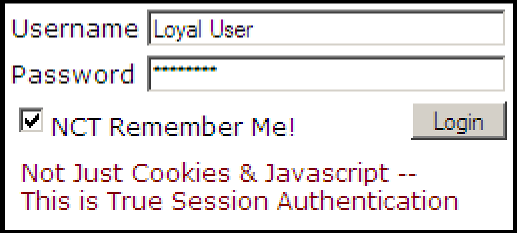
Creating an SSL Certificate for IBM Lotus Domino Servers

Step by Step – Courtesy of Northern Collaborative Technologies



Username Loyal User

Password *********

☑ NCT Remember Me!

Not Just Cookies & Javascript --
This is True Session Authentication

Sponsored by: NCT Remember Me!

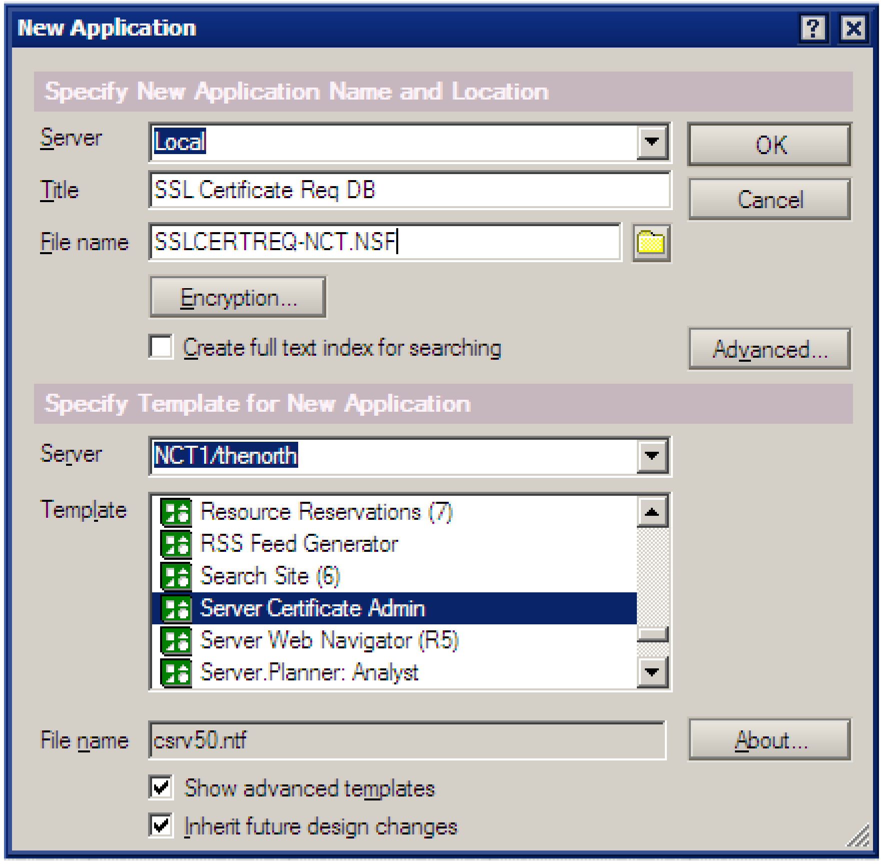
Automatically log-in returning Domino users

Installs in Minutes to existing or new web pages
Does not require a DSAPI filter
Fully Supports ACLs, Reader Names, Groups, etc.
Fully Supports Multi-Server Session Based Authentication

http://www.Thenorth.com/ncthome.nsf/html/RememberMe

1. Create A Cert Admin Database

- The template is on your server
- Click the advanced templates button



New Application

Specify New Application Name and Location

Server: Local

Title: SSL Certificate Req DB

File name: SSLCERTREQ-NCT.NSF

☐ Create full text index for searching

Specify Template for New Application

Server: NCT1/thenorth

Template:
- Resource Reservations (7)
- RSS Feed Generator
- Search Site (6)
- Server Certificate Admin
- Server Web Navigator (R5)
- Server.Planner: Analyst

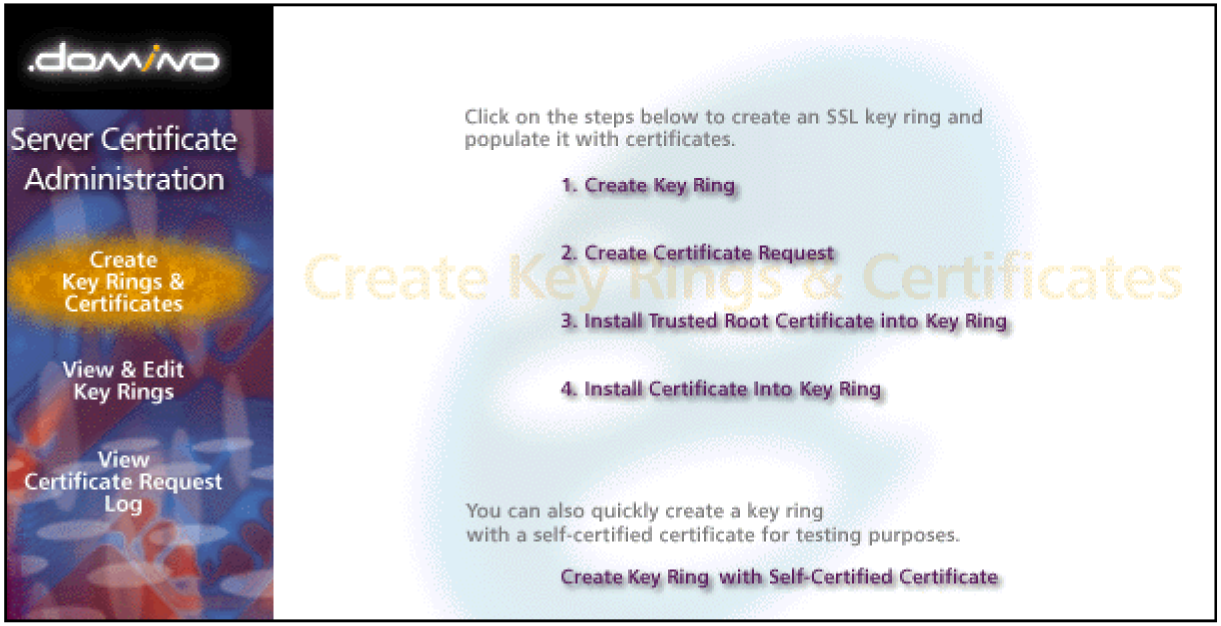
File name: csrv50.ntf

☑ Show advanced templates

☑ Inherit future design changes

Open the Database

- See the Nice Menu


.domino
Server Certificate Administration
Create Key Rings & Certificates
View & Edit Key Rings
View Certificate Request Log
Create Key Rings & Certificates

Click on the steps below to create an SSL key ring and populate it with certificates.

1. Create Key Ring
2. Create Certificate Request
3. Install Trusted Root Certificate into Key Ring
4. Install Certificate Into Key Ring

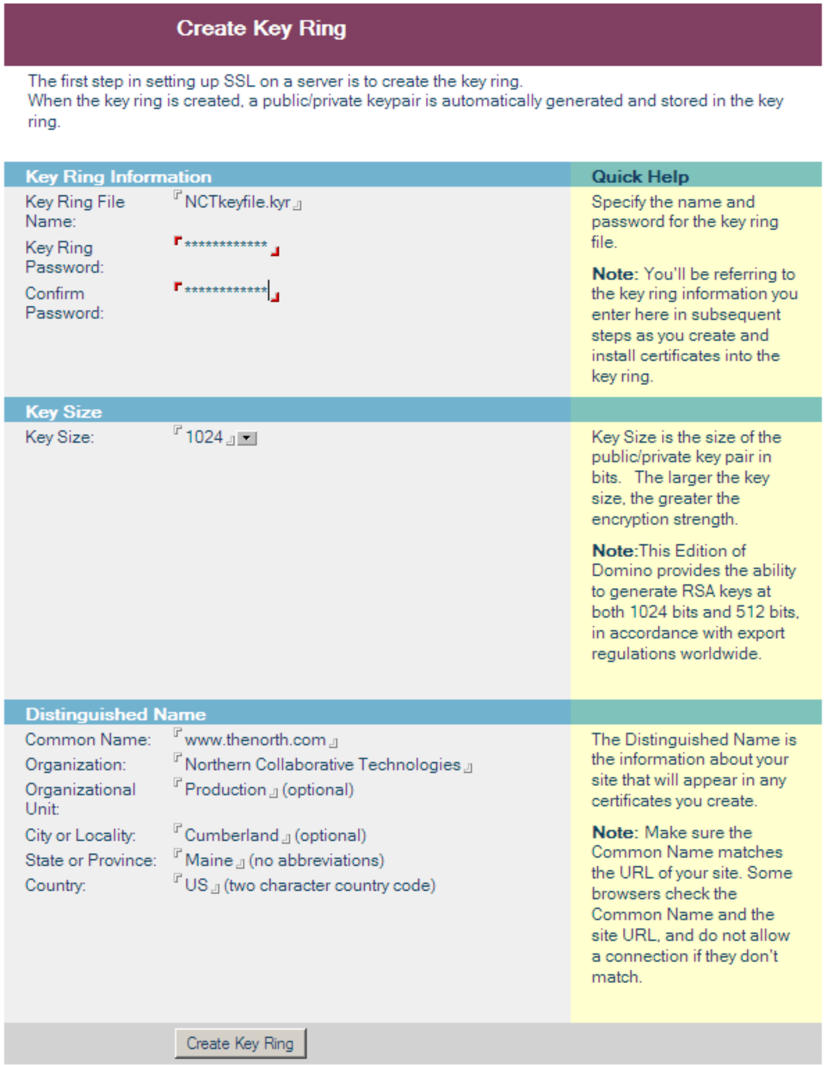
You can also quickly create a key ring with a self-certified certificate for testing purposes.

