



## **Sterling Commerce Certificate Wizard 1.1.00**

Document Number: **SC-EMEA-C-007-001**

Status: **Approved**

Author: **Gurmit Hayre**

Date: **25<sup>th</sup> July 2003**

Introduction .....	2
Generate Self-Signed Certificate.....	3
Create the 'Keycert' file .....	10
Verify Certificates .....	12
Configure Connect:Direct Windows to use Secure+ .....	15
Setting up Secure+ between Windows and Unix .....	18
Setting up Secure+ between Windows and OS/390.....	20

## **Introduction**

The Sterling Commerce Certificate Wizard enables the generation of a certificate signing request (CSR) or a self-signed certificate on a computer running the Windows or UNIX operating system. This paper addresses how the Certificate Wizard can be used to generate a 'Self-Signed Certificate', and subsequently how to configure Connect:Direct systems to use these certificates.

For information on System Requirements for the Certificate Wizard, see the 'Sterling Commerce Certificate Wizard Version 1.1 Readme'.

A basic knowledge of SSL is assumed. For further information on SSL, see the 'Related Documentation' section.

**WARNING** : Using Self-Signed Certificates is not recommended for production environments and should only be used to facilitate test environments prior to production. Check with your Certificate Authority for Production Certificates.

## **Sterling Commerce Software used**

Certificate Wizard 1.1.00  
Connect:Direct Windows 4.1.00 Build 024  
Connect:Direct Secure+ Option for Windows 3.0  
Connect:Direct for Unix 3.5.00 Fix Level 03Jun2003  
Connect:Direct Secure+ Option for Unix 3.0  
Connect:Direct for OS/390 4.2.00 Put Level 4203  
Connect:Direct Secure+ Option for OS/390 2.0

## **Related Documentation**

Sterling Commerce Certificate Wizard Version 1.1 Readme

IBM OS/390 V2R8.0 System SSL Programming Guide and Reference  
( Document Number: SC24-5877-01 ).

## **1. Generate Self-Signed Certificate.**

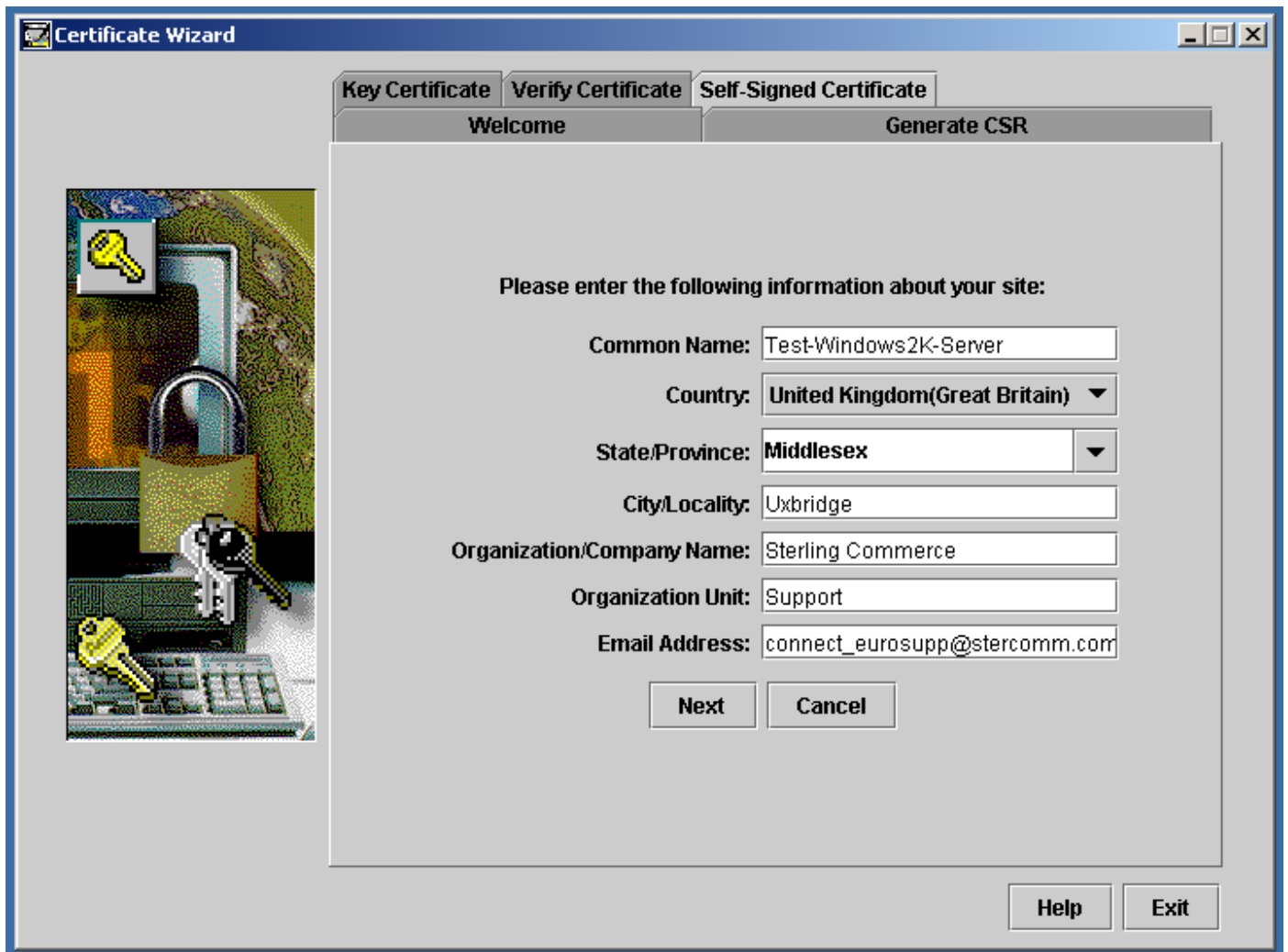
Run Certificate Wizard.

The following details the creation of the required files for Secure+ on Windows.

**If you need more information on any field in Certificate Wizard, click ‘Help’.**

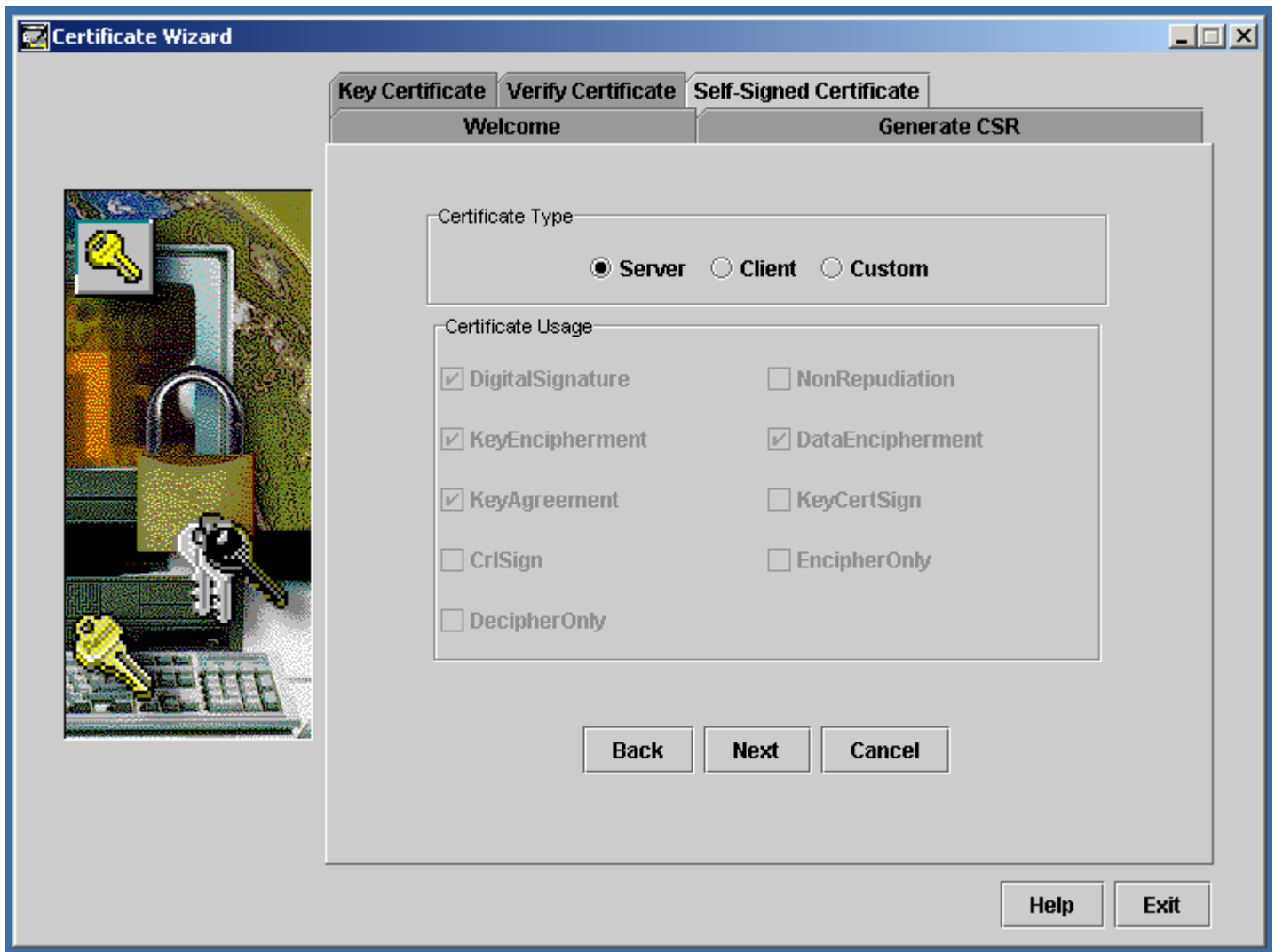


Click on the ‘Self-Signed Certificate’ tab:



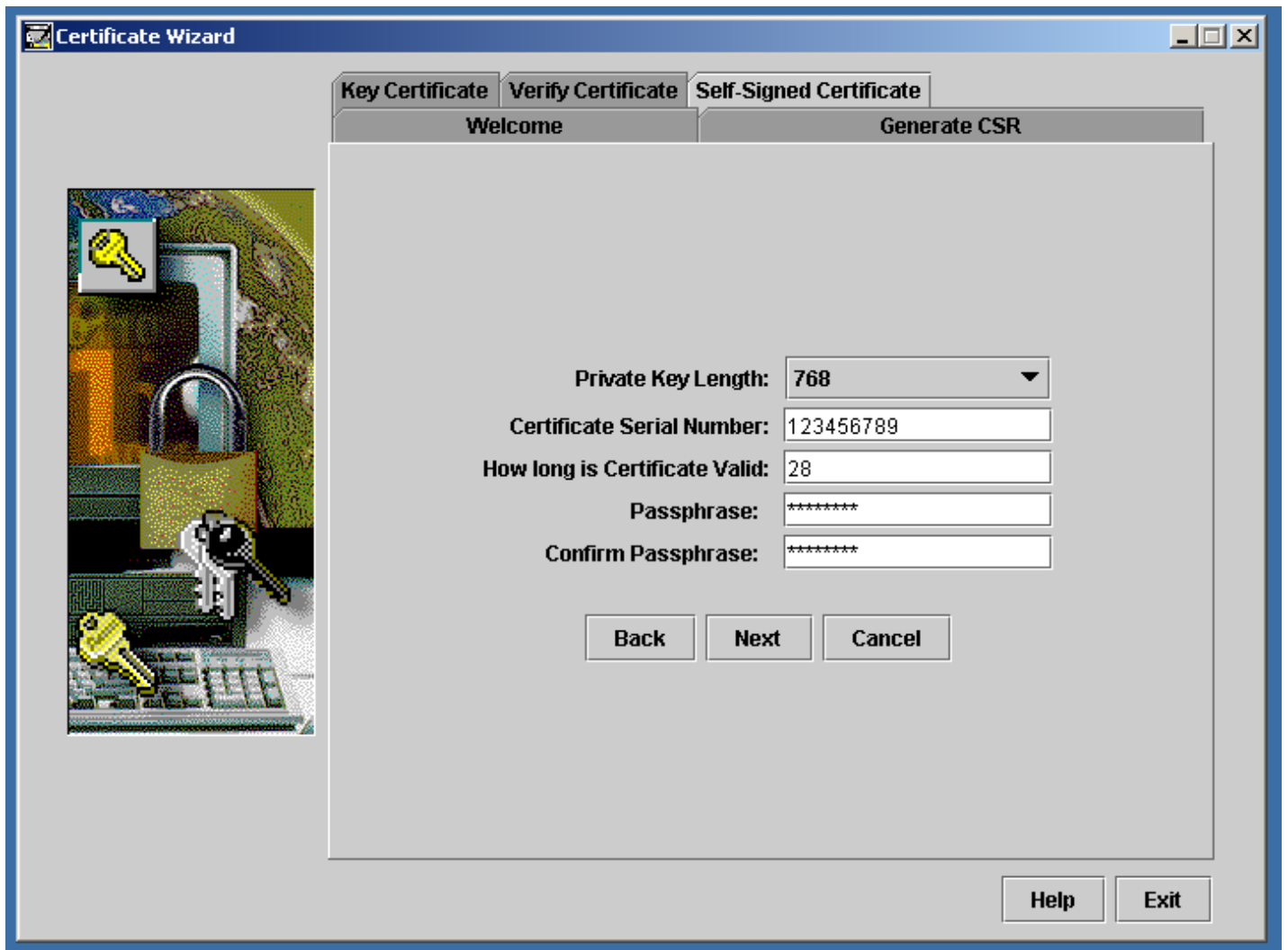
Enter appropriate values into the panel. To get more information on any of the fields, click 'Help'.

Click 'Next'.



Working just with 'Server Authentication', accept Default values.

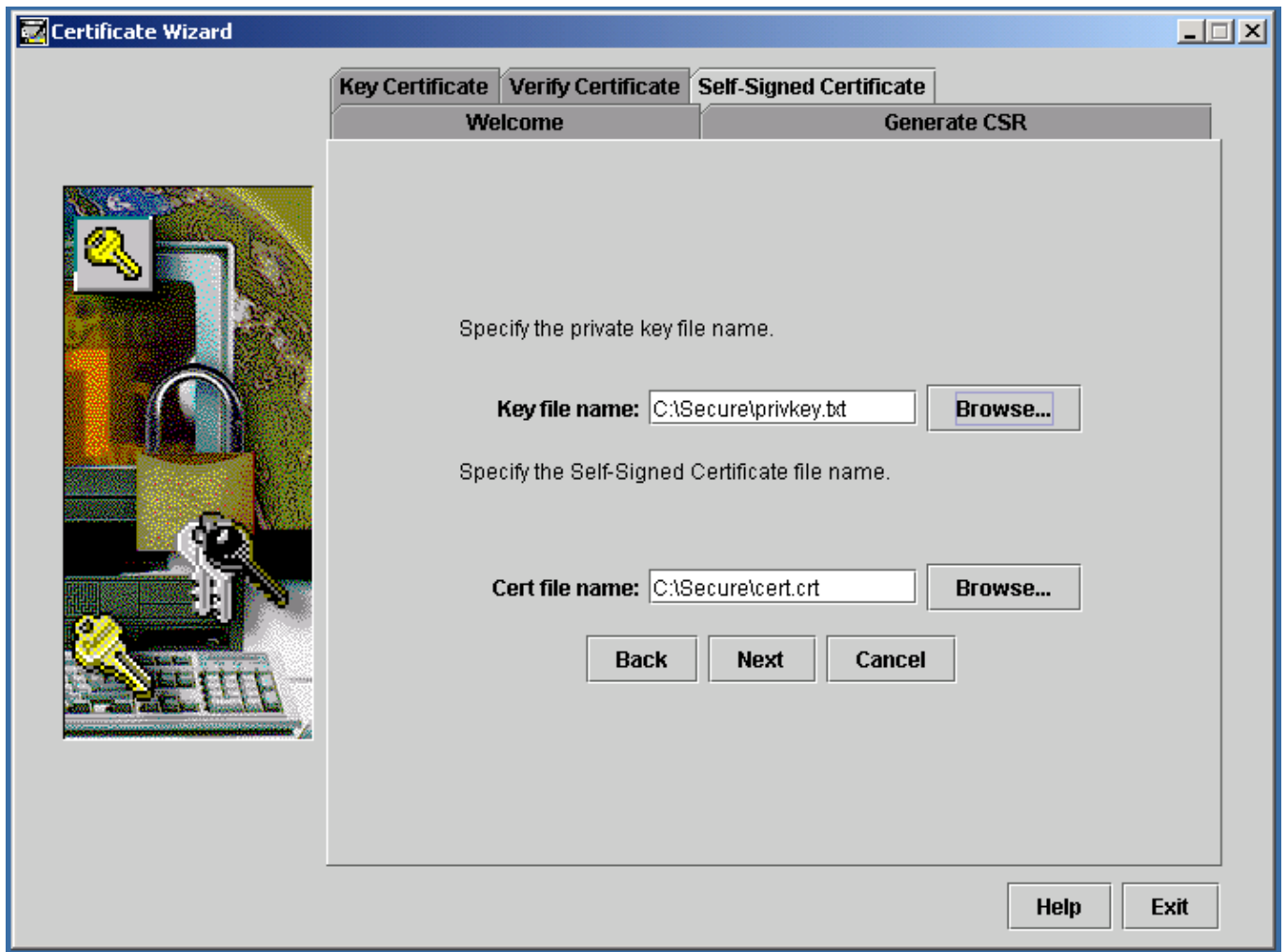
Click 'Next'.



