.

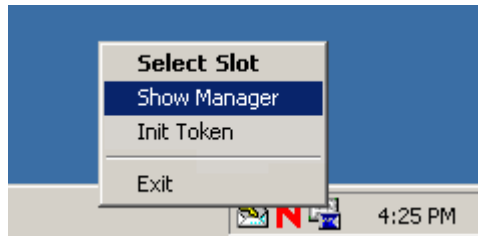
 **Note:** If the user name is different in the certificate from the user table in server, logon will fail!

- In the enrollment form you should specify the key usgae. Please make sure to mark “Client Authentication”. If you don't, the VPN-1 SecuRemote client would not be able to use the keys and certificate created.
- Press the submit button in the enrollment page.

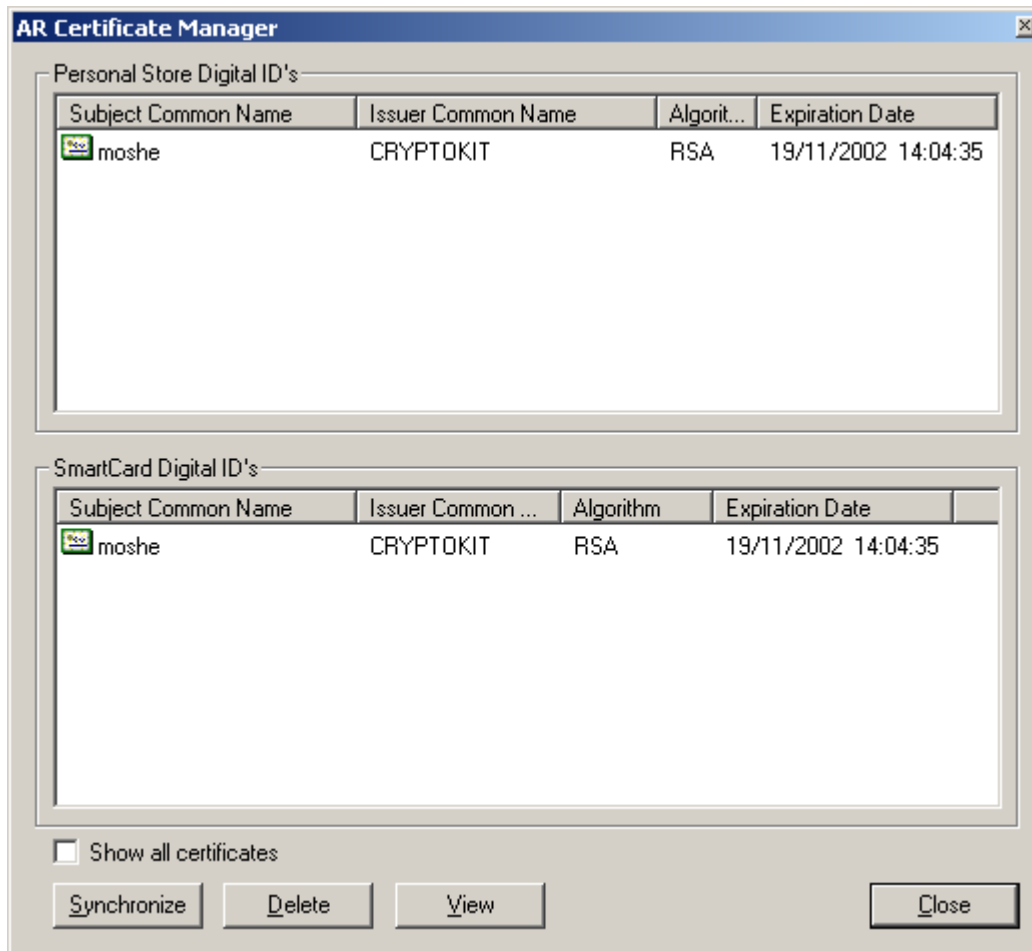
-
- Enter the PIN of the MiniKey.
 - At this stage, you should see that the light on the MiniKey blinks. The RSA private and public keys are created on the MiniKey. This may take about 30 seconds. When the process finishes, the public key is sent to the CA.
 - As a response the CA generates a certificate and the Web browser should show a new screen where you are asked whether to “Install the Certificate” on the token or not.
 - Press, “Install the Certificate” and enter the MiniKey Pin again. The certificate should be written on the MiniKey.