Create Key Ring with Self-Certified Certificate

Create A Key Ring

- This file, and its sibling will be copied to your Domino server when you're done. Use a good password – you won't have to enter it when you restart Domino.

- The entries in these fields are picky. Make sure to read the help line as you're entering the information



Create Key Ring

The first step in setting up SSL on a server is to create the key ring.
When the key ring is created, a public/private keypair is automatically generated and stored in the key ring.

Key Ring Information

Key Ring File Name:	NCTkeyfile.kyr
Key Ring Password:	*************
Confirm Password:	*************

Quick Help

Specify the name and password for the key ring file.

Note: You'll be referring to the key ring information you enter here in subsequent steps as you create and install certificates into the key ring.

Key Size

Key Size:	1024

Key Size is the size of the public/private key pair in bits.   The larger the key size, the greater the encryption strength.

Note:This Edition of Domino provides the ability to generate RSA keys at both 1024 bits and 512 bits, in accordance with export regulations worldwide.

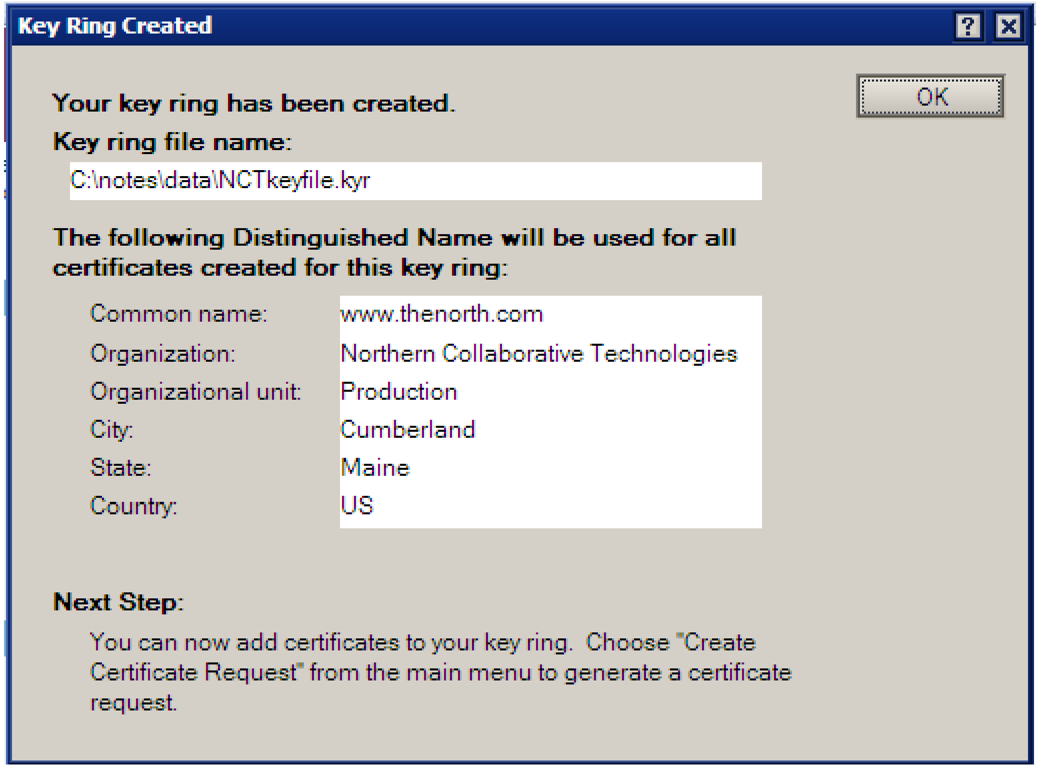
Distinguished Name

Common Name:	www.thenorth.com
Organization:	Northern Collaborative Technologies
Organizational Unit:	Production (optional)
City or Locality:	Cumberland (optional)
State or Province:	Maine (no abbreviations)
Country:	US (two character country code)

The Distinguished Name is the information about your site that will appear in any certificates you create.

Note: Make sure the Common Name matches the URL of your site. Some browsers check the Common Name and the site URL, and do not allow a connection if they don't match.

Hooray! You have a keyring!



Your key ring has been created.

Key ring file name:

C:\notes\data\NCTkeyfile.kyr

The following Distinguished Name will be used for all certificates created for this key ring:

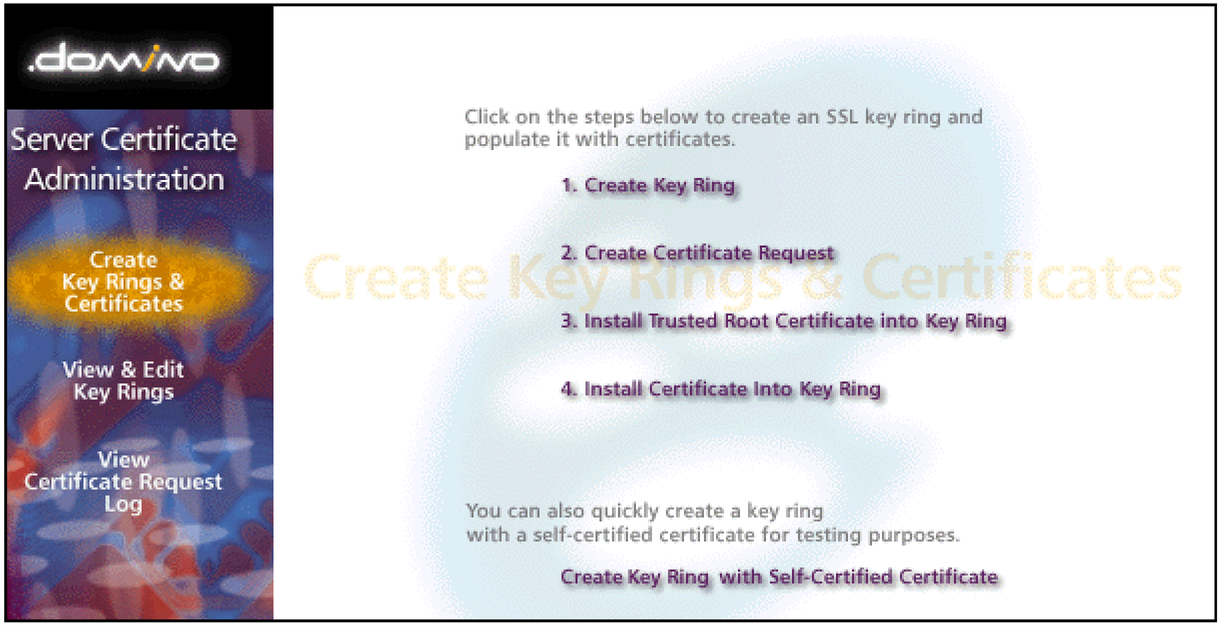
Common name:	www.thenorth.com
Organization:	Northern Collaborative Technologies
Organizational unit:	Production
City:	Cumberland
State:	Maine
Country:	US

Next Step:

You can now add certificates to your key ring. Choose "Create Certificate Request" from the main menu to generate a certificate request.

Back to the Menu

- Now Create A Certificate Request



Click on the steps below to create an SSL key ring and populate it with certificates.

1. Create Key Ring
2. Create Certificate Request
3. Install Trusted Root Certificate into Key Ring
4. Install Certificate Into Key Ring

You can also quickly create a key ring
with a self-certified certificate for testing purposes.

