

Sterling Commerce Certificate Wizard 1.1.00

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

Status: Approved

Author: Gurmit Hayre

Date: 25th 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).

<u>1. Generate Self-Signed Certificate.</u>

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:

| Zertificate Wizard | | | | | | |
|--------------------|-----------------|---------------------------------------|----------------------------|---|------|-----|
| | Key Certificate | Verify Certificate | Self-S | inned Certificate | | |
| | We | lcome | | Generate CSR | _ | |
| | | Please enter the fo Common f Co | llowing łame: untry: | ninformation about your site: Test-Windows2K-Server United Kingdom(Great Britain) | • | |
| | | State/Pro | vince: | Middlesex | • | |
| | | City/Lo | cality: | Uxbridge | | |
| | Orga | nization/Company I | lame: | Sterling Commerce | | |
| | | Organizatio | n Unit: | Support | | |
| | | Email Add | lress: | connect_eurosupp@stercomm. | corr | |
| | | N | ext | Cancel | | |
| | | | | | | |
| | | | | Help |) E | xit |

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

| 🛃 Certificate Wizard | | | |
|----------------------|------------------------------------|-------------------------|------|
| | Key Certificate Verify Certificate | Self-Signed Certificate | |
| | Welcome | Generate CSR | |
| | Certificate Type | ○ Client ○ Custom | 1 |
| | Certificate Usage | | |
| | ☑ DigitalSignature | NonRepudiation | |
| | KeyEncipherment | DataEncipherment | |
| es l | ✓ KeyAgreement | KeyCertSign | |
| | CrlSign | EncipherOnly | |
| | DecipherOnly | | |
| | | | - |
| | Back | Next Cancel | |
| | | | |
| | | Help | Exit |

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

| Zertificate Wizard | | | | _O× |
|--------------------|------------------------------------|-----------|-----------------|----------|
| | Key Certificate Verify Certificate | Self-Sigr | ned Certificate | |
| | Welcome | | Generate CSR | |
| | Private Key | Length: | 768 💌 | |
| | Certificate Serial N | lumber: | 123456789 | |
| | How long is Certificat | e Valid: | 28 | |
| - Color | Passp | hrase: | ***** |] |
| | Confirm Passp | hrase: | ***** |] |
| | Back | Next | Cancel | |
| | | | H | elp Exit |

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

The Passphrase you specify here will be used later.

| 🛃 Certificate Wizard | | | _ | |
|----------------------|--|--|-------------------------|--|
| | Key Certificate Verify Certificate | Self-Signed Certificate | | |
| | Welcome | Gene | rate CSR | |
| | Specify the private key fi Key file name: CAS Specify the Self-Signed Cert file name: CAS Back | le name. Secure\privkey.bt Certificate file name. Secure\cert.crt | Browse Browse Help Exit | |

Specify a location for the Private key and the Certificate.



Check the details.

Click 'Finish'.

| 🔀 Certificate Wizard | | | _ IX |
|----------------------|--|-------------------------|-----------|
| | Key Certificate Verify Certificate S | Self-Signed Certificate | |
| | Welcome | Generate (| CSR |
| | You have entered the follow Common Name:Test-Wind Country:United Kinαdom(G Message A self-signed certificate OK Certificate Usage:{0, 2, 3, 4 Key file name:C:\Secure\pri Certific name:C:\Secure\pri Certific name:C:\Secure\pri Certific name:C:\Secure\pri Certific name:C:\Secure\pri Certific name:C:\Secure\pri Certific name:C:\Secure\pri | e has been created. | |
| | | | |
| | | | |
| | | | Help Exit |

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 :

| Key Certificate Verify Certificate Self-Signed Certificate Welcome Generate CSR |
|--|
| |
| Specify the private key file name. C:1Secure\privkey.txt Browse C:1Secure\cert.crt Browse C:1Secure\keycert.file name. C:1Secure\keycert.txt Browse C:1Secure\keycert.txt Browse |

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:

| Zertificate Wizard | | | | | |
|---------------------------------------|--|--|---|--|------|
| | Key Certificate | Verify Certificate | Self-Signed Certificate | | |
| | Wel | lcome | Gener | rate CSR | |
| | Specify verify (File, ce signat file, | y the name of Key C keycert.txt and trust artificates in that file ure. The passphrae | Certificate file and the Trus ed.bd). If you only identify t will be verified against tin se is required to verify the f | ted Root file to he Trusted Root ne and Key Certificate | |
| | | Passphrase: *** | ***** | | |
| | | Keycert: C:V | Secure\keycert.txt | Browse | |
| | С | ertificate File: C:V | Secure\cert.crt | Browse | |
| ATT THE ALL OF | Trus | sted Root File: C:\ | Secure\TrustedRoot.txt | Browse | |
| and "Anny" and have a fermionic line. | | | | Verify | |
| | | | | | |
| | | | | Help | Exit |

Enter the filenames from Steps 1 and 2.