As this is for TESTING ONLY, enter any appropriate values for the fields above.

The Passphrase you specify here will be used later.

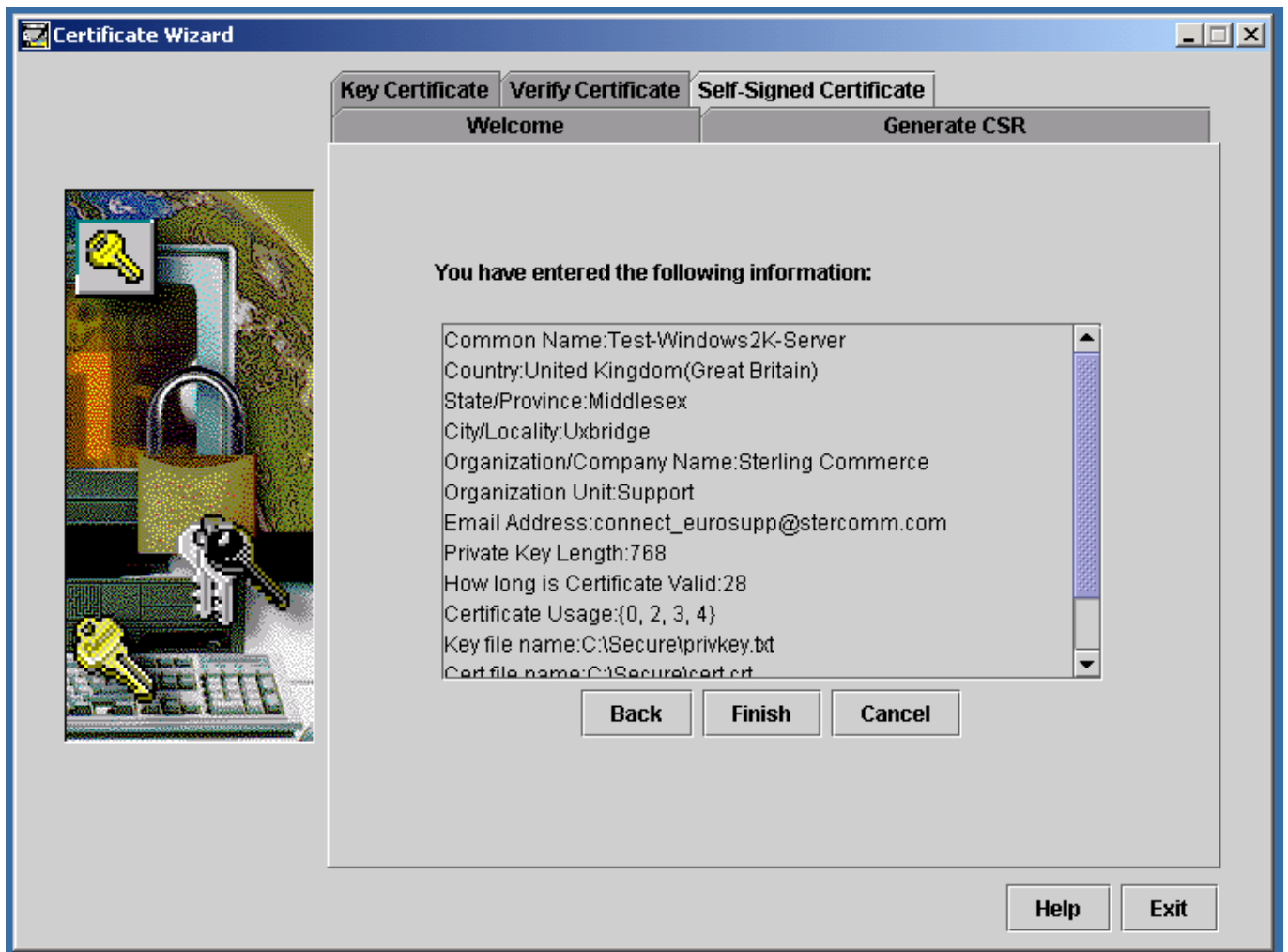
Click 'Next'.



Specify a location for the Private key and the Certificate.

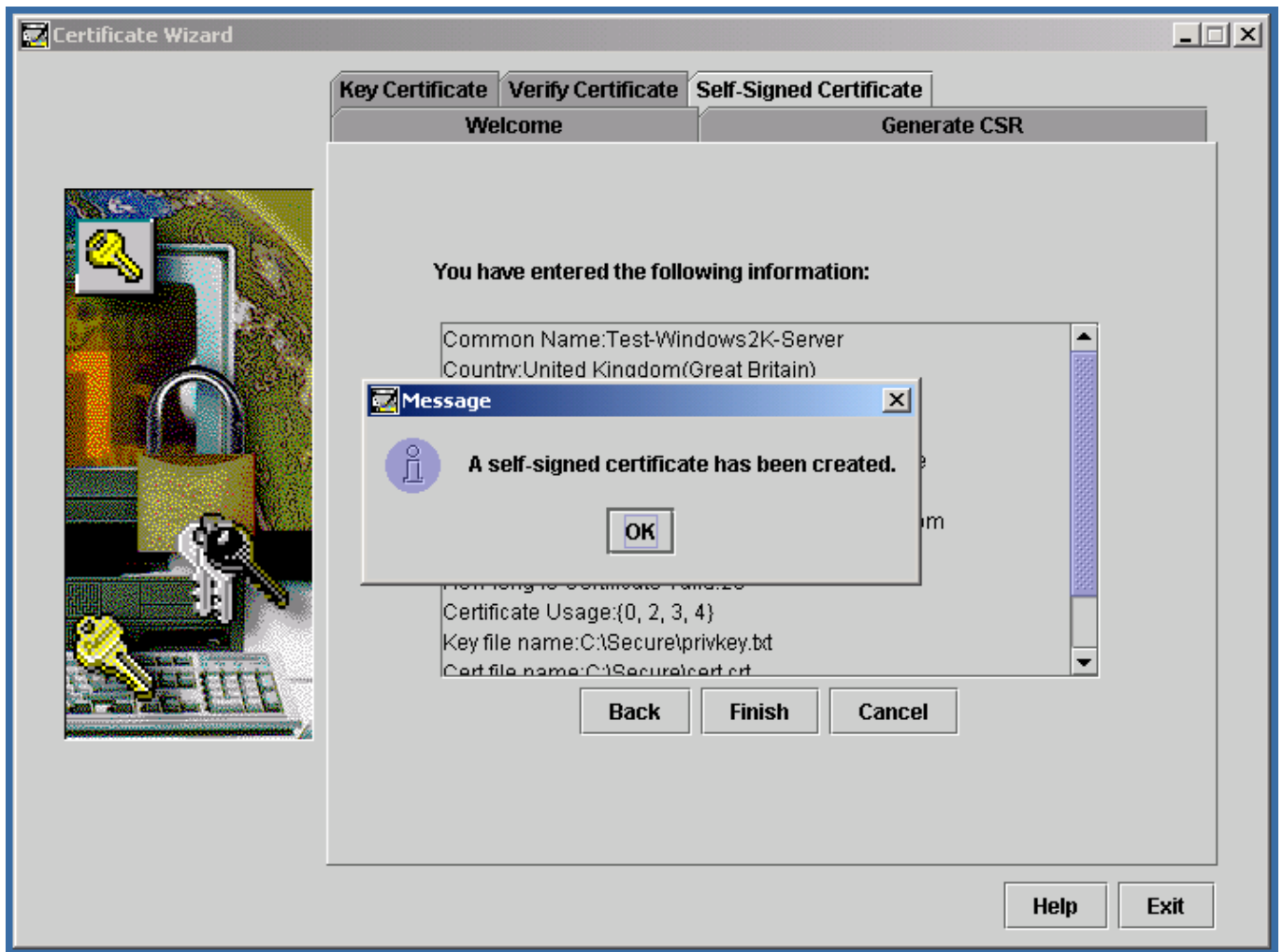
Click 'Next'.





Check the details.

Click 'Finish'.