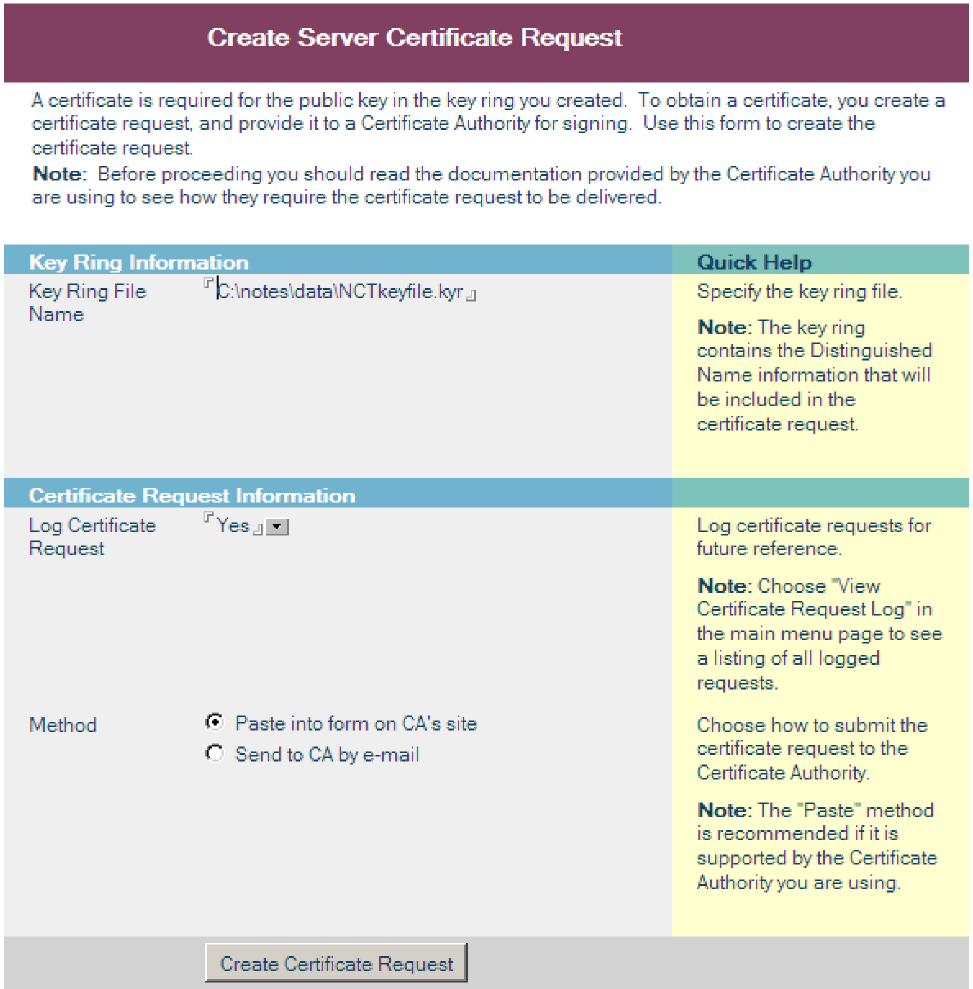
Create Key Ring with Self-Certified Certificate

.domino
Server Certificate Administration
Create Key Rings & Certificates
View & Edit Key Rings
View Certificate Request Log
Create Key Rings & Certificates

Creating A Certificate Request

- Make sure to log the request, so you can get back to it if you need a new copy of the request key.

- You almost always will be pasting this value into the CA's website



Create Server Certificate Request

A certificate is required for the public key in the key ring you created. To obtain a certificate, you create a certificate request, and provide it to a Certificate Authority for signing. Use this form to create the certificate request.

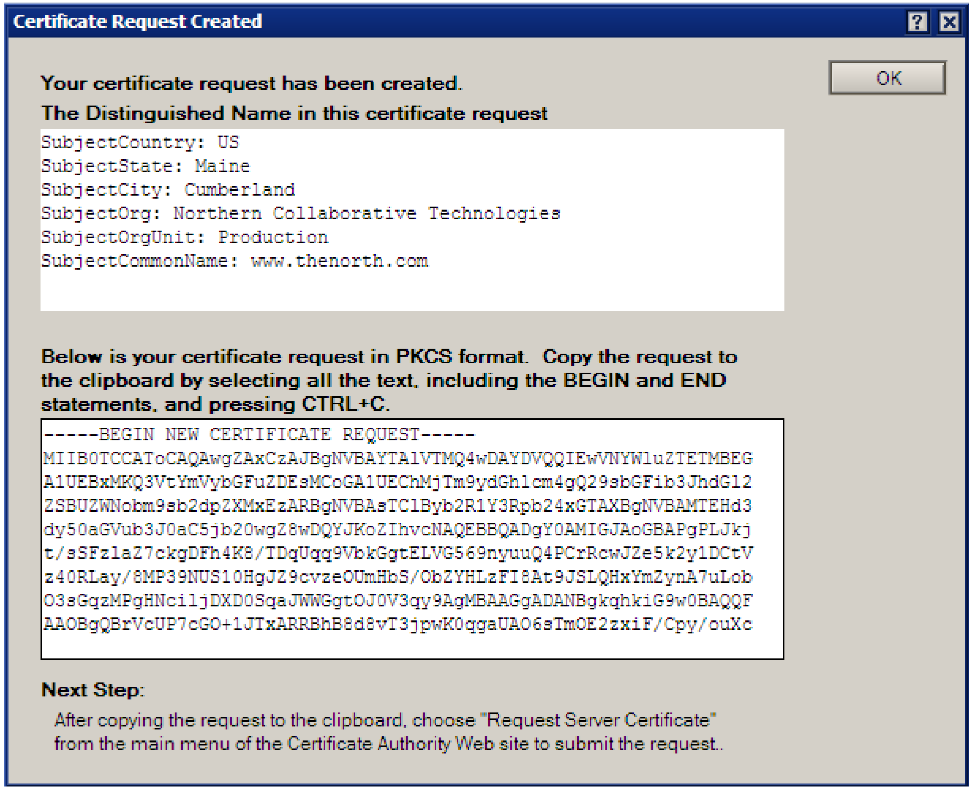
Note: Before proceeding you should read the documentation provided by the Certificate Authority you are using to see how they require the certificate request to be delivered.

Key Ring Information		**Quick Help**
Key Ring File Name	C:\notes\data\NCTkeyfile.kyr	Specify the key ring file. **Note**: The key ring contains the Distinguished Name information that will be included in the certificate request.
Certificate Request Information		
Log Certificate Request	Yes ▾	Log certificate requests for future reference. **Note**: Choose "View Certificate Request Log" in the main menu page to see a listing of all logged requests.
Method	● Paste into form on CA's site ○ Send to CA by e-mail	Choose how to submit the certificate request to the Certificate Authority. **Note**: The "Paste" method is recommended if it is supported by the Certificate Authority you are using.

Copy Your Certificate Request

- You want the whole text from "Begin" to "End" including those lines

- If you click ok and need to get this back, its in the log document



Your certificate request has been created.

The Distinguished Name in this certificate request

```
SubjectCountry: US
SubjectState: Maine
SubjectCity: Cumberland
SubjectOrg: Northern Collaborative Technologies
SubjectOrgUnit: Production
SubjectCommonName: www.thenorth.com
```