 **Note:** The process of enrollment may change, from one CA to another. Please consult your network administrator for additional details.

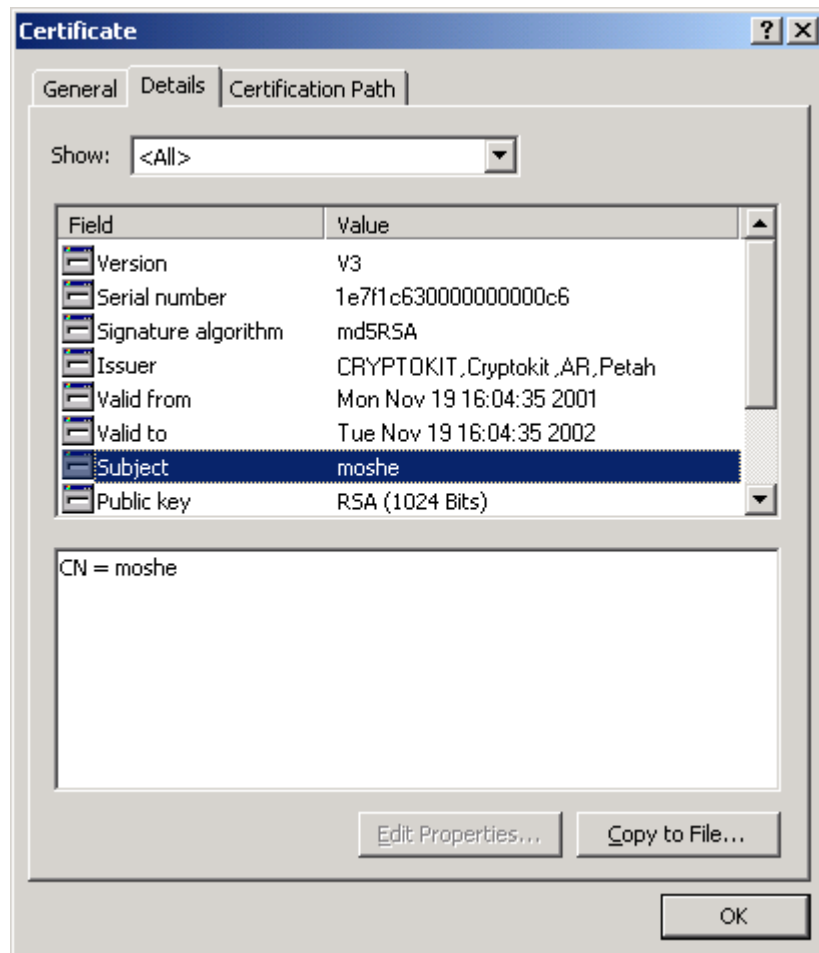
- To check the contents of the MiniKey, you can use another utility, the “Show Manger”. Activate it by pressing right click on the icon of “AR Certificate Manager” at the system tray and selecting “Show Manager”.



- “AR Certificate Manager” Window should open and display all the certificates in the personal store of digital ID’s and the certificates on the smart card.



- Double click a certificate, to view it's details



6. Connect to the VPN with AR MiniKey

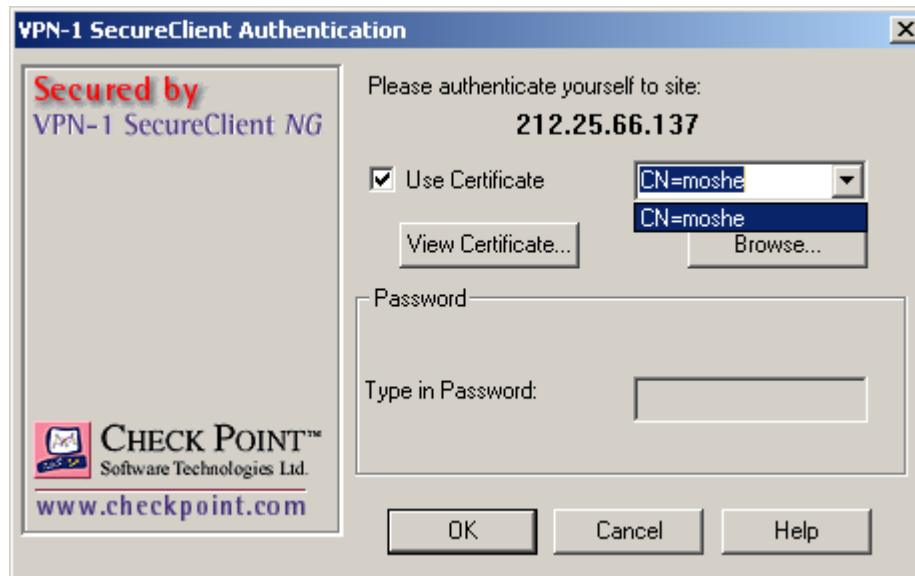
Once the installation and enrollment process has finished the user is ready to connect to the server with the certificate stored on the MiniKey.