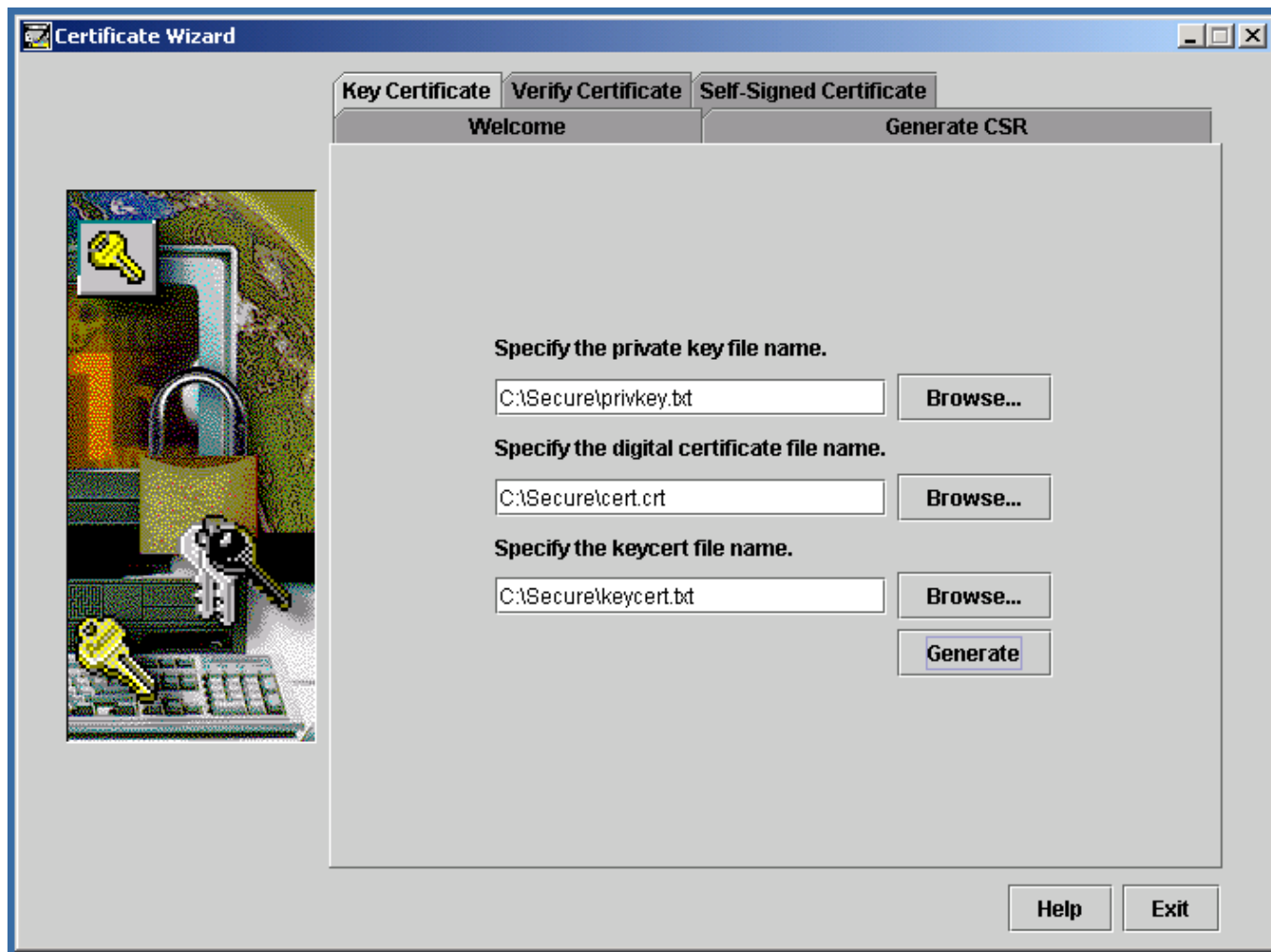


Self-Signed certificate created.

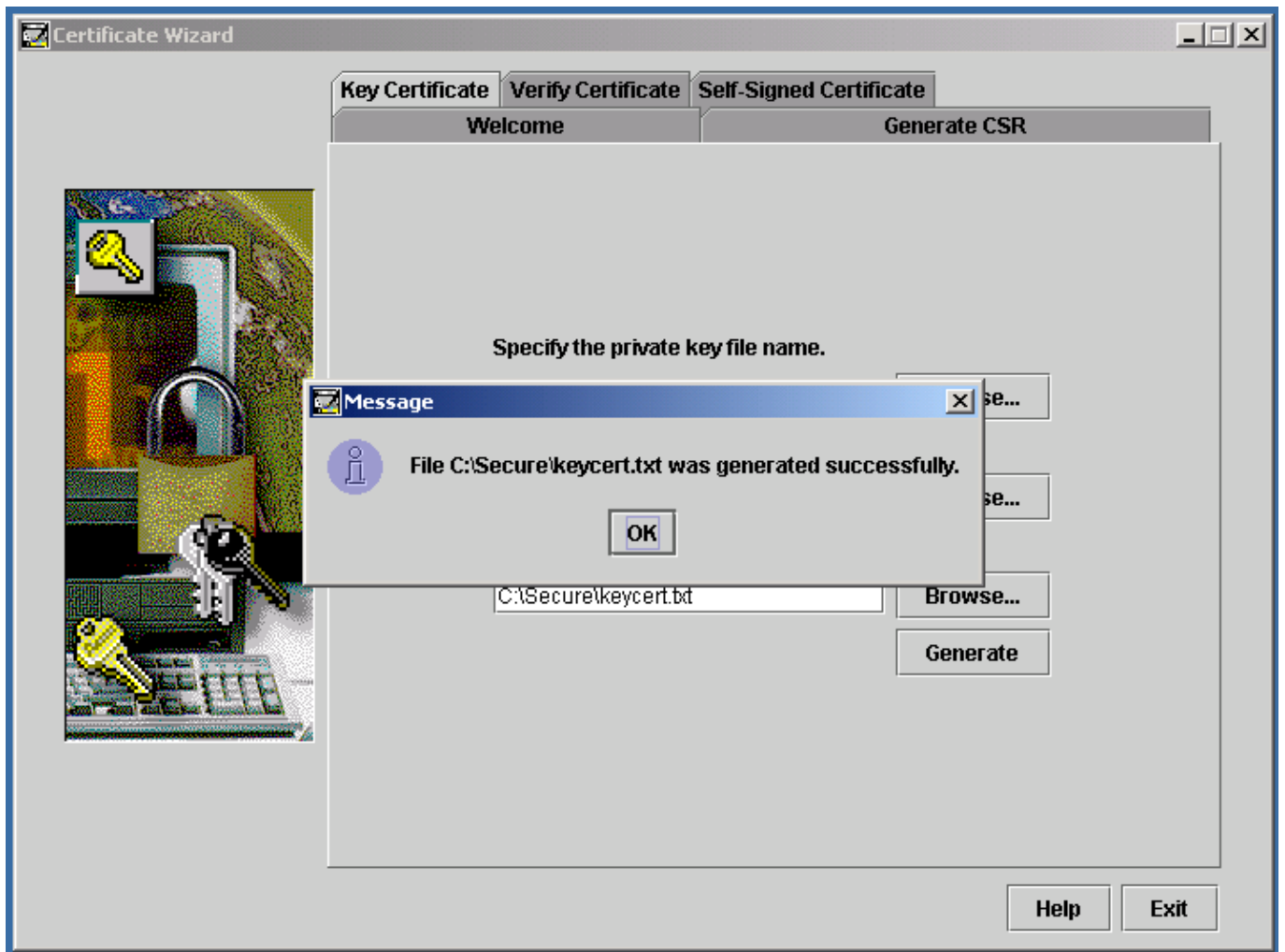
This Self-Signed certificate will also act as a 'Trusted Root Certificate'. For simplicity, copy the 'cert.crt' file, naming the new file, 'TrustedRoot.txt'

## 2. Create the 'Keycert' file

Click the 'Key Certificate' tab :



Specify the previously created 'Private Key' and Certificate from Step 1. In the 'Specify the keycert file name' box, specify the name and location of the keycert file you wish to create. Click on 'Generate'. You should see the following:



'Keycert' file has been created.