If verification is successful, the following screens appear:

| 🔀 Certificate Wizard | | | | <u>_ ×</u> |
|----------------------|--|--|--|--------------|
| | Key Certificate Verify Certificate Welcome | Self-Signed Certificate Genera | ate CSR | |
| | Message Active date is:Thu May 22 Expiration date is:Thu Ju Issuer Info: Test-Window Certificate Infomation: Country: GB State: Middlesex City/Locality: Uxbridge Organization Unit: Sup Organization: Sterling Common Name: Test- Serial number: 12345 Signature algorithm: S Version number: 2 Key certificate file verific OK | 2 11:48:59 BST 2003 n 19 11:48:59 BST 2003 vs2K-Server oport Commerce Windows2K-Server 6789 SHA1withRSA ation succeeded. | ed Root file to e Trusted Root e and ey Certificate Browse Browse Verify | |
| | | | Help | Exit |

| 🔀 Certificate Wizard | | | | _ | |
|----------------------|--|--|---|--|---|
| | Key Certificate | Verify Certificate | Self-Signed Certificate | | |
| | We | lcome | Gene | erate CSR | L |
| | Specify verify (File, c signal Messag | iy the name of Key (keycert.bt and trust ertificates in that file ture. The passphras e Checking root certif OK Certificate File: C:10 sted Root File: C:10 | Certificate file and the True ed.txt). If you only identify will be verified against ti se is required to verify the Cates succeeded. Gecure\cert.crt Secure\TrustedRoot.txt | sted Root file to the Trusted Root me and Key Certificate Browse Browse Verify | |
| | | | | Help Exit | |

Verification is done.

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

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

| Secure + Admin Tool - [E:\CD4100\Server\Secure +\nodes] | | | | | | | | | | |
|---|-----------|---------|----------|----------|------------|------------|-----------|---------|--------|-------------|
| File Edit Key Man | agement H | lelp | | | | | | | | |
| Node Name Filter: | | | | | | | | | | |
| Node Name | Туре | 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 | * | Υ | * | |
| NED.W2KS.4100 | R | * | * | | * | N | * | Υ | * | |
| | | | | | | | | | | |

Expand the '.Local' record:

| <mark>la</mark> s i | 🔒 Edit Record | | × | ١× |
|---------------------|---|---------------------------------|-------------|----------|
| File | Node Name: Local Ba | se Record: NED.W2KS.4100 | Type: Local | <u> </u> |
| Node | Security Options TLS/SSL Protocol STS Protocol | | | |
| | Secure+ Protocol | Node or Copy Statement Override | | |
| NED./ | C Disable Secure+ | Disable Override | | |
| NED.(NED.) | C Enable TLS Protocol | C Enable Override | | |
| | Enable SSL Protocol | | | |
| | C Enable STS Protocol | C Default to Local Node | | |
| | C Default to Local Node | | | |
| | Authentication Timeout: 120 seconds. | | | |
| | Update History (Last 3 Updates): | | | |
| | 2003/05/22 17:02:03 ctsuplv11 2003/05/22 16:29:45 ctsuplv11 2003/05/22 15:56:21 ctsuplv11 | | | |
| | | | | |
| | <u></u> | OK Cancel | Help | |

Check the boxes as above. Click OK.

Click the 'TLS/SSL Protocol' tab.

| 🔒 Edit Record | | × |
|--|---|-------------|
| Node Name: Local | Base Record: NED.W2KS.4100 | Type: Local |
| Security Options TLS/SSL Protocol TLS/SSL Options | STS Protocol | |
| Trusted Root Certificate File: Certificate File: | C: \Secure \TrustedRoot.txt Browse C: \Secure \keycert.txt Browse Clear Certificate | |
| Enable Client Authentication: Certificate Common Name: Cipher Suites | O Yes O No O Default to Local Node | |
| Available | Add >> SSL_RSA_WITH_NULL_MD5 Add >> SSL_RSA_WITH_NULL_SHA < | |
| | OK Cancel | Help |

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:

| Edi | t Record |
|---|--|
| Node Name: .Local Base | Record: NED.AIX1.3500 Type: Local |
| Security Options TLS/SSL Protocol STS Protocol Secure + Protocol Disable Secure + Enable TLS Protocol Enable SSL Protocol Enable STS Protocol Default to Local Node | Node or Copy Statement Override Disable Override Enable Override Default to Local Node |
| Authentication Timeout: 120 seconds. | |
| Update History (Last 3 Updates) 2003/05/22 14:53:09 ghayr1 2003/05/16 16:48:25 ghayr1 2003/05/16 16:45:25 ghayr1 | |
| | OK Cancel Help |

Check the boxes as above, click OK.