Please follow the instructions below:

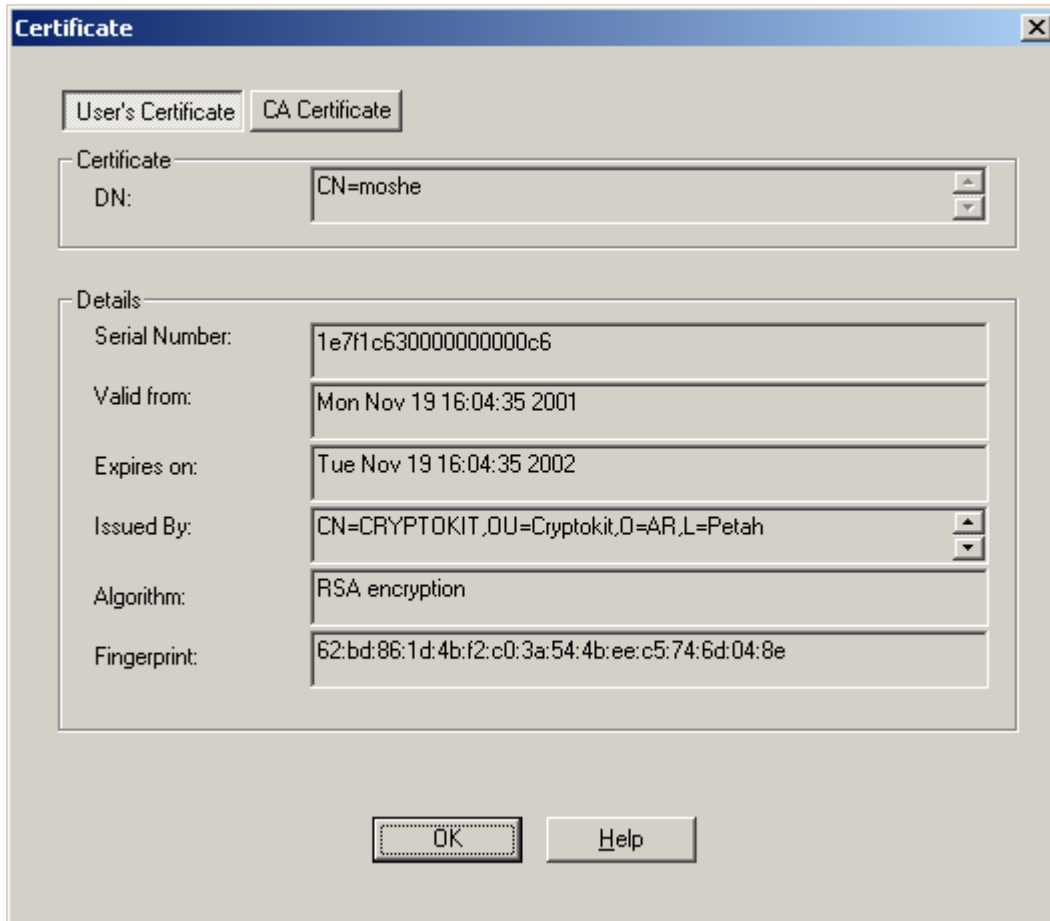
- Insert the MiniKey into the USB port of the computer.
- Open the “VPN-1 SecureClient” window and select “Set Password”.



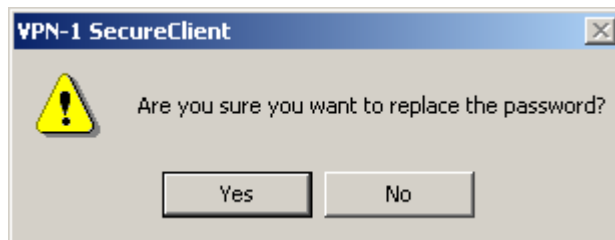
- In the “VPN-1 SecureClient Authentication” window, check “Use Certificate” and select your certificate from the list.