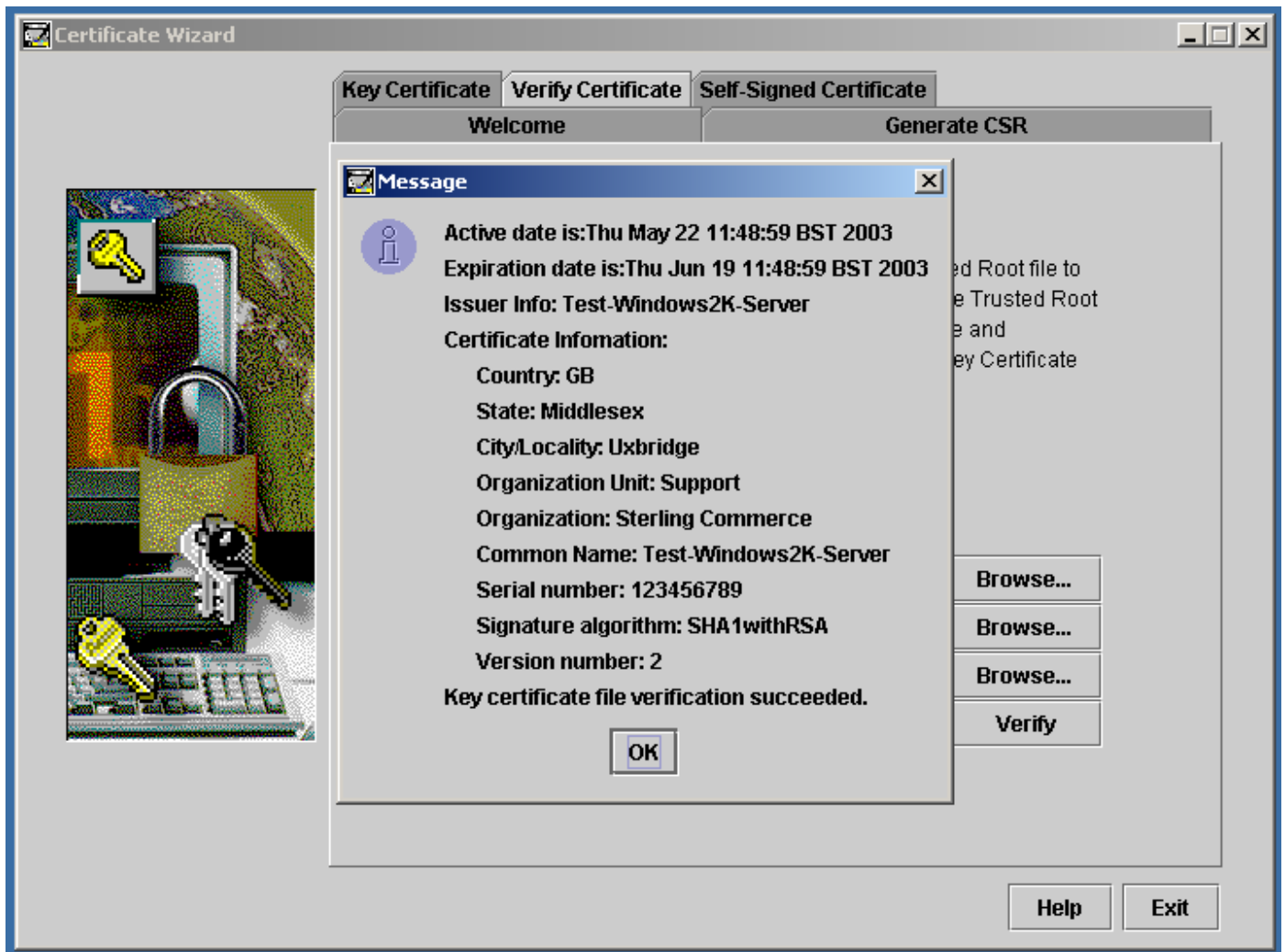
### 3. Verify Certificates

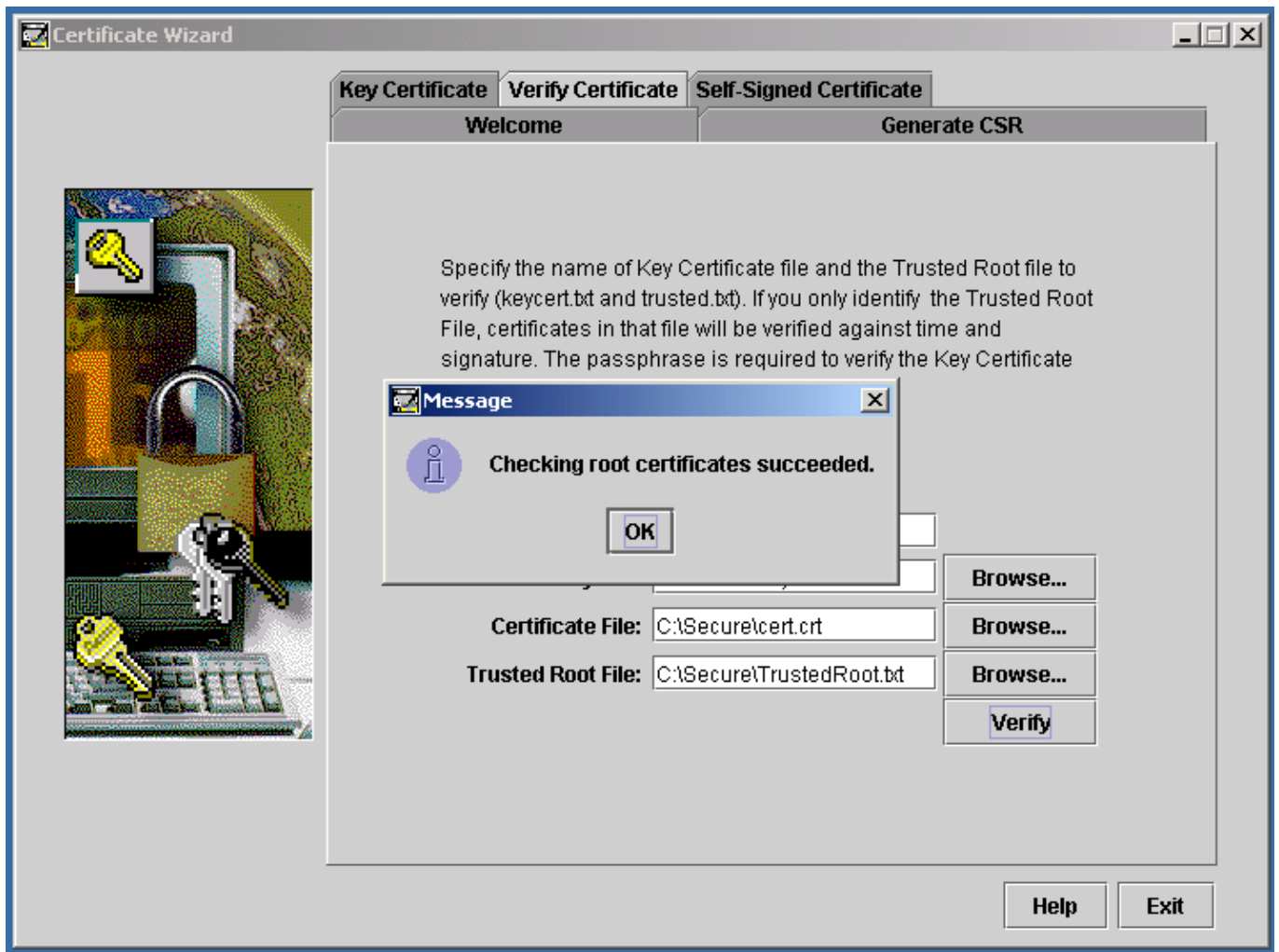
Verify Certificates by clicking on the 'Verify Certificate' tab:



Enter the filenames from Steps 1 and 2.

If verification is successful, the following screens appear:

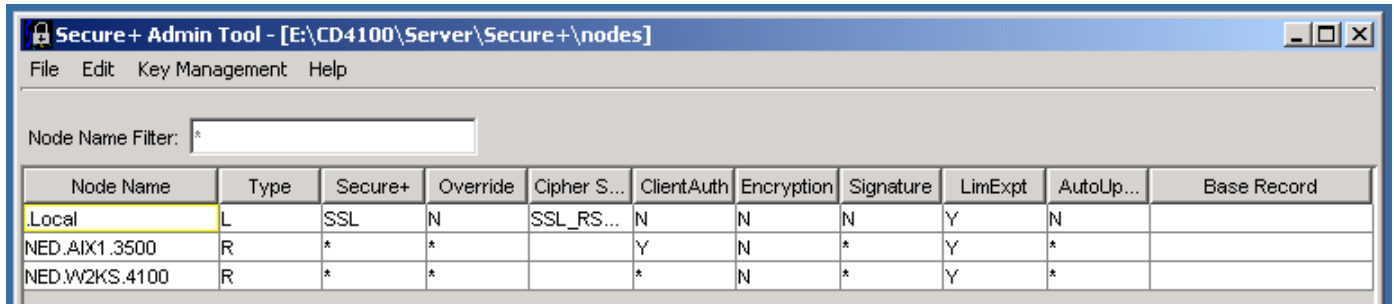




Verification is done.