Click the 'TLS/SSL Protocol' tab:

| - | Edit Record | |
|-------------------------------------|--|-------------|
| Node Name: .Local | Base Record: NED.AIX1.3500 | Type: Local |
| Security Options TLS/SSL Protocol S | TS Protocol | |
| TLS/SSL Options | | |
| Trusted Root Certificate File: | /home/support/ls/ghayr1/Secure/TrustedRoot.txt Browse | 7 [] |
| Certificate File: | /home/support/ls/dhayr1/Secure/keycert.txt Browse | - |
| | | |
| | | |
| Enable Client Authentication: | ○ Yes | [|
| Certificate Common Name | | |
| | | |
| Cipher Suites | | 1 |
| Default to Local Node | | |
| Available | Enabled SSL RSA_WTH_RC4_128_MD5 | |
| | Add >> SSL_RSA_WITH_NULL_SHA | |
| | SSL_RSA_EXPORT_WITH_RC4_40_MD5 | |
| | Up SSL_RSA_WITH_DES_CBC_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA | |
| | Down SSL_RSA_WITH_RC4_128_SHA | |
| | | |
| | | |
| | OK Cancel | Help |

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 'GSKKYMAN'. See the IBM manual in the 'Related Documents' section for more details on GSKKYMAN.

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

Copy the file 'TrustedRoot.txt' to OS390.

Start GSKKYMAN:

| | Key Manageme | nt Menu | | | | |
|--|---|--|--|--|------------------------|----------------------|
| | Database: /u | /ghayr1/ghk | ey.kdb | | | |
| 1 - 2 - 3 - 5 - 6 - 7 - 8 - 9 - 10 - 11 - | Manage keys Manage certi Manage certi Create new c Receive cert Create a sel Import a cer Import a cer Show the def Store databa Show databas | and certific ficates ficate reque ertificate issu f-signed cent tificate tificate tificate and ault key se password e record len | cates ests request ued for your rtificate d a private ngth | request <ey< th=""><th></th><th></th></ey<> | | |
| 0 - | Exit program | I | | | | |
| Enter (===> | option number | (press ENTI | ER to return | to previous | menu): | TNDUT |
| ESC=¢ | 1=Help 7=BackScr | 2=SubCmd 8=Scroll | 3=HlpRetrn 9=NextSess | 4=Top 10=Refresh | 5=Bottom 11=FwdRetr | 6=TSO 12=Retrieve |

