NetScreen Remote with DataKey 330 SmartCard on Windows 2000

1 Summary
This implementation guide will document how to use the DataKey 330 model smartcard with NetScreen Remote 7 to store the user’s credentials. VPN access would require the user to enter their smartcard and enter their pass phrase to unlock their smartcard key container.

2 Requirements
This section will detail the products and versions used for this guide.

- NetScreen Remote 7.0r1
- DataKey 330 smartcard
- DataKey CIP V4.5
- PCSC compatible reader- (For this guide the Infineer 2750 USB Keyboard with integrated smartcard reader was used)
- Windows 2000

3 Installation
This section covers the basic installation steps to achieve the desired functionality. Detailed installation instructions are available with each product. The following products do not have to be installed in the order provided- they are just listed to verify installation requirements.

3.1 Install Infineer 2750 Keyboard
Follow the instructions provided with the Infineer reader to install the USB Keyboard. The Reader will also be installed.

3.2 Install DataKey CIP V4.5
Follow the instructions provided with the DataKey CIP to install the Datakey CSP.

3.3 Install NetScreen Remote
Follow the instructions provided with the NetScreen Remote product.

4 Configuration

4.1 Initialize the Smartcard
After installing the DataKey CIP V4.5, the Datakey Token Utility will be installed on the machine (image below).
From the file menu, select Initialize token. The token will be erased and a new password (PASSWORD) will be assigned. The default password can be changed. This password will be required to access the smartcard.

After the token has been initialized, the smartcard can be used as a key container for certificates generated with SoftRemote for VPN access.

4.2 Generate Certificate

The user can now generate a certificate requested using SoftRemote’s Certificate Manager and store their certificate and private key on the smartcard. Follow the following steps to enroll certificate:

1) Obtain Root CA certificate
2) Request Personal certificate- Fill out the certificate request form for your personal certificate and then select Advanced.
3) Select the Datakey RSA CSP (see below).
4) Submit your certificate request- The RSA key pairs will be generated on the smartcard and then the certificate request will be sent to the CA. Once the CA Administrator has approved the certificate, you will be able to use your smartcard for VPN access.

4.3 Verify Certificate

Using Certificate Manager, the certificate on the smartcard can be verified. You will be prompted for the password to access the smartcard.
If the password is correct and the certificate verifies properly, you will receive the following message:

If the smartcard is not present, you will receive a message indicating that the certificate has no private key. This message is correct in the fact that Certificate Manager was unable to access the key container for the smartcard.

If the smartcard is present but the user presses cancel, Certificate Manager will display the following error. The private key is not corrupt but inaccessible. If the user supplies the correct password, then the key container and private key will be accessed.

4.4 View Certificate with DataKey Token utility (optional)

The Datakey Token Utility provides an interface to the smartcard, which allows the user to get Token Status, View certificates, and View objects. After logging into the smartcard with the user’s password, the following information can be obtained.
5 Operation

5.1 Establish VPN

Configure your policy to have a secure connection utilizing the certificate obtained above. When establishing the VPN connection, you will be prompted for the password to access the key container containing the certificate.

If the smartcard is unavailable, the View log will display the following message:

12:17:47.456 Security Policy entry <My Connections\New Connection/My Identity> doesn't refer to a valid certificate.
12:17:47.456 CryptAcquireContext error 0.
12:17:47.456 Failed to initiate negotiation.

6 Usability Issues

When attempting to establish a VPN which requires access to the smartcard key container, it takes approx 10 seconds to get the CSP smartcard password dialog box, once a secure packet is attempted.