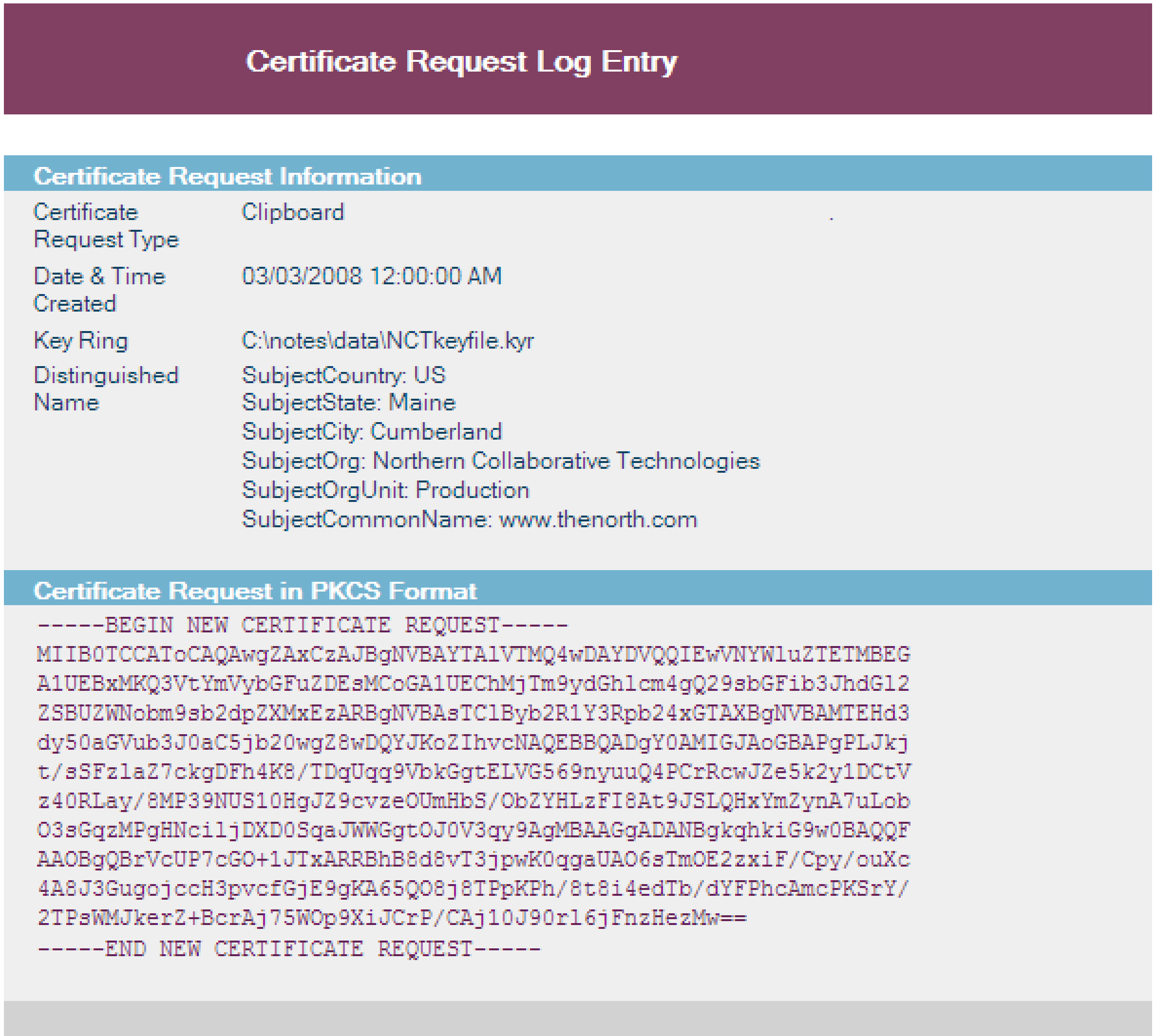
Below is your certificate request in PKCS format. Copy the request to the clipboard by selecting all the text, including the BEGIN and END statements, and pressing CTRL+C.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB0TCCAToCAQAwgZAxCzAJBgNVBAYTAlVTMQ4wDAYDVQQIEwVNYWluZTETMBEG
A1UEBxMKQ3VtYmVybGFuZDEsMCoGA1UEChMjTm9ydGhlcm4gQ29sbGFib3JhdGl2
ZSBUZWNobm9sb2dpZXMxEzARBgNVBAsTClByb2R1Y3Rpb24xGTAXBgNVBAMTEHd3
dy50aGVub3J0aC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAPgPLJkj
t/sSFzlaZ7ckgDFh4K8/TDqUqq9VbkGgtELVG569nyuuQ4PCrRcwJZe5k2y1DCtV
z40RLay/8MP39NUS10HgJZ9cvzeOUmHbS/ObZYHLzFI8At9JSLQHxYmZynA7uLob
O3sGqzMPgHNciljDXD0SqaJWWGgtOJ0V3qy9AgMBAAGgADANBgkqhkiG9w0BAQQF
AAOBgQBrVcUP7cGO+1JTxARRBhB8d8vT3jpwK0qgaUAO6sTmOE2zxiF/Cpy/ouXc
```

Next Step:

After copying the request to the clipboard, choose "Request Server Certificate" from the main menu of the Certificate Authority Web site to submit the request.

Here’s the Log Entry



Certificate Request Log Entry

Certificate Request Information

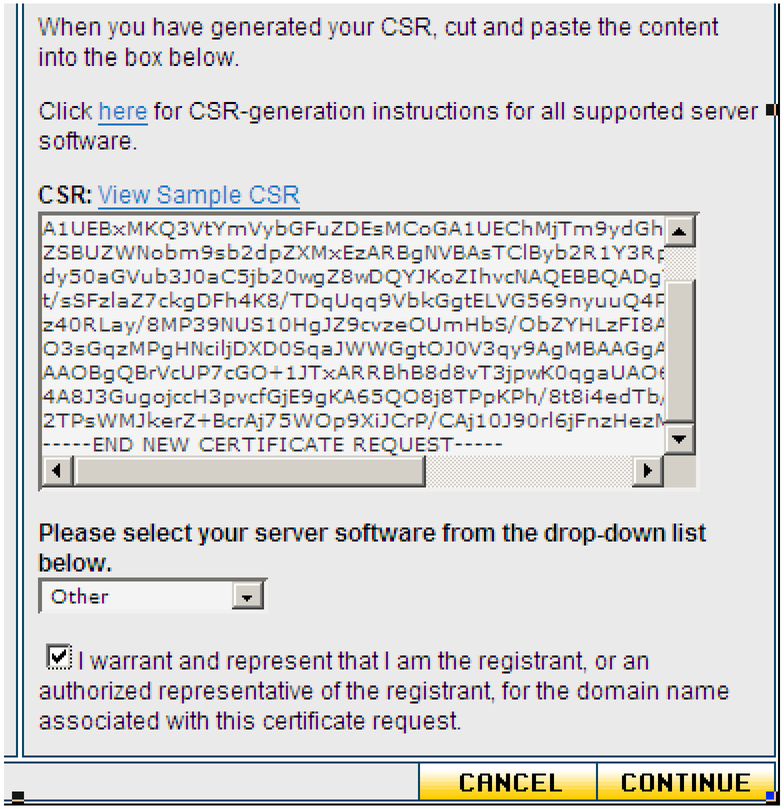
Certificate Request Type	Clipboard
Date & Time Created	03/03/2008 12:00:00 AM
Key Ring	C:\notes\data\NCTkeyfile.kyr
Distinguished Name	SubjectCountry: US SubjectState: Maine SubjectCity: Cumberland SubjectOrg: Northern Collaborative Technologies SubjectOrgUnit: Production SubjectCommonName: www.thenorth.com

Certificate Request in PKCS Format

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB0TCCAToCAQAwgZAxCzAJBgNVBAYTAlVTMQ4wDAYDVQQIEwVNYWluZTETMBEG
A1UEBxMKQ3VtYmVybGFuZDEsMCoGA1UEChMjTm9ydGhlcm4gQ29sbGFib3JhdGl2
ZSBUZWNobm9sb2dpZXMxEzARBgNVBAsTClByb2R1Y3Rpb24xGTAXBgNVBAMTEHd3
dy50aGVub3J0aC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAPgPLJkj
t/sSFzlaZ7ckgDFh4K8/TDqUqg9VbkGgtELVG569nyuuQ4PCrRcwJZe5k2y1DCtV
z40RLay/8MP39NUS10HgJZ9cvzeOUmHbS/ObZYHLzFI8At9JSLQHxYmZynA7uLob
O3sGqzMPgHNciljDXD0SqaJWWGgtOJ0V3qy9AgMBAAGgADANBgkqhkiG9w0BAQQF
AAOBgQBrVcUP7cGO+1JTxARRBhB8d8vT3jpwK0qgaUAO6sTmOE2zxiF/Cpy/ouXc
4A8J3GugojccH3pvcfGjE9gKA65QO8j8TPpKPh/8t8i4edTb/dYFPhcAmcPKSrY/
2TPsWMJkerZ+BcrAj75WOp9XiJCrP/CAj10J90rl6jFnzHezMw==
-----END NEW CERTIFICATE REQUEST-----
```

Now Go to the Certificate Authority

- Each CA will have their own byzantine process by which you must submit the certificate request.
- Most will need to verify you are who say you are.
- This is a tricky step, and you have to deal with poorly designed CA web sites.
- GoDaddy, Verisign, and InstantSSL are three of many CA's to pick from.



When you have generated your CSR, cut and paste the content into the box below.

Click here for CSR-generation instructions for all supported server software.