## **4. Configure Connect:Direct Windows to use Secure+.**

Run the Connect:Direct Windows 'Secure+ Admin Tool':

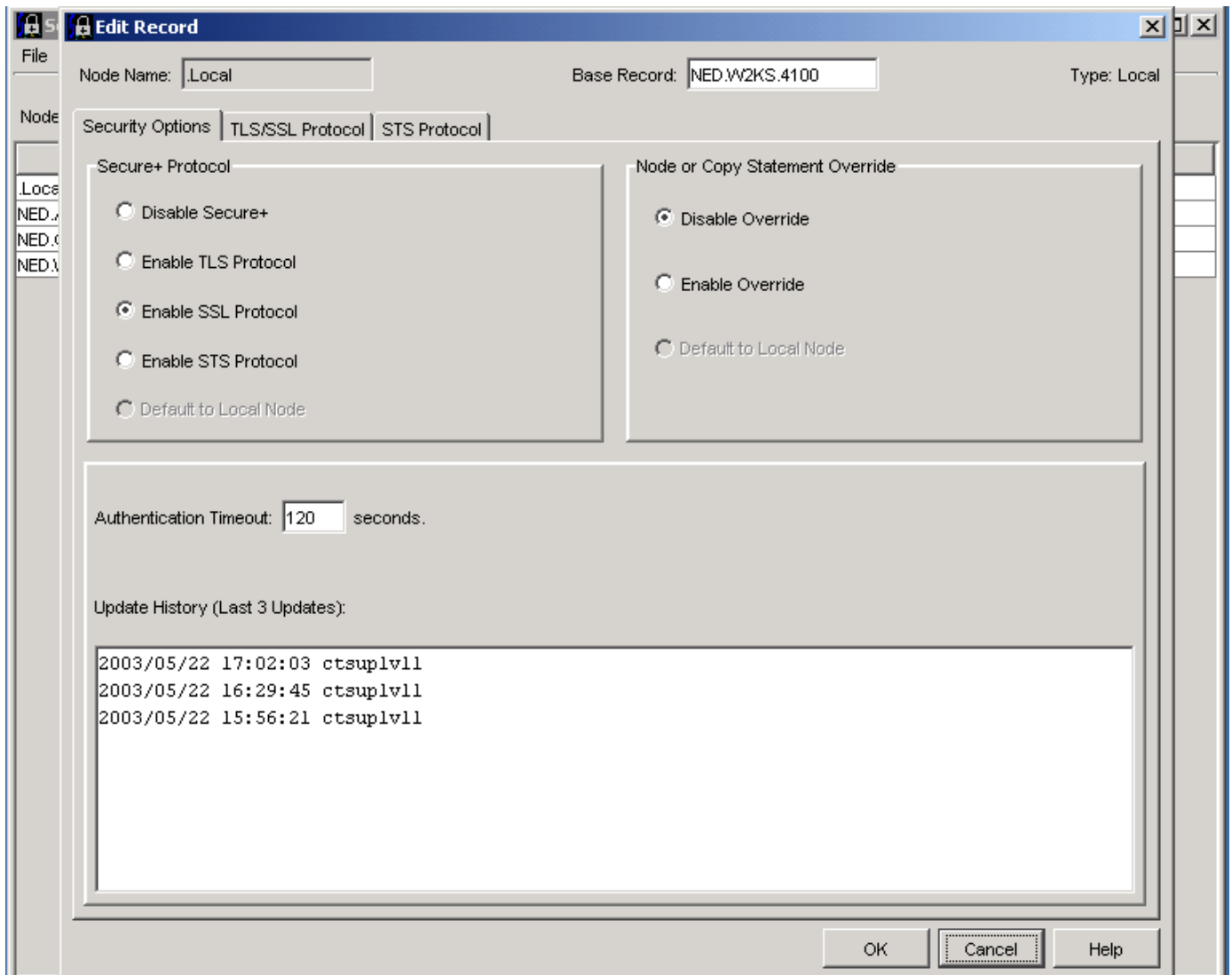


The screenshot shows the 'Secure+ Admin Tool' window with the following table of node configurations:

Node Name	Type	Secure+	Override	Cipher S...	ClientAuth	Encryption	Signature	LimExpt	AutoUp...	Base Record
.Local	L	SSL	N	SSL_RS...	N	N	N	Y	N	
NED.AIX1.3500	R	*	*		Y	N	*	Y	*	
NED.W2KS.4100	R	*	*		*	N	*	Y	*	

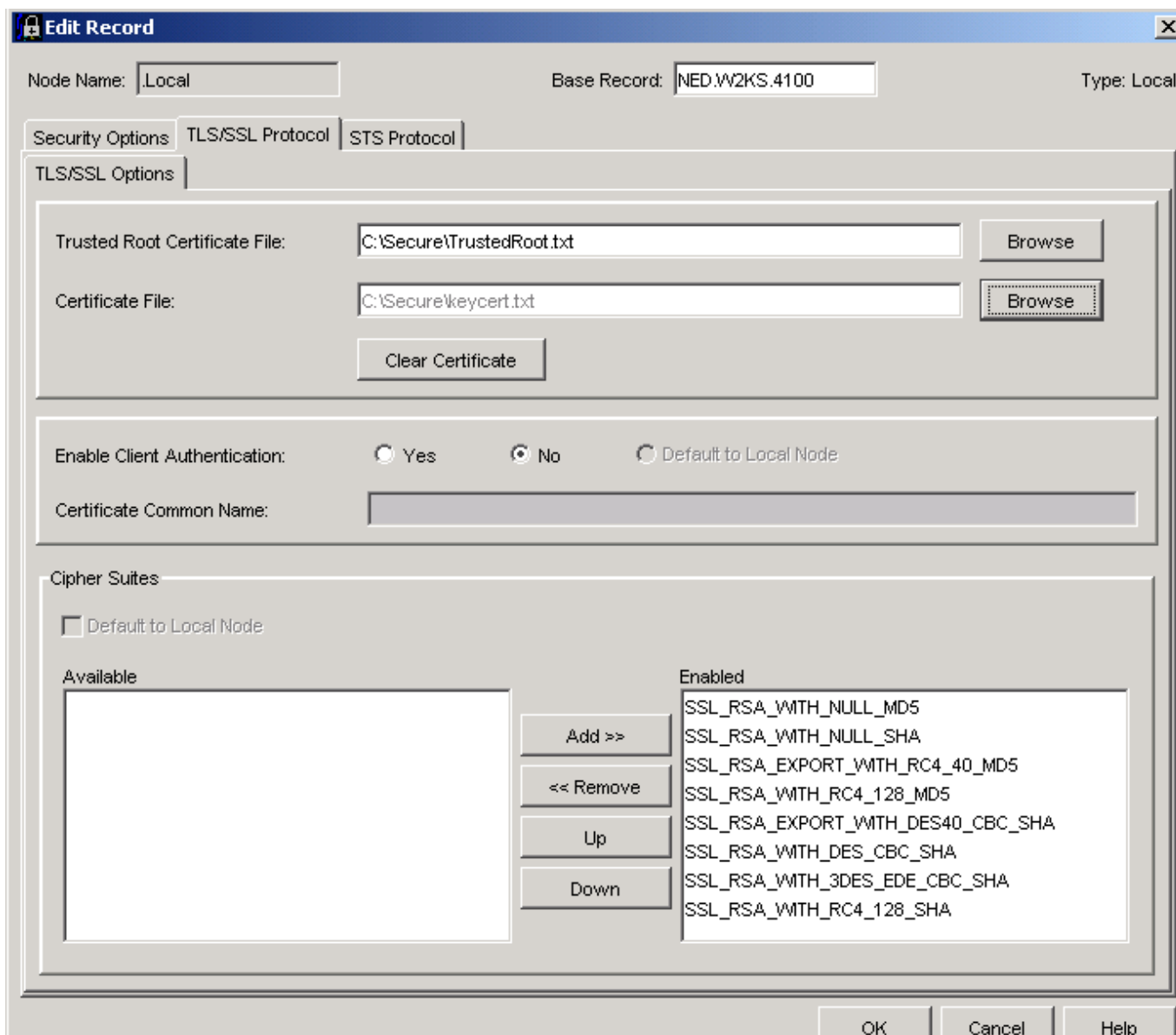
Expand the '.Local' record:





Check the boxes as above. Click OK.

Click the 'TLS/SSL Protocol' tab.



