

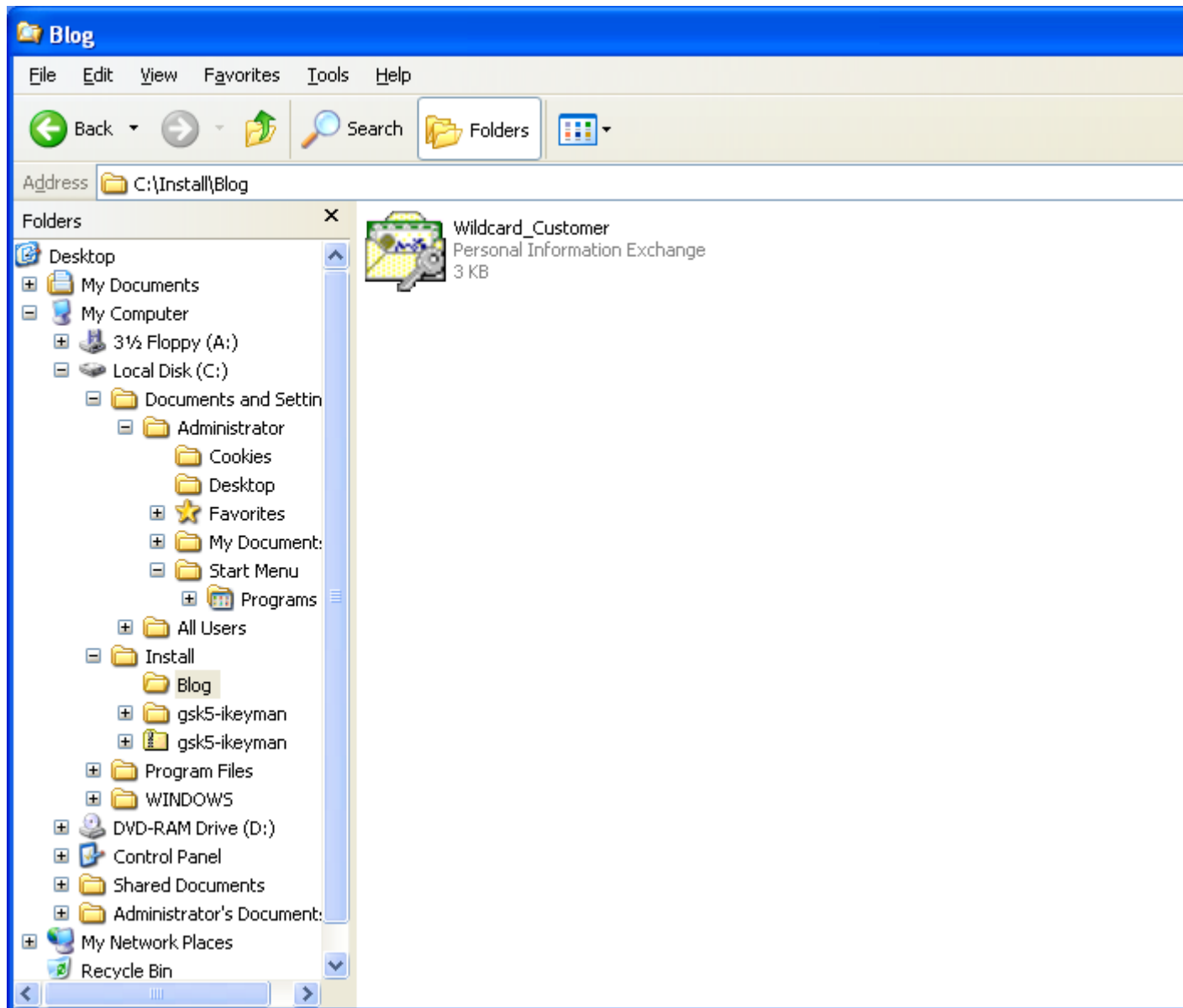
## Contents

What do I need.....	1
Import your P12/PFX file into your browser inside XP.....	2
Export root and any intermediate certificates to file.....	13
Run iKeyman to create new kyrfile and then Add and Import certificate information .....	21
Check your file and add sth file to enable it for Domino use .....	30
Implement the files on the server .....	33
Check out if it works .....	34
Conclusion .....	35

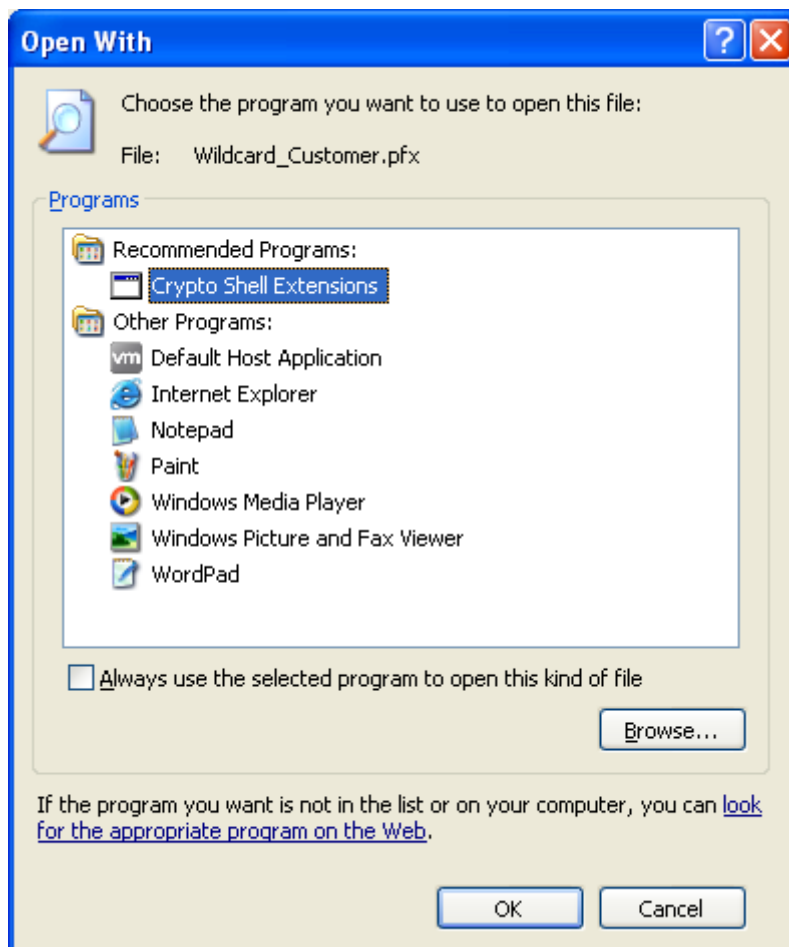
## What do I need:

1. One instance of a 32 bit Windows operating system, I used 32 bit Windows XP running on my laptop with VMware 10. You can not use 64 bit Windows for this task.
2. GSK5 that you can download from <http://www-01.ibm.com/support/docview.wss?uid=swg21615277&aid=1>. This should be unzipped inside your XP virtual machine.  
Source: <http://www-01.ibm.com/support/docview.wss?uid=swg21615277>
3. An exported P12/PFX file from in my case IIS, containing the wildcard certificate as well as the certification path to it, more on this later on