CSR: View Sample CSR

```
A1UEBxMKQ3VtYmVybGFuZDEsMCoGA1UEChMjTm9ydGh
ZSBUZWNobm9sb2dpZXMxEzARBgNVBAsTClByb2R1Y3Rp
dy50aGVub3J0aC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADg
t/sSFzlaZ7ckgDFh4K8/TDqUqq9VbkGgtELVG569nyuuQ4F
z40RLay/8MP39NUS10HgJZ9cvzeOUmHbS/ObZYHLzFI8A
O3sGqzMPgHNciljDXD0SqaJWWGgtOJ0V3qy9AgMBAAGgA
AAOBgQBrVcUP7cGO+1JTxARRBhB8d8vT3jpwK0qgaUAO
4A8J3GugojccH3pvcfGjE9gKA65QO8j8TPpKPh/8t8i4edTb
2TPsWMJkerZ+BcrAj75WOp9XiJCrP/CAj10J90rl6jFnzHez
-----END NEW CERTIFICATE REQUEST-----
```

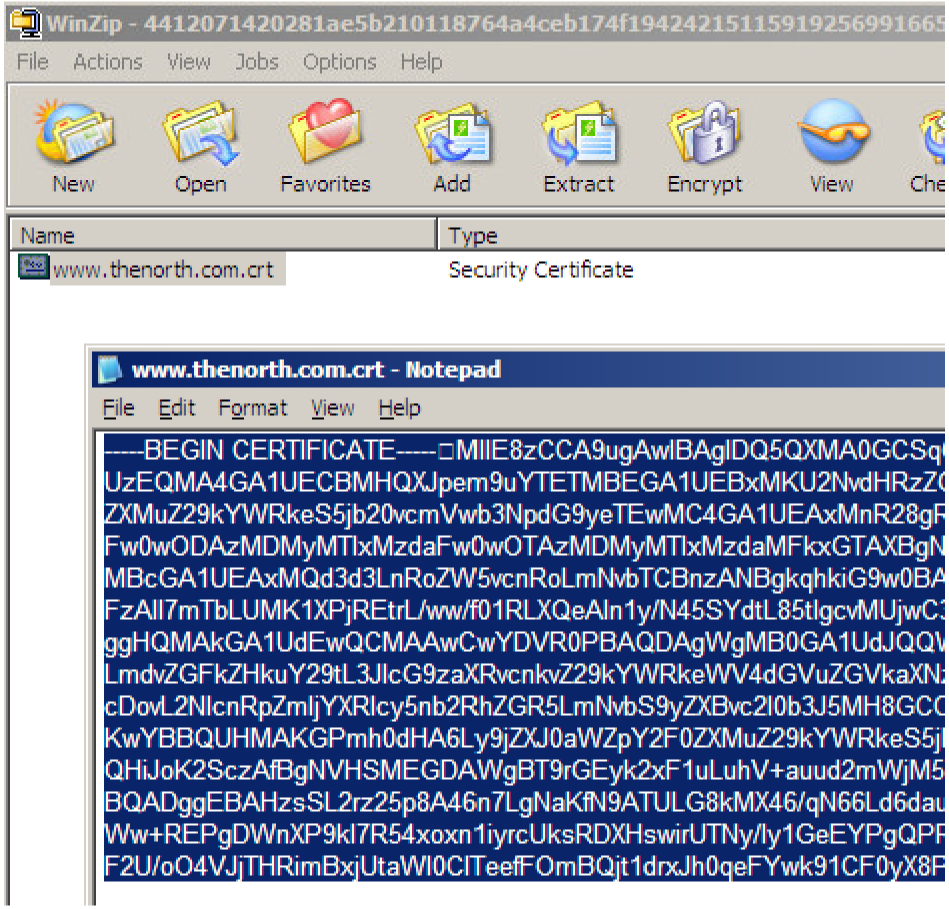
Please select your server software from the drop-down list below.

Other

☑ I warrant and represent that I am the registrant, or an authorized representative of the registrant, for the domain name associated with this certificate request.

Get the Certificate From The CA

- The CA will have a strange and painful process to give you the certificate.
- In this case, when I finally got it, it is in a certificate file.
- I just open that file in NOTEPAD and copy the text.
- Most CA's will let you just get the certificate as text.

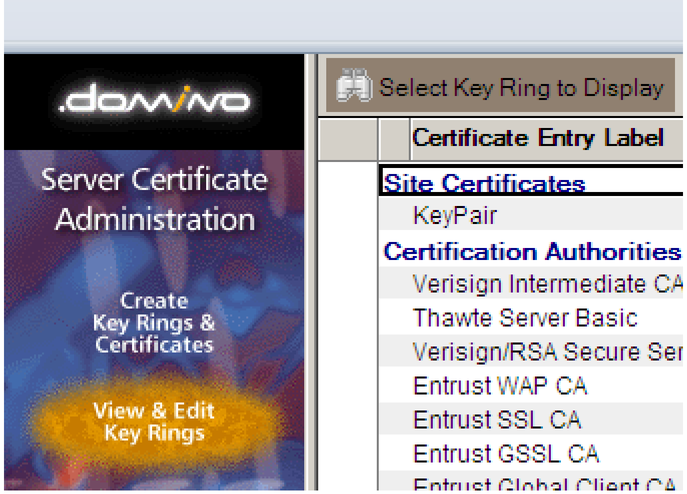

WinZip - 4412071420281ae5b210118764a4ceb174f19424215115919256991665
File
Actions
View
Jobs
Options
Help
New
Open
Favorites
Add
Extract
Encrypt
View
Che
www.thenorth.com.crt - Notepad
File
Edit
Format
View
Help

Name	Type
www.thenorth.com.crt	Security Certificate

```
-----BEGIN CERTIFICATE-----□MIIE8zCCA9ugAwIBAgIDQ5QXMA0GCSq
UzEQMA4GA1UECBMHQXJpem9uYTETMBEGA1UEBxMKU2NvdHRzZ
ZXMuZ29kYWRkeS5jb20vcmVwb3NpdG9yeTEwMC4GA1UEAxMnR28gR
Fw0wODAzMDMyMTIxMzdaFw0wOTAzMDMyMTIxMzdaMFkxGTAXBgN
MBcGA1UEAxMQd3d3LnRoZW5vcnRoLmNvbTCBnzANBgkqhkiG9w0BA
FzAII7mTbLUMK1XPjREtrL/ww/f01RLXQeAIn1y/N45SYdtL85tlgcvMUjwC
ggHQMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMB0GA1UdJQQ
LmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvZ29kYWRkeWV4dGVuZGVkaXN
cDovL2NlcnRpZmljYXRlcy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5MH8GC
KwYBBQUHMAKGPmh0dHA6Ly9jZXJ0aWZpY2F0ZXMuZ29kYWRkeS5j
QHiJoK2SczAfBgNVHSMEGDAWgBT9rGEyk2xF1uLuhV+auud2mWjM5
BQADggEBAHzsSL2rz25p8A46n7LgNaKfN9ATULG8kMX46/qN66Ld6da
Ww+REPgDWnXP9kI7R54xoxn1iyrcUksRDXHswirUTNy/ly1GeEYPgQP
F2U/oO4VJjTHRimBxjUtaWI0CITeefFOmBQjt1drxJh0qeFYwk91CF0yX8
```

Back to the Database

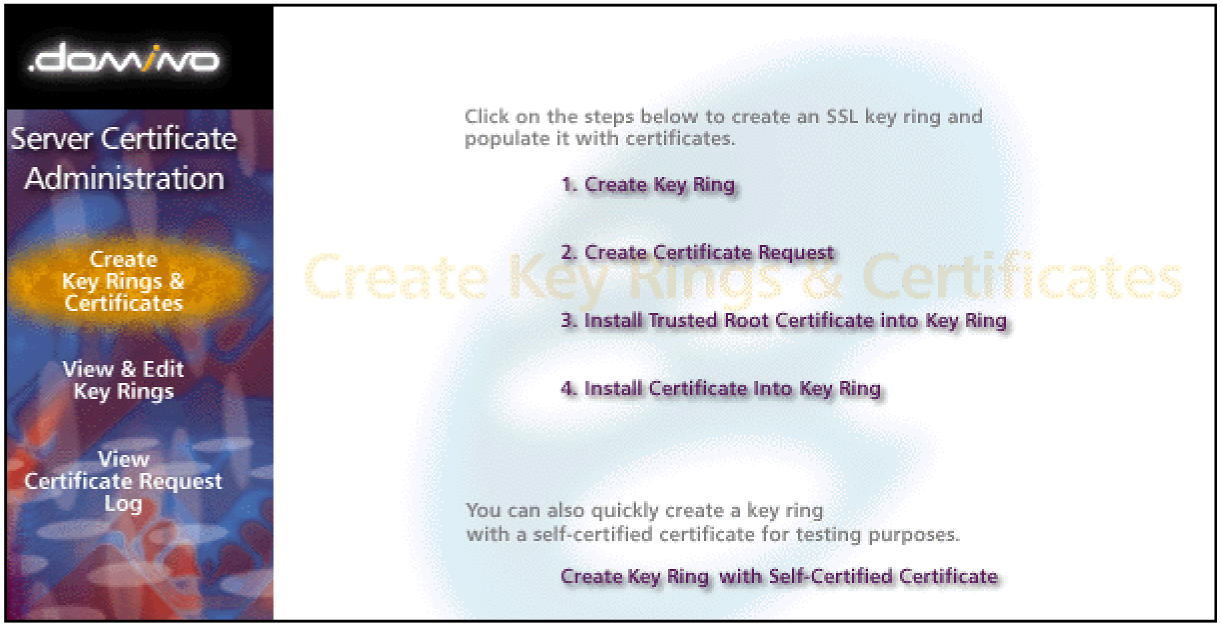
- You may have to select “View & Edit Key Rings” to open yours before you can proceed