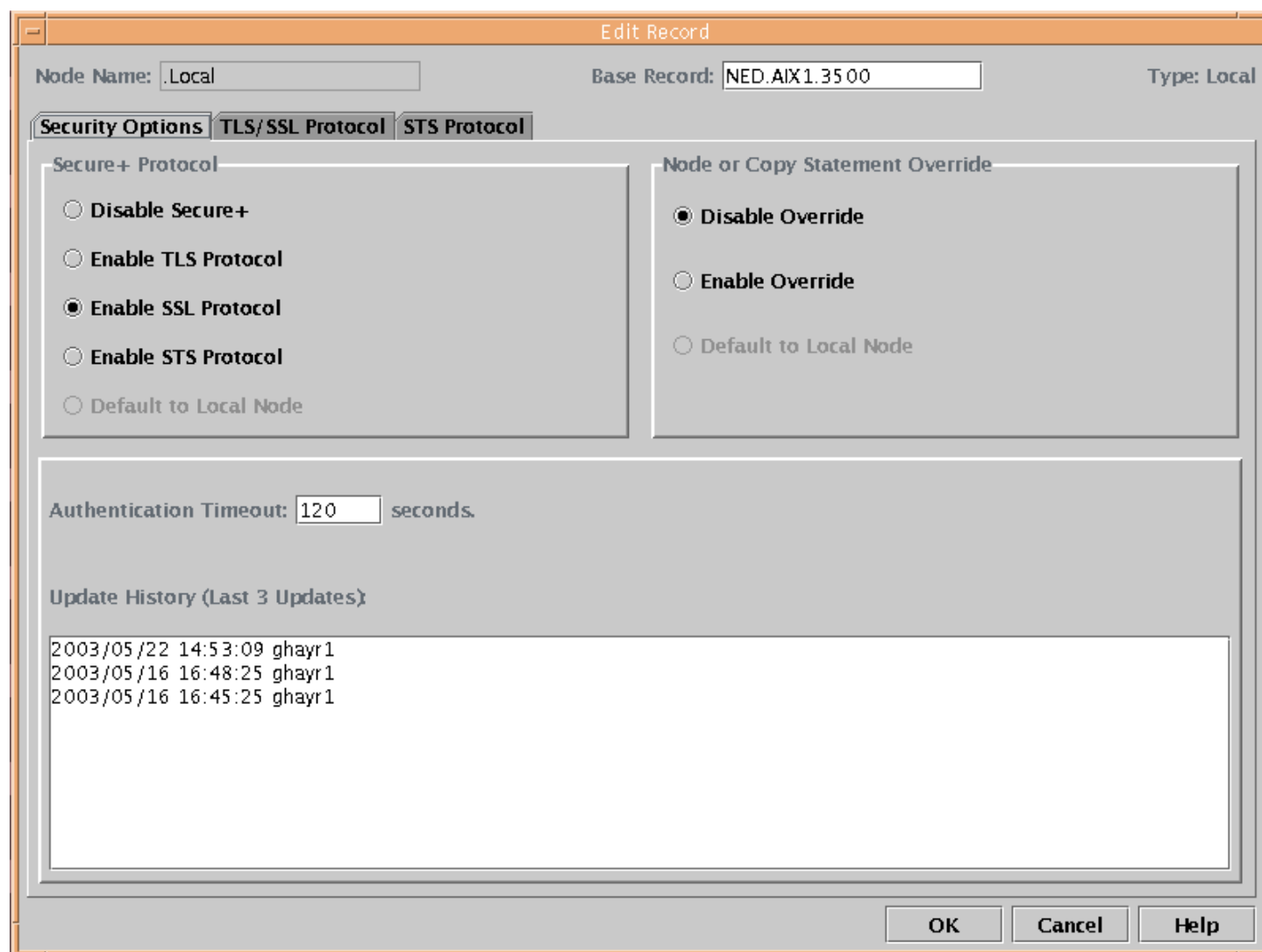
Set the 'Trusted Root Certificate File' and the 'Certificate File' using the files created in the previous steps ( the Passphrase used on Page7 is used here when specifying the 'Certificate File'). Enable all Cipher Suites. Click OK. Secure+ setup complete.

Submit a Connect:Direct 'Pnode=Snode' or 'Loopback' process to prove the connection is secure.

## 5. Setting up Secure+ between Windows and Unix

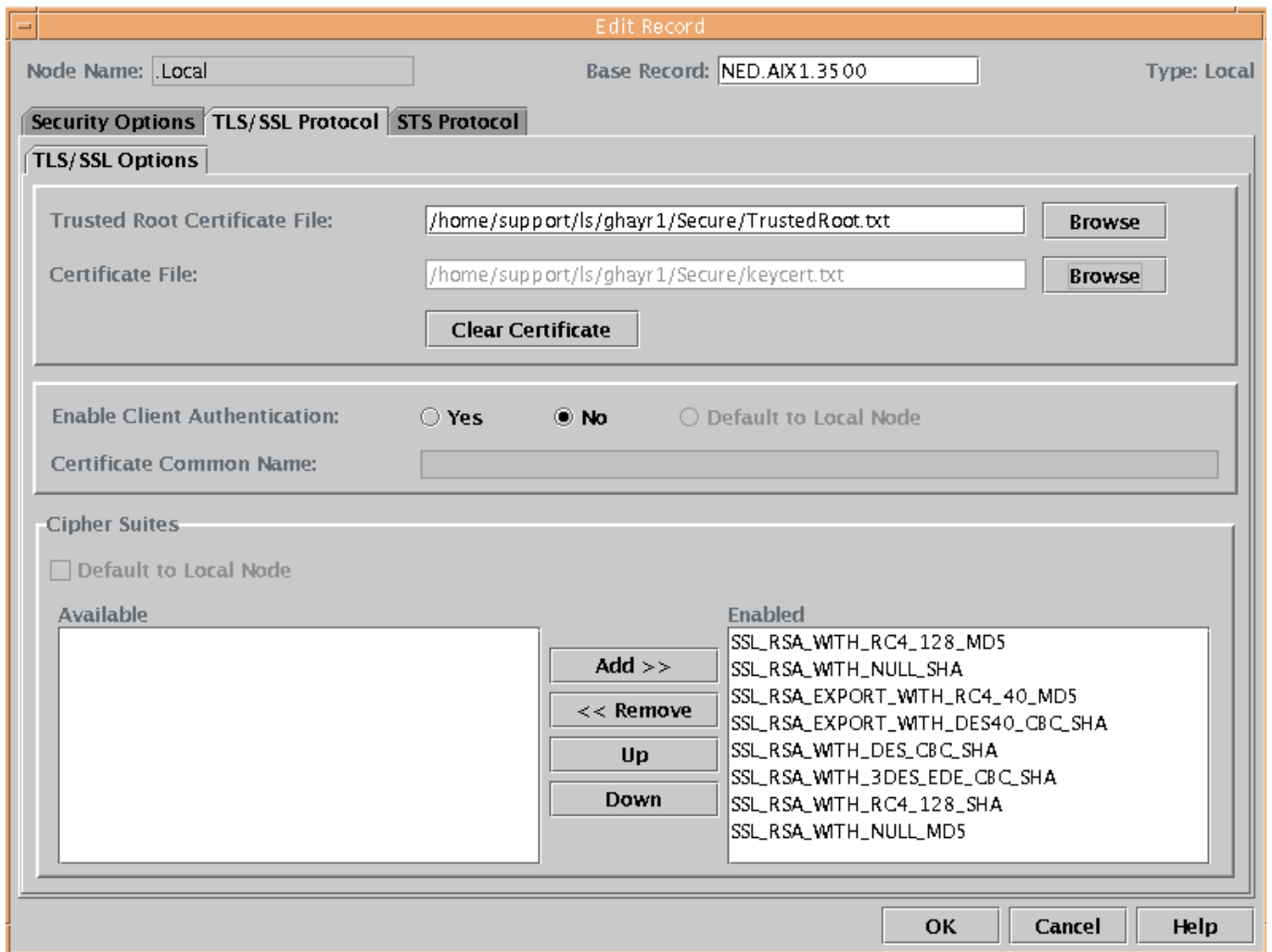
Steps 1 and 2 could now be repeated for setting up the Secure+ files for Unix. Alternatively, ( and **only** to expedite setup), copy the 'TrustedRoot.txt' and 'keycert.txt' file to the Unix system.

Run the Connect:Direct Unix Secure+ Admin Utility. Expand the '.Local' record:



Check the boxes as above, click OK.

Click the 'TLS/SSL Protocol' tab:



Enter the filenames for the ‘Trusted Root Certificate File’ and ‘Certificate File’ that were copied to Unix. Enable all Ciphers. Secure+ setup is complete.