## Import your P12/PFX file into your browser inside XP

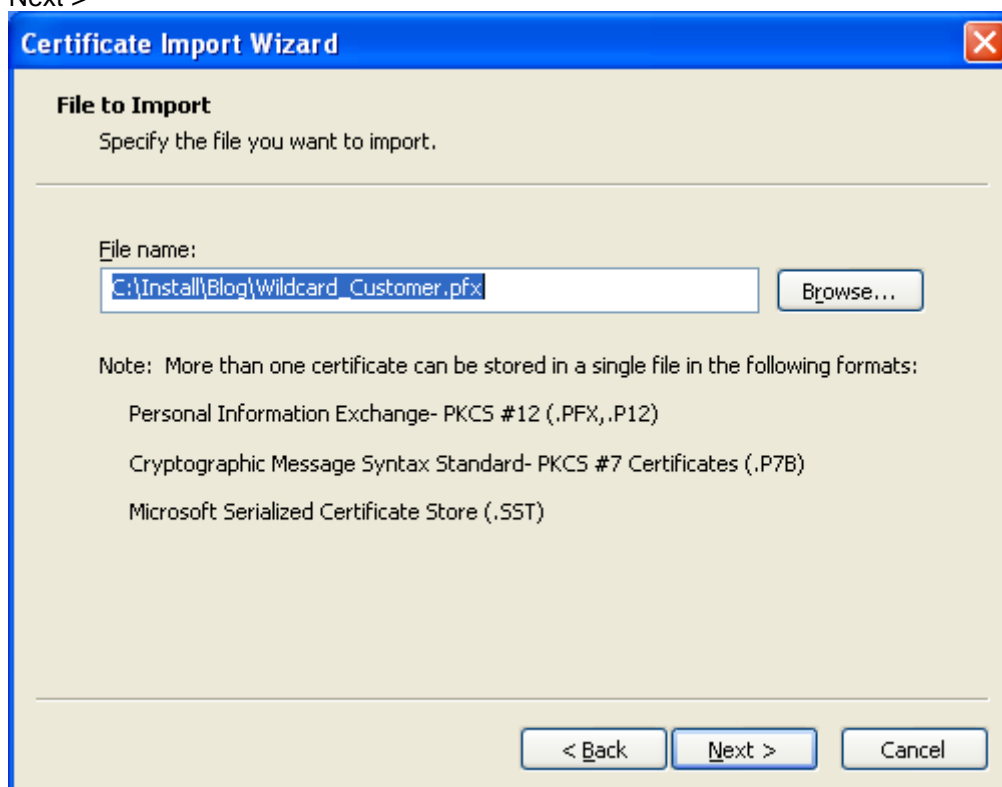


Open With...



OK

Next >



Next >

**Certificate Import Wizard**

**Password**

To maintain security, the private key was protected with a password.

---

Type the password for the private key.

Password:

\*\*\*\*\*

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

---

< Back   Next >   Cancel

Next >

**Certificate Import Wizard**

**Certificate Store**

Certificate stores are system areas where certificates are kept.

---

Windows can automatically select a certificate store, or you can specify a location for

☒ Automatically select the certificate store based on the type of certificate

☐ Place all certificates in the following store

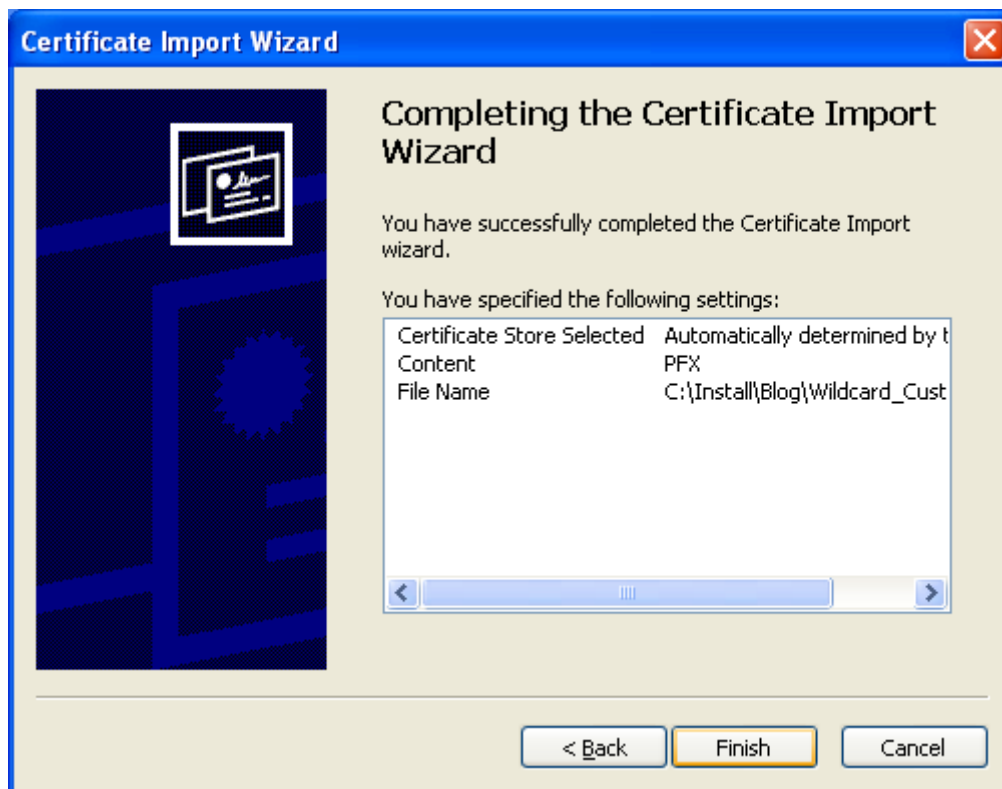
Certificate store:

  Browse...