.domino
Server Certificate Administration
Create Key Rings & Certificates
View & Edit Key Rings
Select Key Ring to Display

Certificate Entry Label
Site Certificates
KeyPair
Certification Authorities
Verisign Intermediate CA
Thawte Server Basic
Verisign/RSA Secure Ser
Entrust WAP CA
Entrust SSL CA
Entrust GSSL CA
Entrust Global Client CA

Back To The Menu

- Install Certificate Into Key Ring



.domino
Server Certificate Administration
Create Key Rings & Certificates
View & Edit Key Rings
View Certificate Request Log
Create Key Rings & Certificates

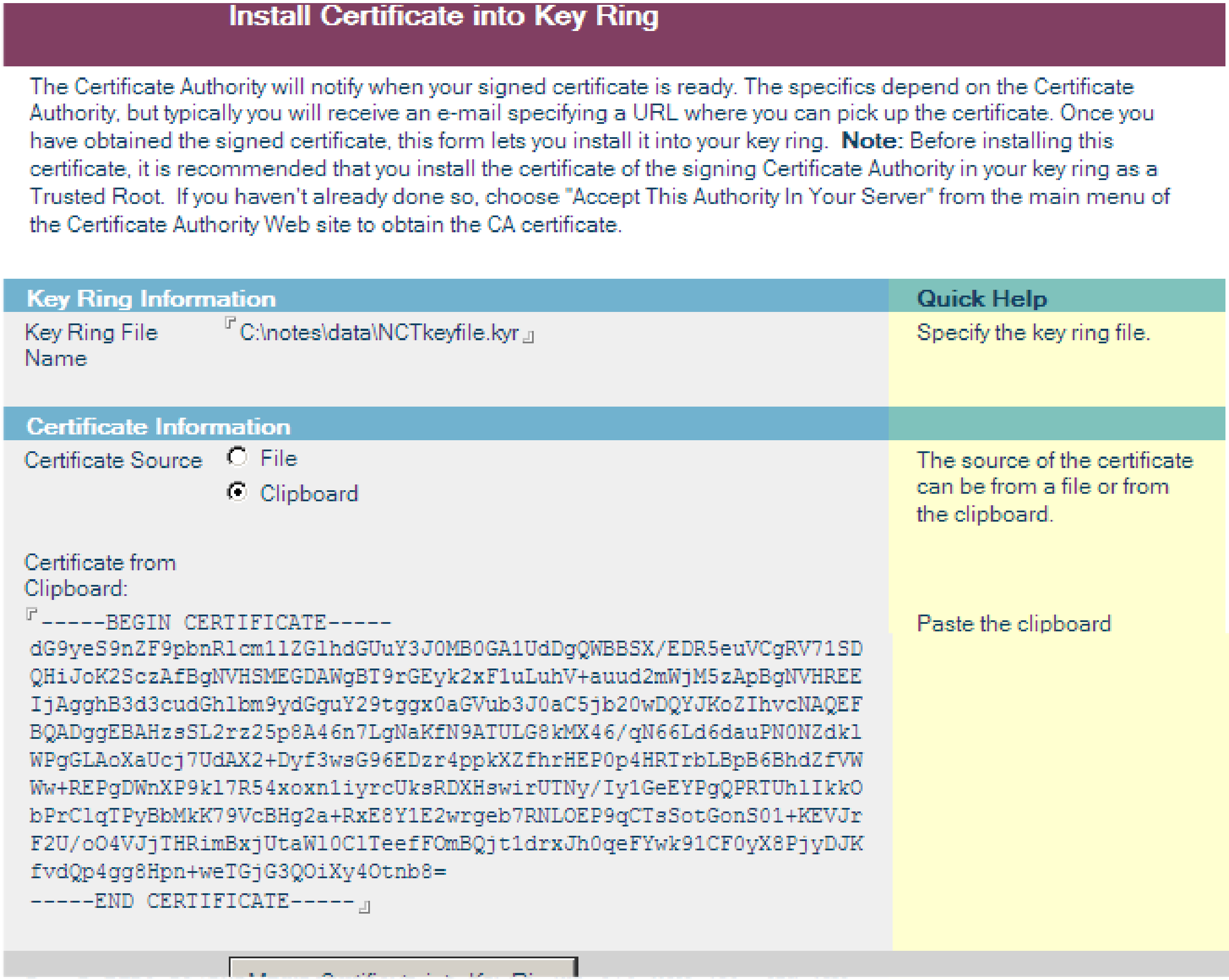
Click on the steps below to create an SSL key ring and populate it with certificates.

1. Create Key Ring
2. Create Certificate Request
3. Install Trusted Root Certificate into Key Ring
4. Install Certificate Into Key Ring

You can also quickly create a key ring with a self-certified certificate for testing purposes.

Create Key Ring with Self-Certified Certificate

Install the Certificate



Install Certificate into Key Ring

The Certificate Authority will notify when your signed certificate is ready. The specifics depend on the Certificate Authority, but typically you will receive an e-mail specifying a URL where you can pick up the certificate. Once you have obtained the signed certificate, this form lets you install it into your key ring. **Note:** Before installing this certificate, it is recommended that you install the certificate of the signing Certificate Authority in your key ring as a Trusted Root. If you haven't already done so, choose "Accept This Authority In Your Server" from the main menu of the Certificate Authority Web site to obtain the CA certificate.

Key Ring Information

Quick Help

Key Ring File Name: C:\notes\data\NCTkeyfile.kyr

Specify the key ring file.

Certificate Information

Certificate Source: ○ File ● Clipboard

The source of the certificate can be from a file or from the clipboard.

Certificate from Clipboard:

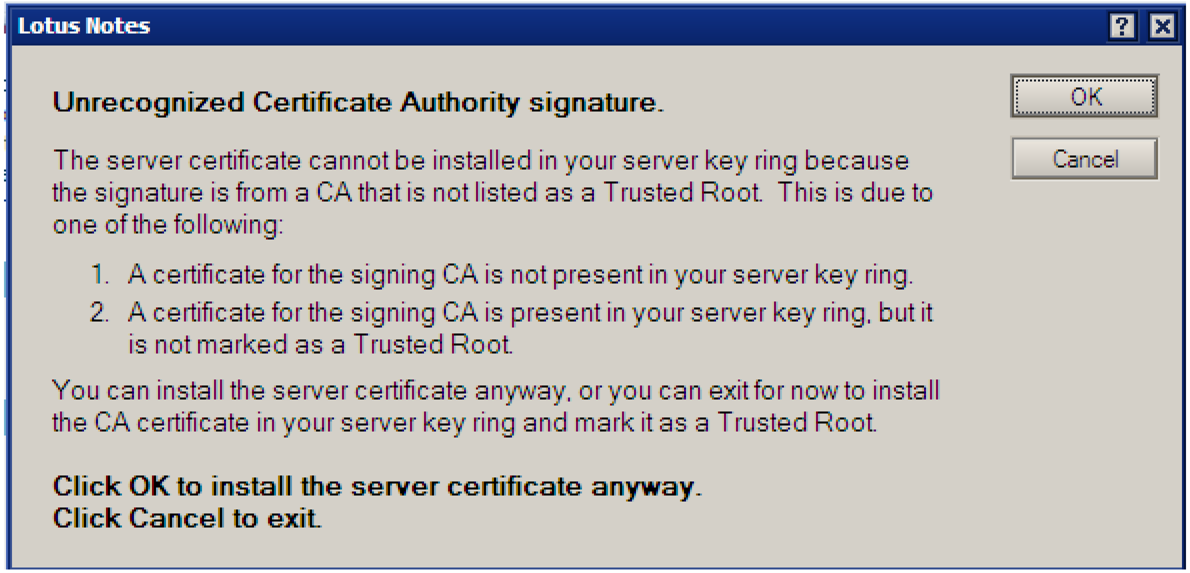
```
-----BEGIN CERTIFICATE-----
dG9yeS9nZF9pbnRlcm1lZGlhdGUuY3J0MB0GA1UdDgQWBBSX/EDR5euVCgRV71SD
QHiJoK2SczAfBgNVHSMEGDAWgBT9rGEyk2xFluLuhV+auud2mWjM5zApBgNVHREE
IjAgghB3d3cudGhlbm9ydGguY29tggx0aGVub3J0aC5jb20wDQYJKoZIhvcNAQEF
BQADggEBAHzsSL2rz25p8A46n7LgNaKfN9ATULG8kMX46/qN66Ld6dauPN0NZdkl
WPgGLAoXaUcj7UdAX2+Dyf3wsG96EDzr4ppkXZfhrHEP0p4HRTrbLBpB6BhdZfVW
Ww+REPgDWnXP9kl7R54xoxn1iyrcUksRDXHswirUTNy/Iy1GeEYPgQPRTUhlIkkO
bPrClqTPyBbMkK79VcBHg2a+RxE8Y1E2wrgeb7RNLOEP9qCTsSotGonS01+KEVJr
F2U/oO4VJjTHRimBxjUtaWl0ClTeefFOmBQjt1drxJh0qeFYwk91CF0yX8PjyDJK
fvdQp4gg8Hpn+weTGjG3QOiXy4Otnb8=
-----END CERTIFICATE-----
```