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
       1=Help
ESC=¢
                   2=SubCmd
                                3=HlpRetrn 4=Top
                                                        5=Bottom
                                                                    6=TS0
       7=BackScr 8=Scroll
                               9=NextSess 10=Refresh 11=FwdRetr 12=Retrieve
```

Enter the name of the certificate you wish to add:

| I | Database: /u/ | ∕ghayr1∕ghke | y.kdb | | | |
|---|---|--|--|-----------------------------------|--------------------------|---------------------------------|
| 1 - 1 2 - 1 3 - 1 4 - 1 5 - 1 6 - 1 7 - 8 - 9 - 2 10 - 2 11 - 2 | Manage keys a Manage certi Create new ca Receive cert: Create a sel Import a cert Show the defa Store database | and certific ficates ficate reque: ertificate re ificate issu f-signed cer tificate tificate ault key se password e record len | ates sts equest ed for your tificate a private # gth | request «ey | | |
| 0 - 1 | Exit program | | | | | |
| Enter o Enter in Enter la | otion number mport file na abel (press B | (press ENTE) ame (press E) ENTER to ret rt | R to return NTER to retu urn to menu) | to previous urn to menu)): | menu): 7 : TrustedRoo | t.t×t |
| ESC=¢ | 1=Help 7=BackScr | 2=SubCmd 8=Scroll | 3=HlpRetrn 9=NextSess | 4=Top 10=Refresh | 5=Bottom 11=EudBetr | RUNNING 6=TSO 12=Retrieve |

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

| 2 | - Manage certi | ficates | | | | | |
|-------------------------|--|---|---|--|------------------------------------|-------------|--|
| 3 | 3 - Manage certificate requests | | | | | | |
| 4 | 4 - Create new certificate request | | | | | | |
| 5 | - Receive certificate issued for your request | | | | | | |
| 6 | - Create a sel | f-signed cer | tificate | | | | |
| 7 | - Import a cer | tificate | | | | | |
| 8 | - Import a cer | tificate and | a private ⊧ | ey | | | |
| 9 | - Show the def | ault key | | | | | |
| 10 | - Store databa | se password | | | | | |
| 11 | - Show databas | e record ler | igth | | | | |
| 0 | - E×it program | | | | | | |
| Enter Enter Enter | option number import file n label (press | (press ENTE ame (press E ENTER to ret | R to return NTER to retu urn to menu) | to previous urn to menu) : trustedse | menu): 7 : TrustedRoo lfcert | t.t×t | |
| Certi | ficate importe | d. | | | | | |
| | | | | | | | |
| Press ===> | ENTER to cont | inue. | | | | | |
| | | | | | | RUNNING | |
| ESC=¢ | 1=Help | 2=SubCmd | 3=HlpRetrn | 4=Top | 5=Bottom | 6=TS0 | |
| | 7=BackScr | 8=Scroll | 9=NextSess | 10=Refresh | 11=FwdRetr | 12=Retrieve | |

Configuration using GSKKYMAN is complete.

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

| <u>F</u> ile <u>E</u> dit <u>K</u> ey Management <u>H</u> elp | | | | | | | |
|---|--------------------------|---------|------------|-------------|------------|------------------|----------------------------|
| Option ===> | Seci | ure+ Ad | lmin Tool: | Main Screen | 1 | Row 1 t _ Scr | o 8 of 8 oll <u>CSR</u> |
| | Table Line Commands are: | | | | | | |
| E Export pub. key | ł | l vieω | History | D De | elete node | | |
| U Update node | | I Inser | t node | | | | |
| | | | | | | | |
| | - | Secure | | | . . | | <u>.</u> |
| LC Node Name | Type | 120 | Uverride | Encryption | Signature | Exlimit | Autoupd |
| CERMM.0S390.V42 | R | YNN | Y | Y | Y | Y | Y |
| NED.AIXGH.3100 | R | жжN | Ν | * | * | Y | * |
| NED.AIX1.3301 | R | **1 | Ν | * | * | Y | * |
| NED.AIX1.3400 | R | жж№ | Ν | * | * | Y | * |
| NED.AS4.330 | R | **! | М | * | * | Y | * |
| NED.0S390.4200 | L | YYN | Y | Ν | Ν | Y | Y |
| NED.W2KS.4000 | R | YNN | Y | Y | Y | Y | Y |
| NED.W2KS.4100 | R | NYN | М | * | * | Y | * |
| жжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжж | | | | | | | |
| | | | | | | | |
| | | | | | | | |

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

| Node Secure- | • <u>Create/Update</u> Pan | el |
|---------------------------------|----------------------------|----------------------------------|
| <u>NED.W2KS.4100 2</u> 1. Local | <u>/</u> Limited | <u>3</u> 1. Y 2. N 3. D Autoupdt |
| 2. Remote | Export | <u>2</u> 1. Y 2. N 3. D Override |
| Alias Auth Timeout: | 120 | <u>2</u> 1. Y 2. N 3. D Secure |
| Names: | | <u>1</u> 1. Y 2. N 3. D SSL |
| TCP Info | ormation: | 2 1. Y 2. N 3. D SSLClient |
| IPaddr: | | 3 1. Y 2. N 3. D Signature |
| Port: | | 3 1. Y 2. N 3. D Encrypt |
| | | Algorithm |
| Create / Reset Auth. Prev. Key | ,s | Expire Date |
| Create / Reset Sig. Prev. Kei | ls | Expire Date |
| | | < > |
| Create / Reset Auth. Pubkey | * | |
| Create / Reset Sig. Pubkey | * | |
| Algorithm Names | * | |
| Auth. Rmt. Key | 0000 | |
| Sig. Rmt. Key | 0000 | |
| SSL Certificate Label | trustedselfcert | |
| SSL Cipher Suites | 0A09060504030201 | |
| SSL Certificate Pathname | * | |
| SSL Client Auth. Compare | * | |
| | | ' |
| Import Remote Keys Get Re | ecord | OK Cancel |
| | | |

In the 'SSL Certficate 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:



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