---

< Back   Next >   Cancel

Next >

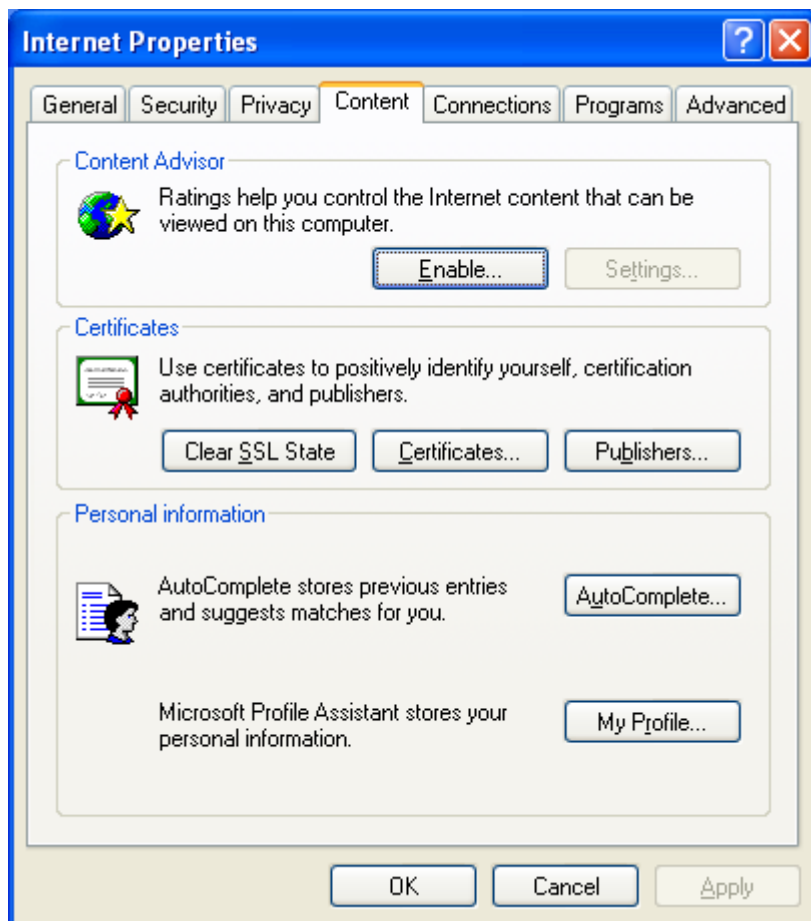


Finish

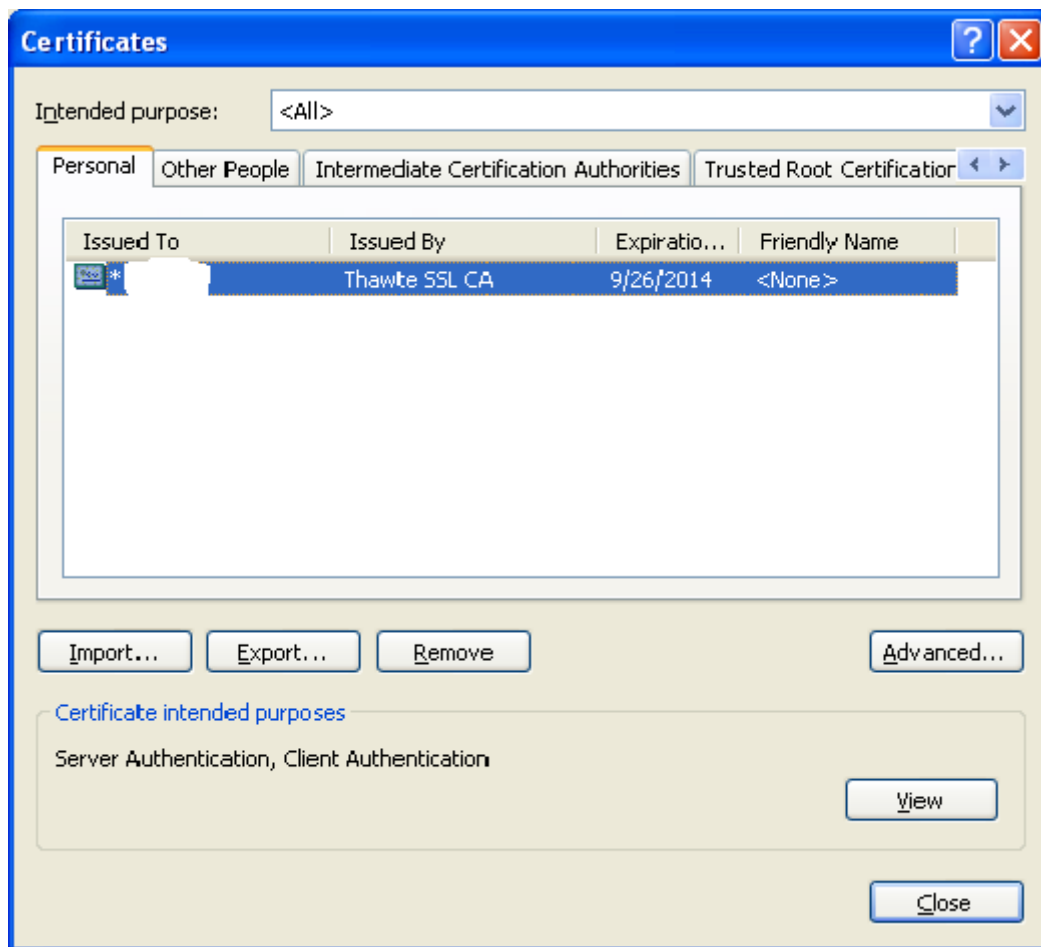


OK

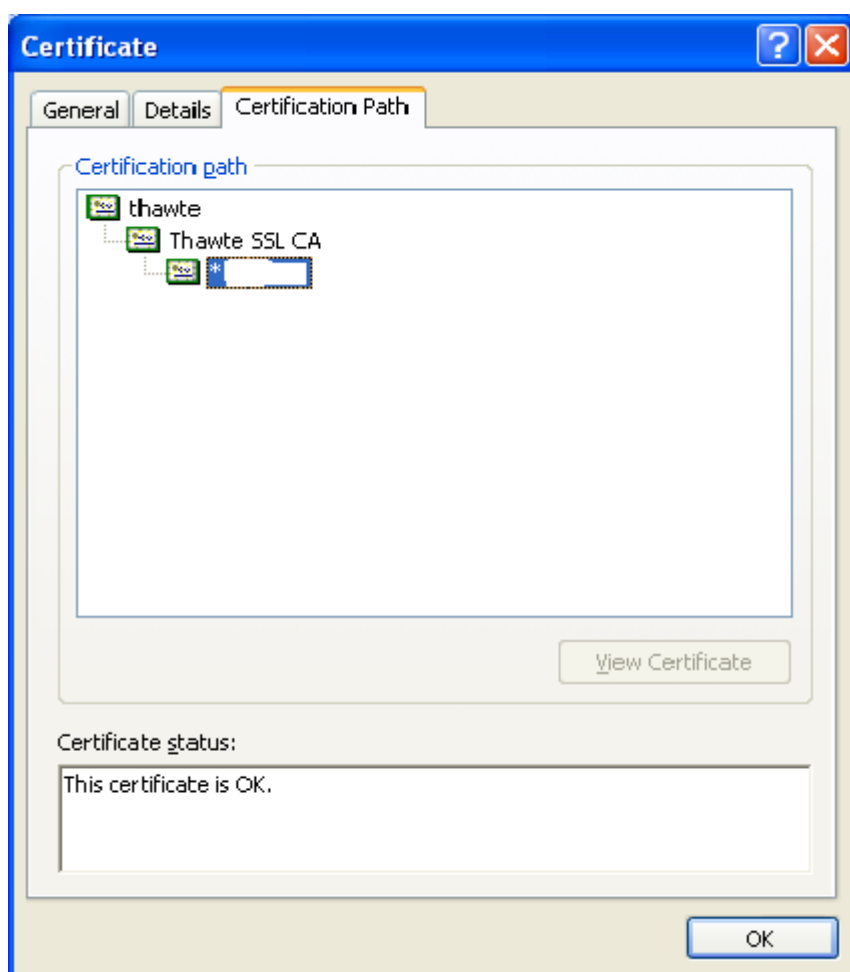
2. Check your imported certificate(s)