Paste the clipboard

You May Need A "Trusted Root"

- You'll get this from your CA Provider

- The Trusted Root is proof to that the actual certificate you have was issued by someone trustworthy even though they're not the top level certifier.



Unrecognized Certificate Authority signature.

The server certificate cannot be installed in your server key ring because the signature is from a CA that is not listed as a Trusted Root. This is due to one of the following:

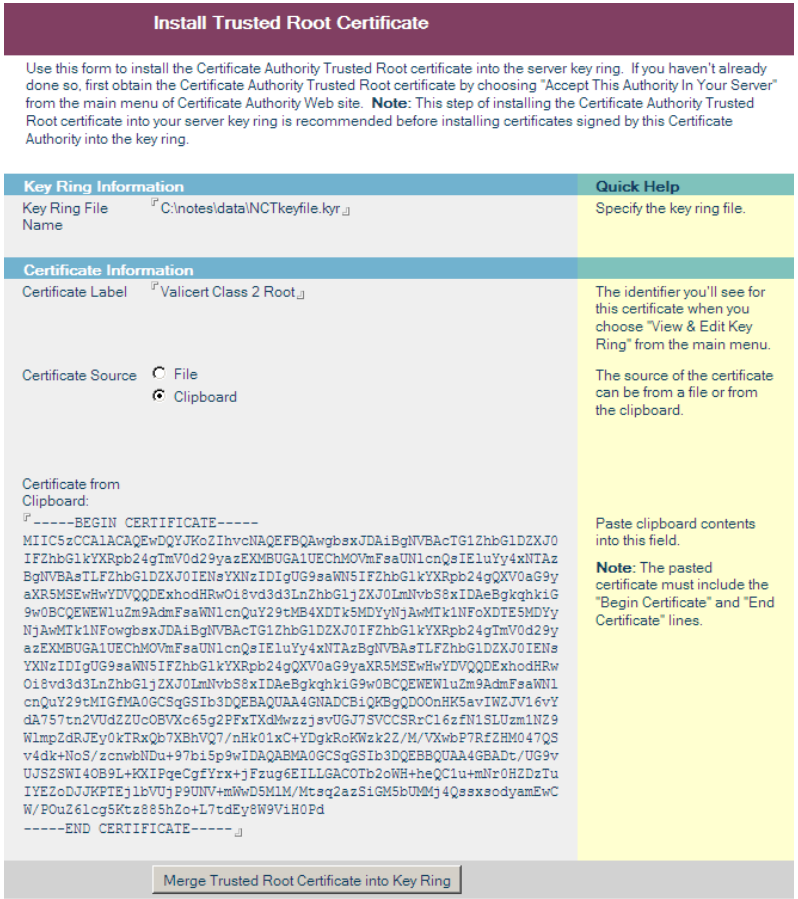
1. A certificate for the signing CA is not present in your server key ring.
2. A certificate for the signing CA is present in your server key ring, but it is not marked as a Trusted Root.

You can install the server certificate anyway, or you can exit for now to install the CA certificate in your server key ring and mark it as a Trusted Root.

Click OK to install the server certificate anyway.
Click Cancel to exit.

Install The Trusted Root Certificate

- Back to the CA who will give you a lengthy set of instructions to download their trusted root certificate.



Install Trusted Root Certificate

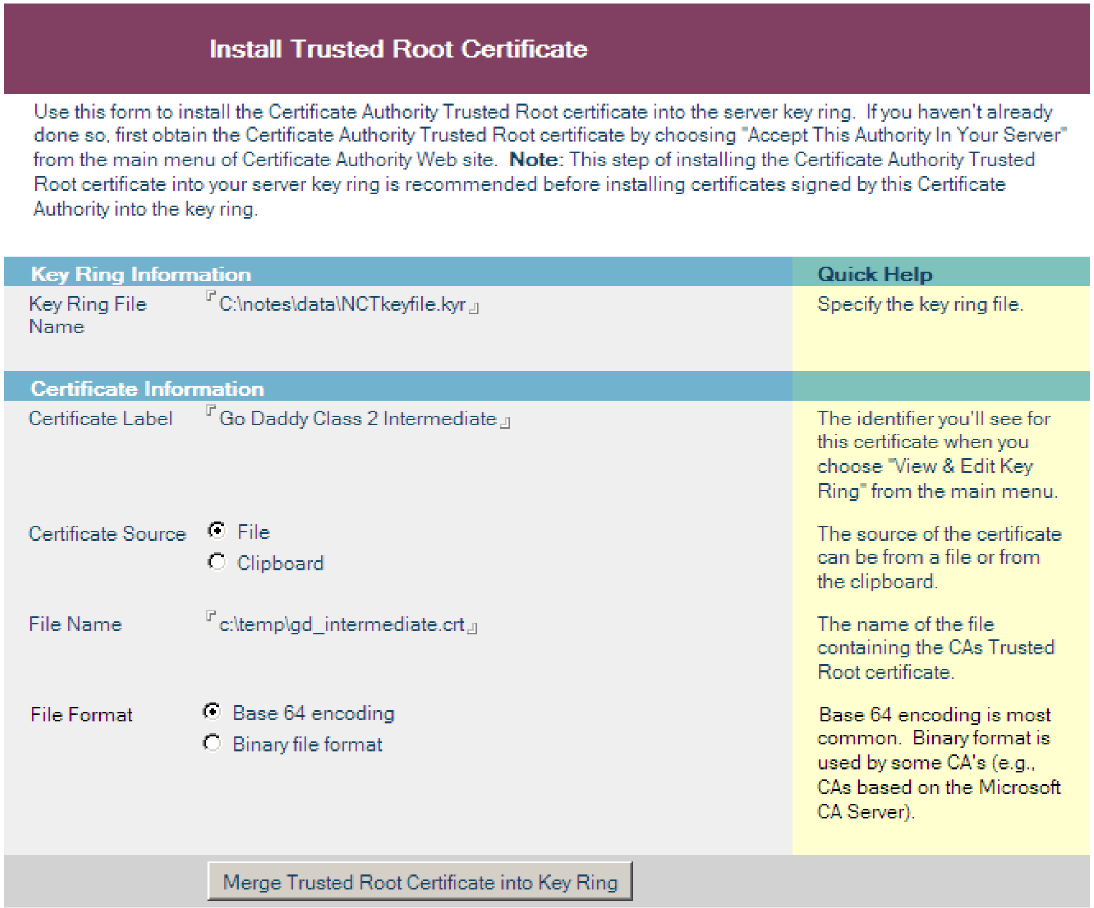
Use this form to install the Certificate Authority Trusted Root certificate into the server key ring. If you haven't already done so, first obtain the Certificate Authority Trusted Root certificate by choosing "Accept This Authority In Your Server" from the main menu of Certificate Authority Web site. **Note:** This step of installing the Certificate Authority Trusted Root certificate into your server key ring is recommended before installing certificates signed by this Certificate Authority into the key ring.

Key Ring Information		Quick Help
Key Ring File Name	C:\notes\data\NCTkeyfile.kyr	Specify the key ring file.