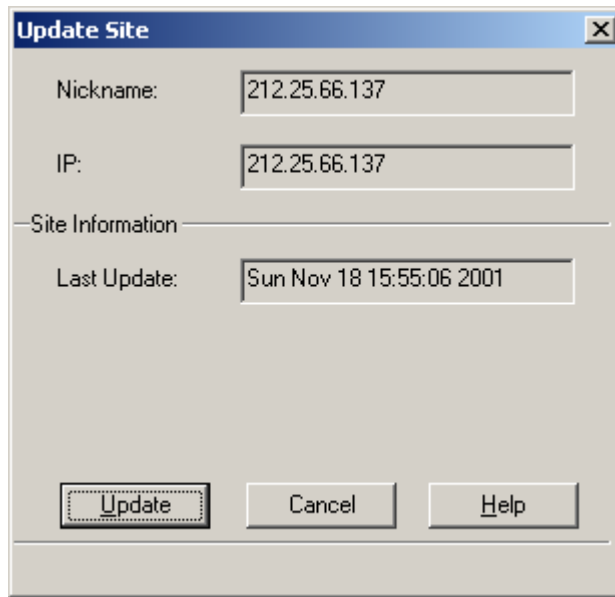
- You can view the certificate details by pressing the “View Certificate” button.



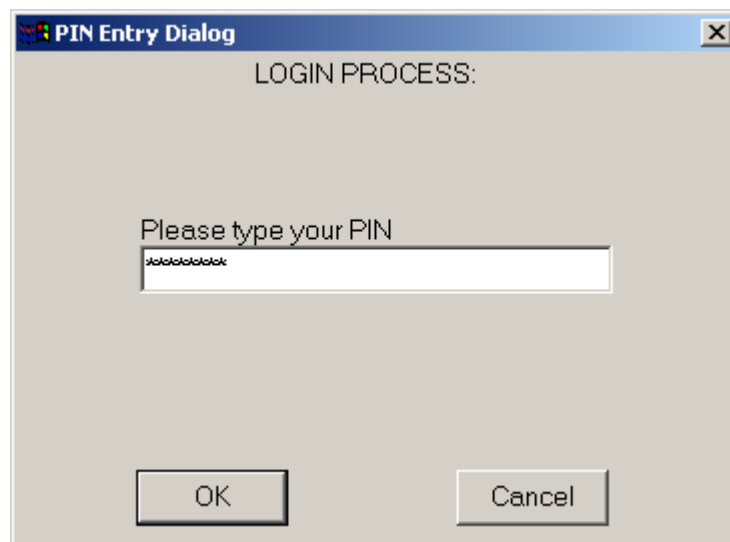
- Press OK. Then confirm the password change.



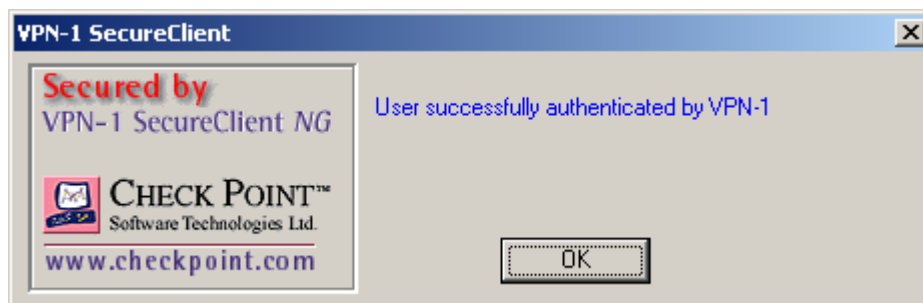
- Select “Update Site” from the VPN-1 SecuRemote menu. Then press the “Update” button.



- The MiniKey PIN entry dialog would open. Type the MiniKey PIN code and press OK.



- The authentication process should start and at the end a success window should show the following message.



-
- In case of failure, please refer to the book “Check Point Virtual Private Networks” for a specific explanation what could have caused the authentication failure.
 - At this point a secure connection with the gateway server has been established. All communication on the TCP port that was defined in the gateway, will be encrypted.