Certificates



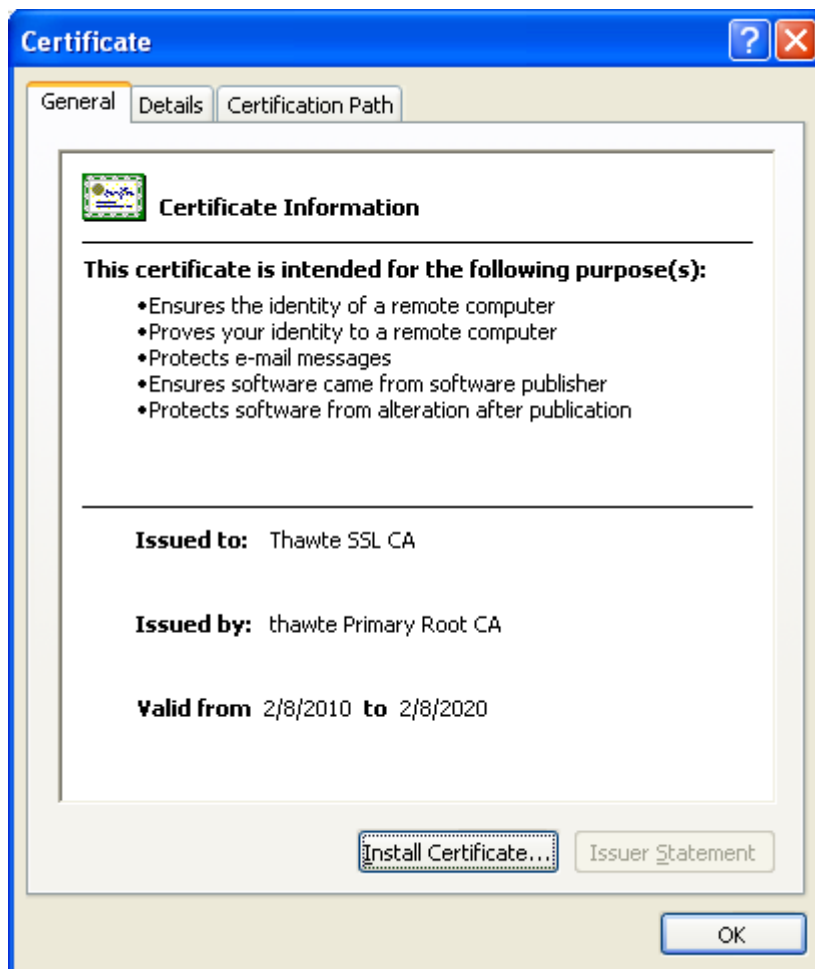
View



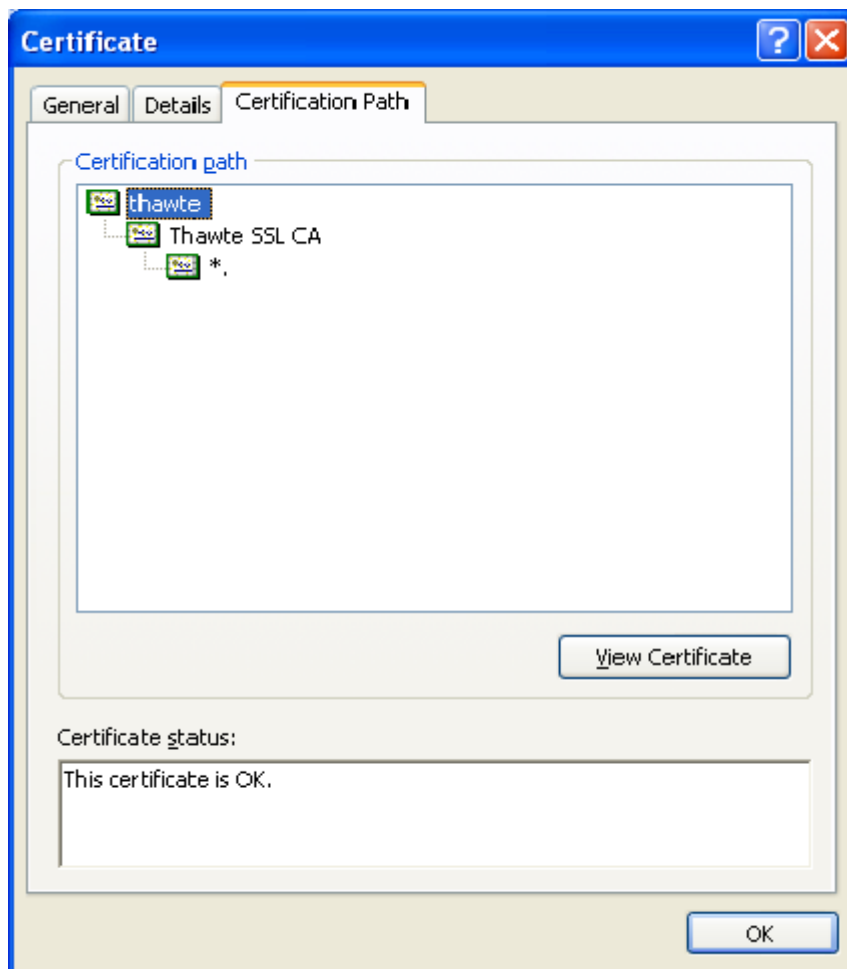




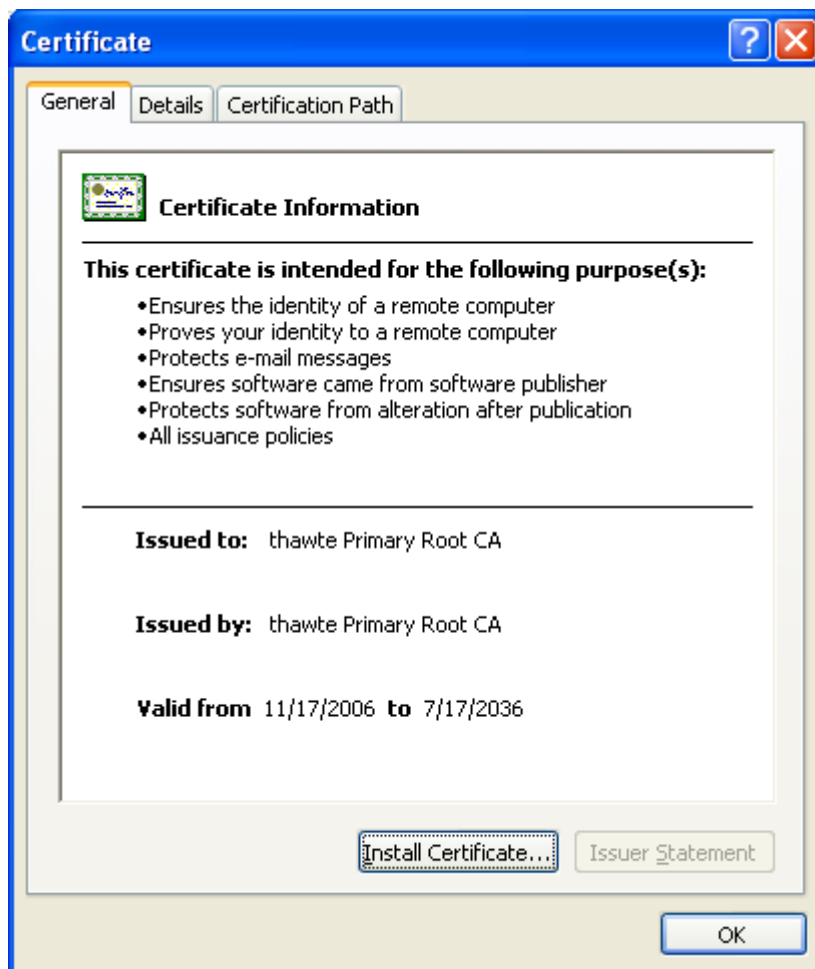
View Certificate



Write down the label on the right of **Issued to:** to use later on inside ikeyman in this case it is:  
Thawte SSL CA  
OK



View Certificate

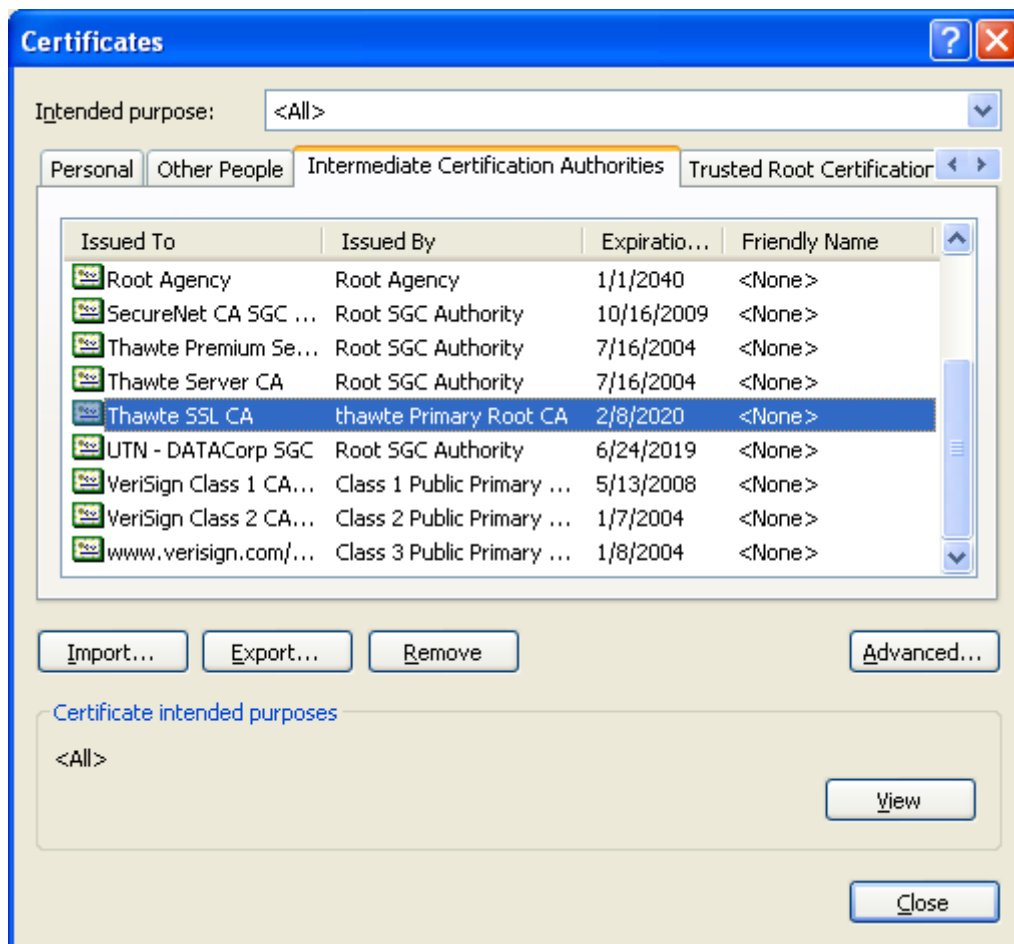


Write down the label on the right of **Issued to:** to use later on inside ikeyman in this case it is:  
thawte Primary Root CA