Certificate Information		
Certificate Label	Valicert Class 2 Root	The identifier you'll see for this certificate when you choose "View & Edit Key Ring" from the main menu.
Certificate Source	○ File ● Clipboard	The source of the certificate can be from a file or from the clipboard.
Certificate from Clipboard:		Paste clipboard contents into this field. **Note:** The pasted certificate must include the "Begin Certificate" and "End Certificate" lines.

```
-----BEGIN CERTIFICATE-----
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
Oi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG9w0BCQEWEWluZm9AdmFsaWNl
cnQuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDOOnHK5avIWZJV16vY
dA757tn2VUdZZUcOBVXc65g2PFxTXdMwzzjsvUGJ7SVCCSRrCl6zfN1SLUzm1NZ9
WlmpZdRJEy0kTRxQb7XBhVQ7/nHk01xC+YDgkRoKWzk2Z/M/VXwbP7RfZHM047QS
v4dk+NoS/zcnwbNDu+97bi5p9wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADt/UG9v
UJSZSWI4OB9L+KXIPqeCgfYrx+jFzug6EILLGACOTb2oWH+heQC1u+mNr0HZDzTu
IYEZoDJJKPTEjlbVUjP9UNV+mWwD5MlM/Mtsq2azSiGM5bUMMj4QssxsodyamEwC
W/POuZ6lcg5Ktz885hZo+L7tdEy8W9ViH0Pd
-----END CERTIFICATE-----
```

You Can Also Install From .CRT Files



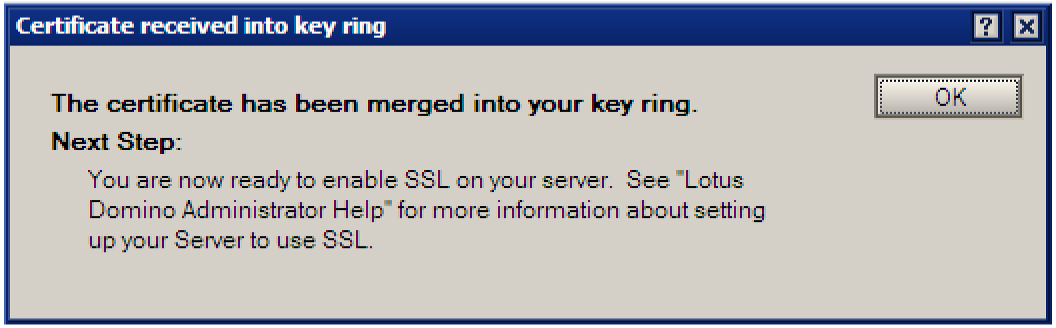
Install Trusted Root Certificate

Use this form to install the Certificate Authority Trusted Root certificate into the server key ring. If you haven't already done so, first obtain the Certificate Authority Trusted Root certificate by choosing "Accept This Authority In Your Server" from the main menu of Certificate Authority Web site. **Note:** This step of installing the Certificate Authority Trusted Root certificate into your server key ring is recommended before installing certificates signed by this Certificate Authority into the key ring.

Key Ring Information		Quick Help
Key Ring File Name	C:\notes\data\NCTkeyfile.kyr	Specify the key ring file.
Certificate Information		
Certificate Label	Go Daddy Class 2 Intermediate	The identifier you'll see for this certificate when you choose "View & Edit Key Ring" from the main menu.
Certificate Source	● File ○ Clipboard	The source of the certificate can be from a file or from the clipboard.
File Name	c:\temp\gd_intermediate.crt	The name of the file containing the CAs Trusted Root certificate.
File Format	● Base 64 encoding ○ Binary file format	Base 64 encoding is most common. Binary format is used by some CA's (e.g., CAs based on the Microsoft CA Server).

Finally – You're All Done

- If you had to install trusted root certificates, you may not see this OK screen unless you re-install your actual certificate at the end.
- It is ok to re-install your certificate if you want to be sure



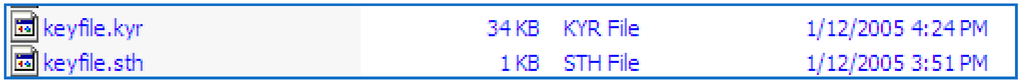
The certificate has been merged into your key ring.

Next Step:

You are now ready to enable SSL on your server. See "Lotus Domino Administrator Help" for more information about setting up your Server to use SSL.

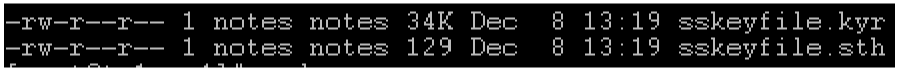
What Do You Do Now?

- Copy your .KYR file and another file with the same first name by the extension .STH which you'll find in the same directory – over to your Domino Data directory



```
keyfile.kyr     34 KB   KYR File   1/12/2005 4:24 PM
keyfile.sth      1 KB   STH File   1/12/2005 3:51 PM
```

- Remember, in Linux, to set its Owner and Group to 'notes' and its permissions to 644 so that the server can read it properly

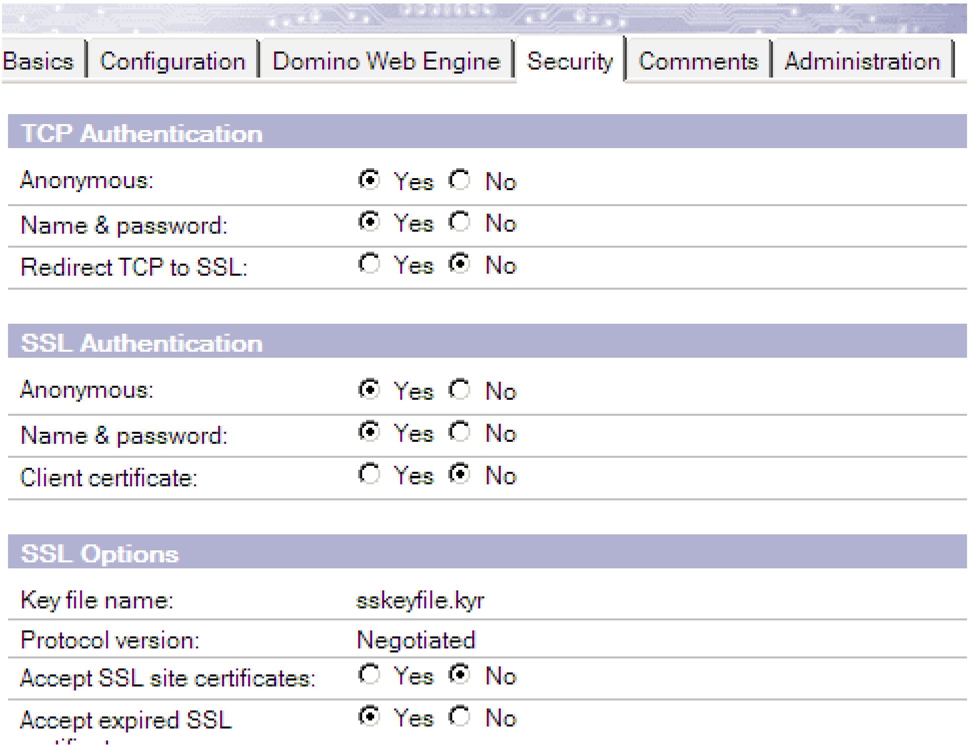


```
-rw-r--r-- 1 notes notes 34K Dec  8 13:19 sskeyfile.kyr
-rw-r--r-- 1 notes notes 129 Dec  8 13:19 sskeyfile.sth
```

And Finally…

- Reference the .KYR file (Key Ring) in your Internet Sites document for the HTTP site you're setting up!

- You have to restart the http task for this to take effect.



TCP Authentication

Anonymous:	● Yes ○ No
Name & password:	● Yes ○ No
Redirect TCP to SSL:	○ Yes ● No

SSL Authentication

Anonymous:	● Yes ○ No
Name & password:	● Yes ○ No
Client certificate:	○ Yes ● No

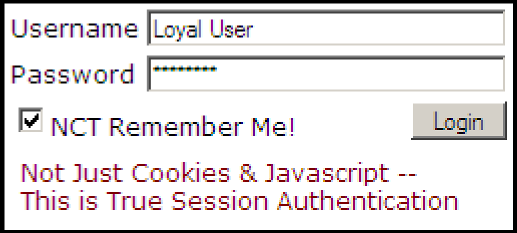
SSL Options

Key file name:	sskeyfile.kyr
Protocol version:	Negotiated
Accept SSL site certificates:	○ Yes ● No
Accept expired SSL	● Yes ○ No

Sponsored by: NCT Remember Me!

Automatically log-in returning Domino users

Installs in Minutes to existing or new web pages
Does not require a DSAPI filter
Fully Supports ACLs, Reader Names, Groups, etc.
Fully Supports Multi-Server Session Based Authentication



Username: Loyal User
Password: *********
☑ NCT Remember Me!

Not Just Cookies & Javascript --
This is True Session Authentication

http://www.Thenorth.com/ncthome.nsf/html/RememberMe