Using either Connect:Direct ( Unix or Windows ) as Pnode, submit a Connect:Direct Process to prove the connection is secure.

## 6. Setting up Secure+ between Windows and OS/390

You will need to use an IBM Utility called 'GSKKYMANT'. See the IBM manual in the 'Related Documents' section for more details on GSKKYMANT.

In this example, Connect:Direct OS/390 will be Pnode.

Copy the file 'TrustedRoot.txt' to OS390.

Start GSKKYMANT:

```
Key Management Menu

Database: /u/ghayr1/ghkey.kdb

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive certificate issued for your request
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length

0 - Exit program

Enter option number (press ENTER to return to previous menu):
===>

ESC=#  1=Help      2=SubCmd      3=HlpRetrn   4=Top        5=Bottom     6=TSO
       7=BackScr   8=Scroll     9=NextSess  10=Refresh   11=FwdRetr   12=Retrieve

INPUT
```

Select option: '7 – Import a certificate'.

```
Key Management Menu

Database: /u/ghayr1/ghkey.kdb

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive certificate issued for your request
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length

0 - Exit program

Enter option number (press ENTER to return to previous menu): 7
Enter import file name (press ENTER to return to menu):
===> TrustedRoot.txt

RUNNING
ESC=4  1=Help    2=SubCmd    3=HlpRetrn  4=Top        5=Bottom    6=TSO
        7=BackScr  8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

Enter the name of the certificate you wish to add:

```
Database: /u/ghayr1/ghkey.kdb

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive certificate issued for your request
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length

0 - Exit program

Enter option number (press ENTER to return to previous menu): 7
Enter import file name (press ENTER to return to menu): TrustedRoot.txt
Enter label (press ENTER to return to menu):
===> trustedselfcert

RUNNING
ESC=4  1=Help    2=SubCmd    3=HlpRetrn  4=Top        5=Bottom    6=TSO
        7=BackScr  8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

Enter a label of your choice. This will be needed when configuring the Secure+ component of Connect:Direct OS/390.

```
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive certificate issued for your request
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length

0 - Exit program

Enter option number (press ENTER to return to previous menu): 7
Enter import file name (press ENTER to return to menu): TrustedRoot.txt
Enter label (press ENTER to return to menu): trustedselfcert

Certificate imported.

Press ENTER to continue.
===>

RUNNING
ESC=␣  1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
        7=BackScr   8=Scroll   9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

Configuration using GSKKYMANT is complete.



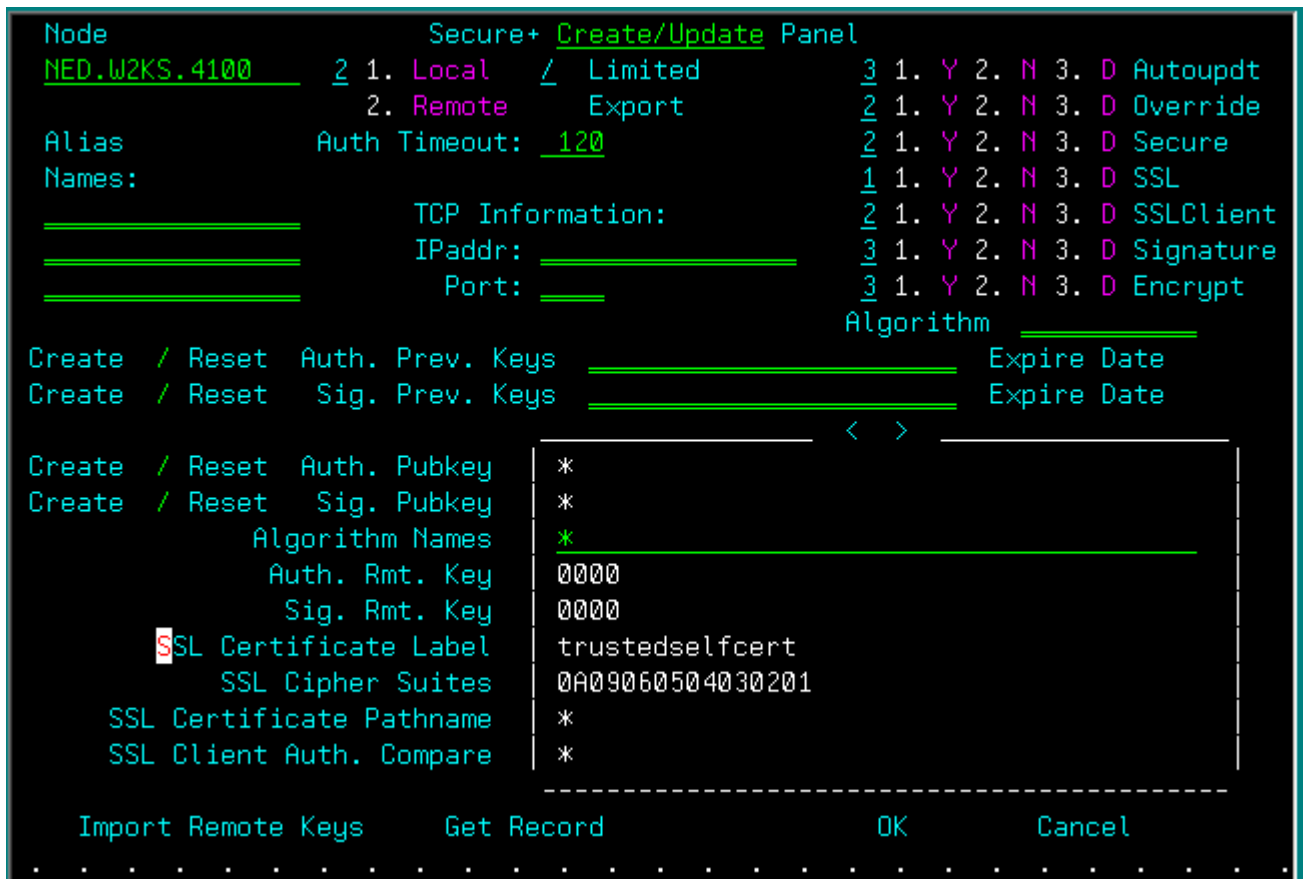
Configure Connect:Direct OS/390 Secure+ . Through the IUI panels, go into Secure+:

```

File Edit Key Management Help
Secure+ Admin Tool: Main Screen Row 1 to 8 of 8
Option ==> | Scroll CSR
Table Line Commands are:
E Export pub. key H view History D Delete node
U Update node I Insert node
Secure
LC Node Name Type 12C Override Encryption Signature Exlimit Autoupd
-----
CERMM.OS390.V42 R YNN Y Y Y Y Y
NED.AIXGH.3100 R **N N * * Y *
NED.AIX1.3301 R **N N * * Y *
NED.AIX1.3400 R **N N * * Y *
NED.AS4.330 R **N N * * Y *
NED.OS390.4200 L YYN Y N N Y Y
NED.W2KS.4000 R YNN Y Y Y Y Y
NED.W2KS.4100 R NYN N * * Y *
***** BOTTOM OF DATA *****

```

In this example, we want to update a Remote Windows Node called: ‘NED.W2KS.4100’.



In the 'SSL Certificate Label' field, enter the label you specified earlier. Enable all Cipher Suites. Click on OK, and save the resulting parmfile. Secure+ setup is complete.

Submit a Connect:Direct process, with Pnode being OS/390 to prove the connection is secure.

Select statistics from Connect:Direct OS/390 for a successful copy will show something like:

```

Menu Utilities Compilers Help
-----
BROWSE      SYS03143.T055526.RA000.GHAYR1.NDMAPI.H01  Line 00000079 Col 001 080
-----
Function    => COPY STEP START           Time           => 06:00:44
Process Name => PROC01                   Process Num    => 2
Step Name   => COPY
Primary Node => NED.OS390.4200          Secondary Node => NED.W2KS.4100
Copy from SNODE to PNODE
Source DSN   => C:\DELETEME.TXT
Destination DSN => GHAYR1.PS.TEST
              SSL Enabled      = Yes
              SSL Ciphersuite = SSL_RSA_WITH_RC4_128_SHA
-----
Function    => COPY                       Start Time    => 06:00:44
Process Name => PROC01                   Stop Time     => 06:00:51
Process Num => 2                         Comp Code     => 00000000
                                                Comp Msg      => SCPA000I
Userid      => GHAYR1
Secondary   => NED.W2KS.4100           Step Name     => COPY
                                                V2 Buffer Size => 4,096
Command ==> 
-----
Scroll ==> CSR
-----

```

This concludes the use of Certificate Wizard in generating Self Signed Certificates, and the subsequent configuration of Connect:Direct to use Secure+.