OK

OK

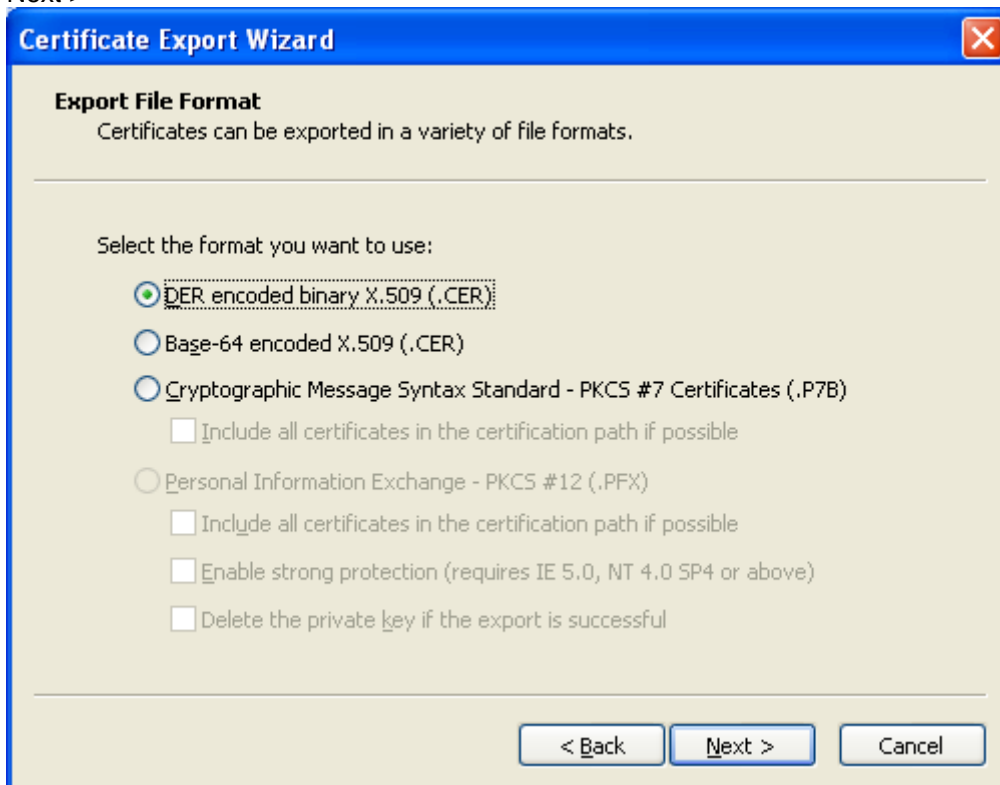
## Export root and any intermediate certificates to file



Export



Next >



**Certificate Export Wizard**

**Export File Format**  
Certificates can be exported in a variety of file formats.

---

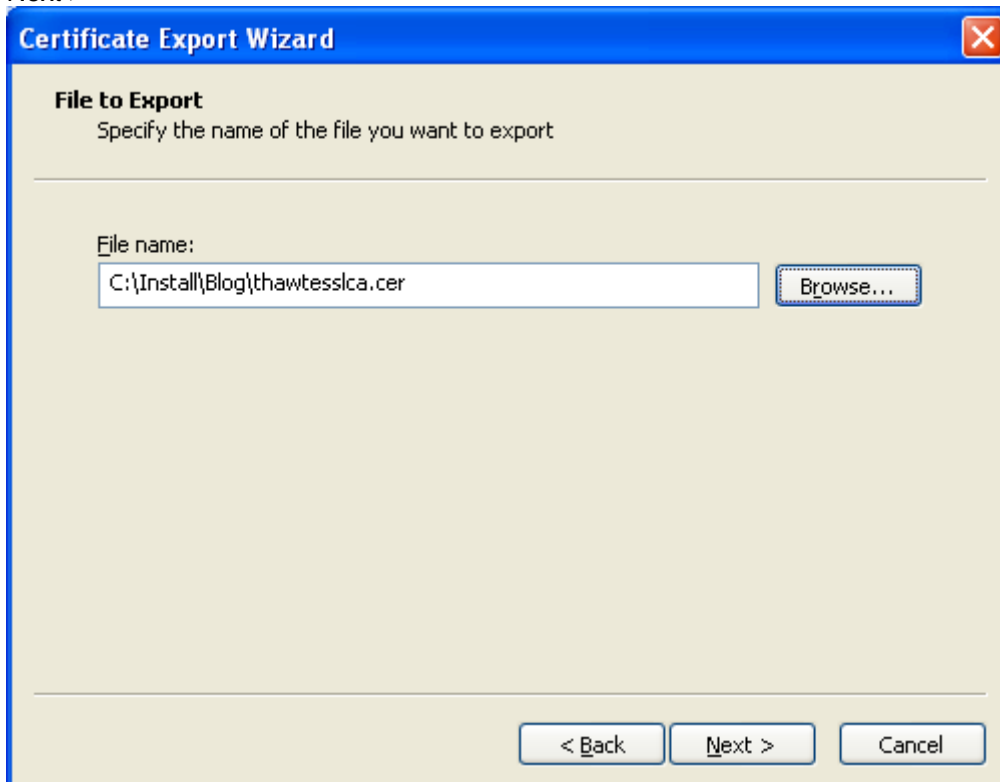
Select the format you want to use:

- ☒ DER encoded binary X.509 (.CER)
- ☐ Base-64 encoded X.509 (.CER)
- ☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - ☐ Include all certificates in the certification path if possible
- ☐ Personal Information Exchange - PKCS #12 (.PFX)
  - ☐ Include all certificates in the certification path if possible
  - ☐ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
  - ☐ Delete the private key if the export is successful

---

< Back   Next >   Cancel

Next >



**Certificate Export Wizard**

**File to Export**  
Specify the name of the file you want to export

---

File name:

---

< Back   Next >   Cancel

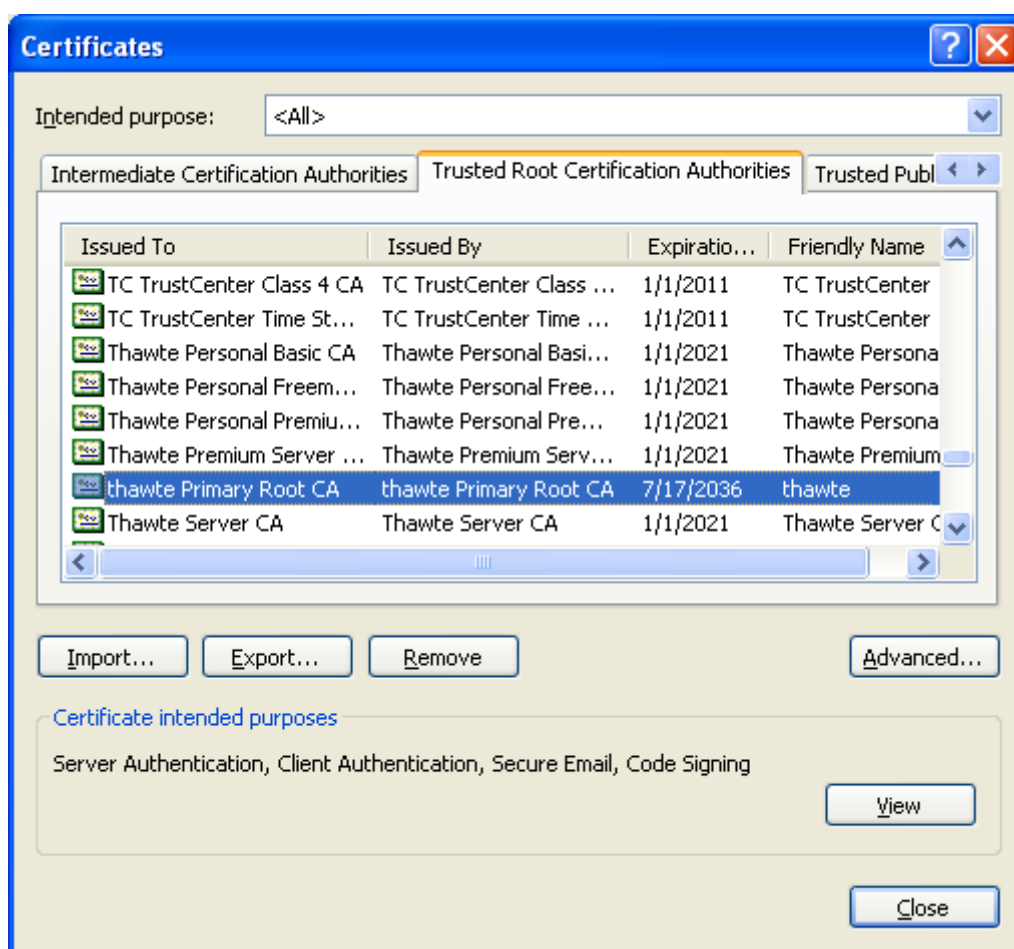
Next >



Finish



OK




Export



Next >



**Certificate Export Wizard** 

**Export File Format**  
Certificates can be exported in a variety of file formats.

---

Select the format you want to use:

☒ DER encoded binary X.509 (.CER)

☐ Base-64 encoded X.509 (.CER)

☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☐ Include all certificates in the certification path if possible

☐ Personal Information Exchange - PKCS #12 (.PFX)


☐ Include all certificates in the certification path if possible

☐ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

☐ Delete the private key if the export is successful

---

Next >

**Certificate Export Wizard** 

**File to Export**  
Specify the name of the file you want to export

---

File name:

---

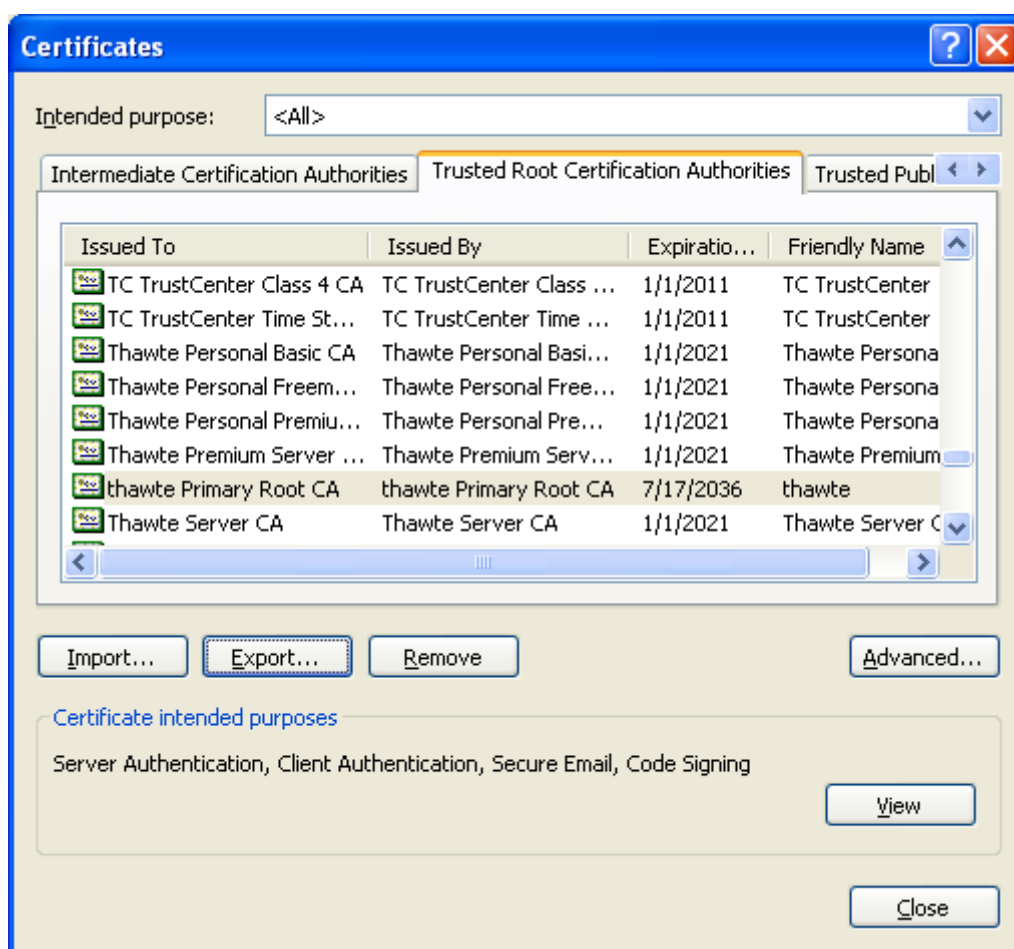
Next >



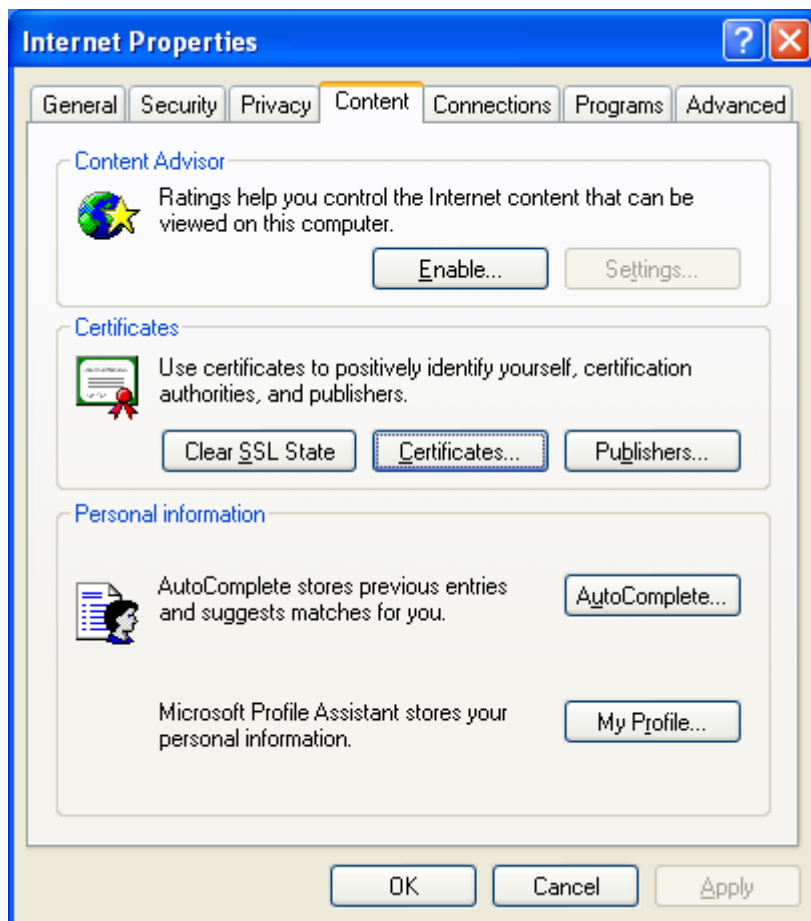
Finish



OK

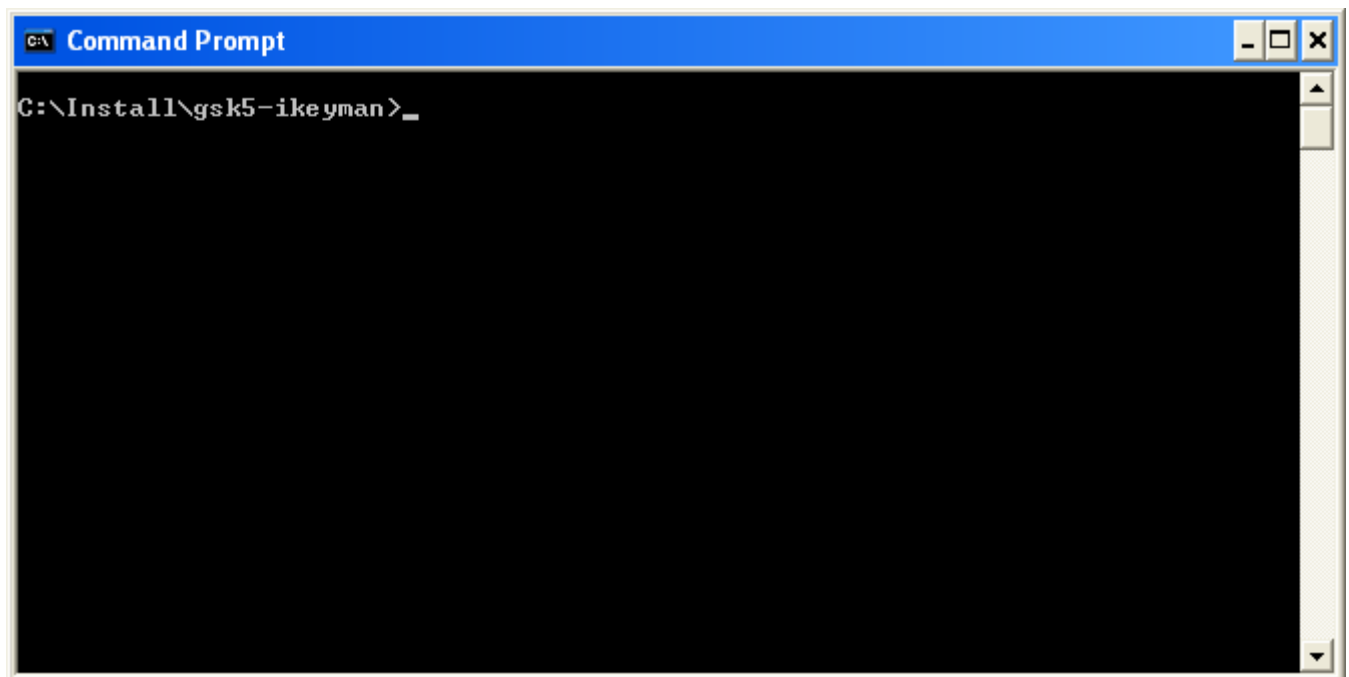


Close

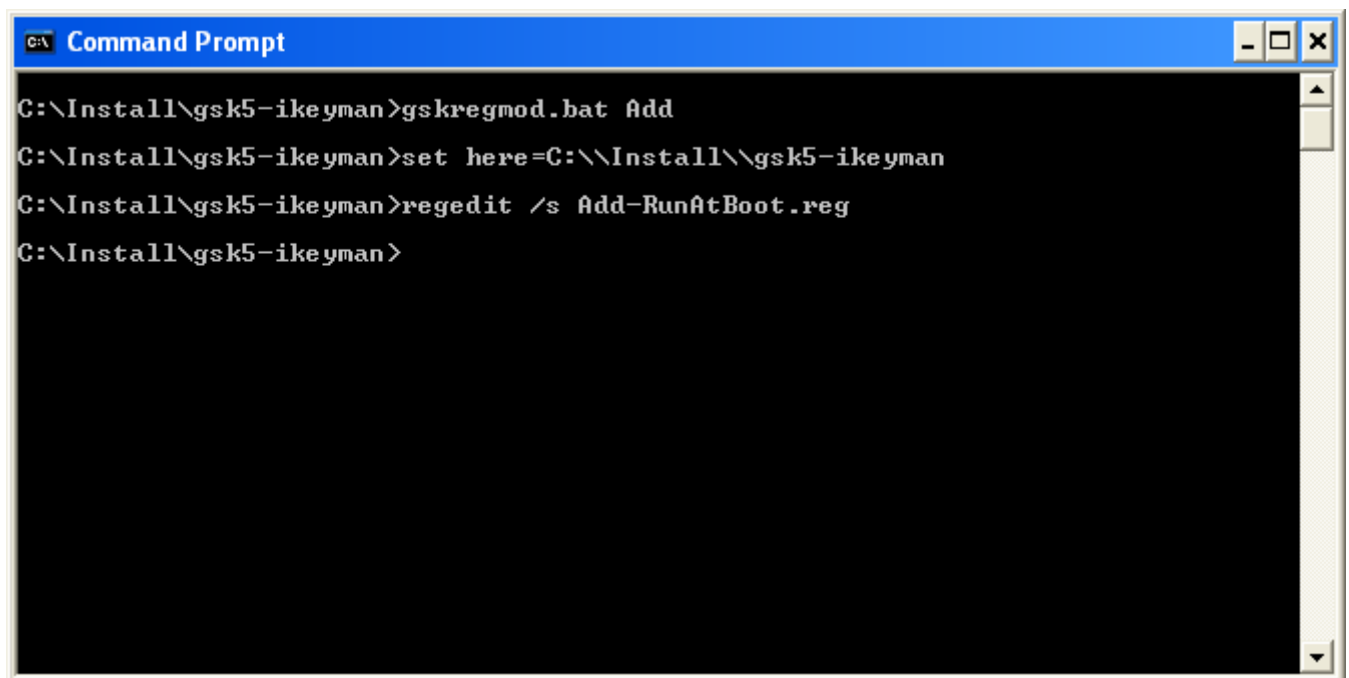


OK

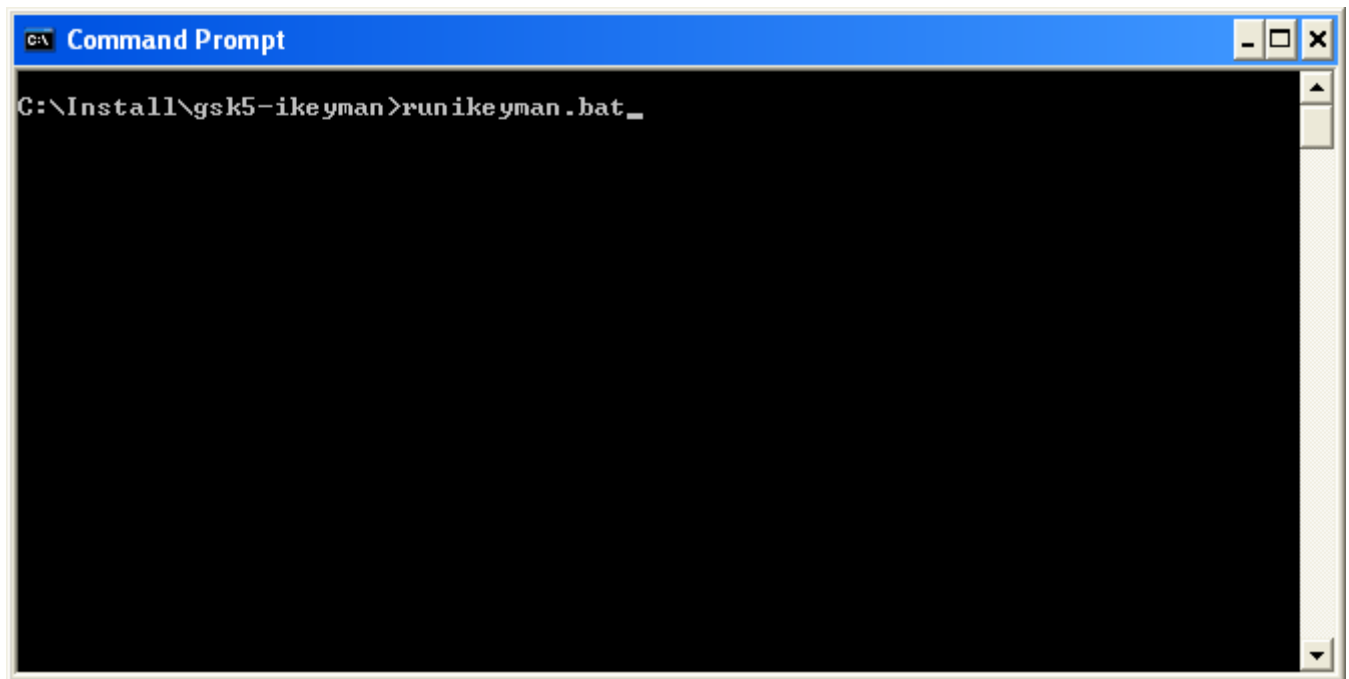
Run iKeyman to create new kyrfile and then Add and Import certificate information



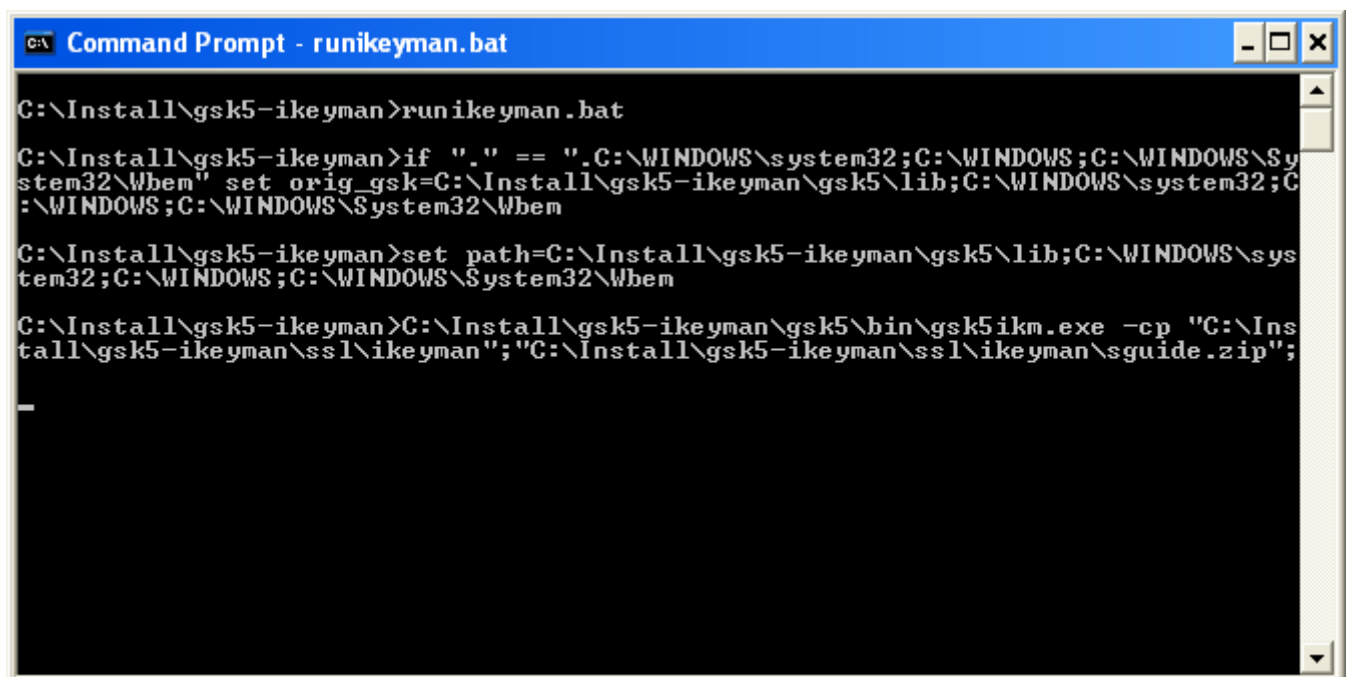
```
C:\ Install\gsk5-ikeyman>
```



```
C:\ Install\gsk5-ikeyman>gskregmod.bat Add
C:\ Install\gsk5-ikeyman>set here=C:\\Install\\gsk5-ikeyman
C:\ Install\gsk5-ikeyman>regedit /s Add-RunAtBoot.reg
C:\ Install\gsk5-ikeyman>
```



```
C:\Install\gsk5-ikeyman>runikeyman.bat
```



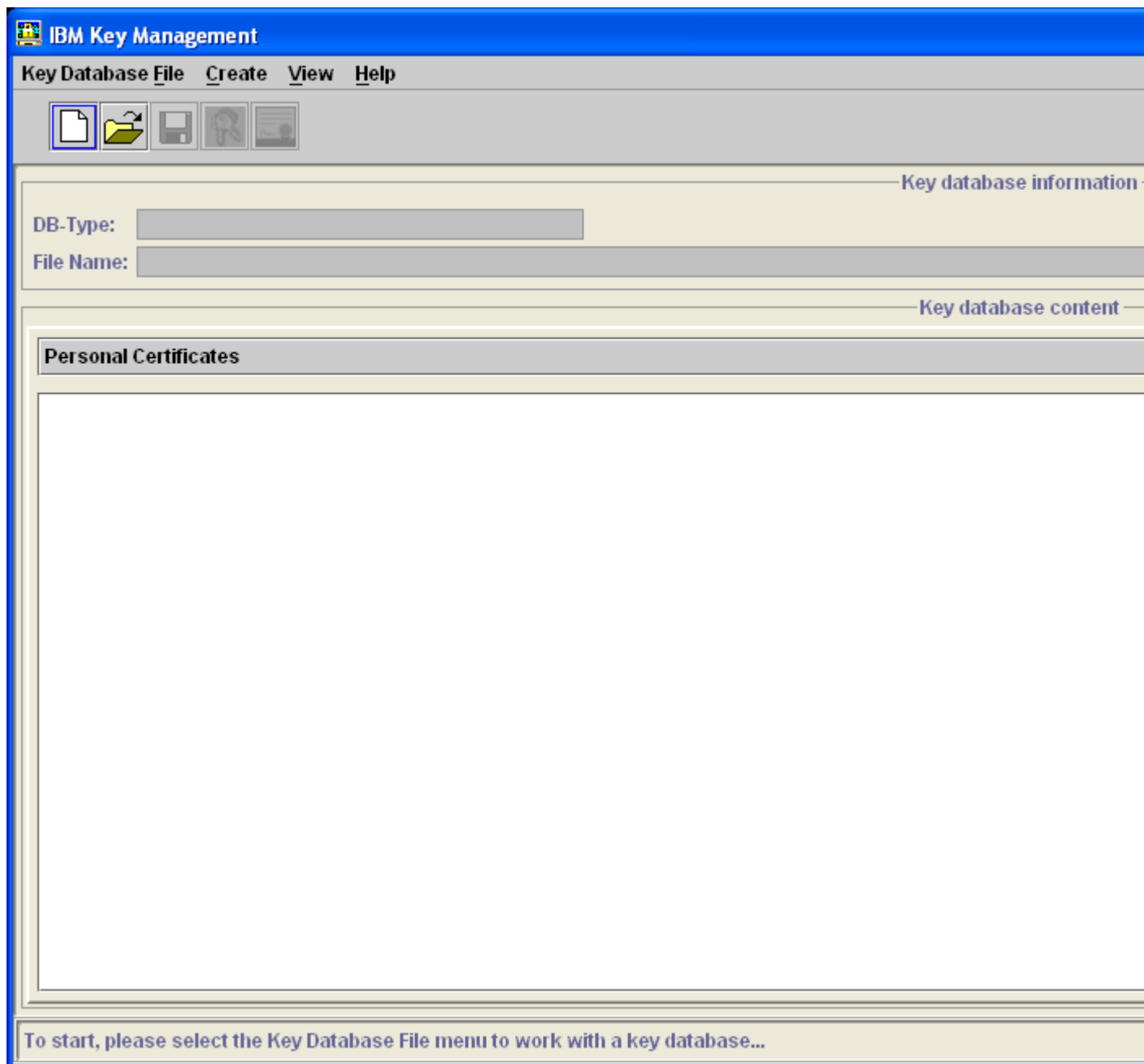
```
C:\Install\gsk5-ikeyman>runikeyman.bat

C:\Install\gsk5-ikeyman>if "." == ".C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem" set orig_gsk=C:\Install\gsk5-ikeyman\gsk5\lib;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem

C:\Install\gsk5-ikeyman>set path=C:\Install\gsk5-ikeyman\gsk5\lib;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem

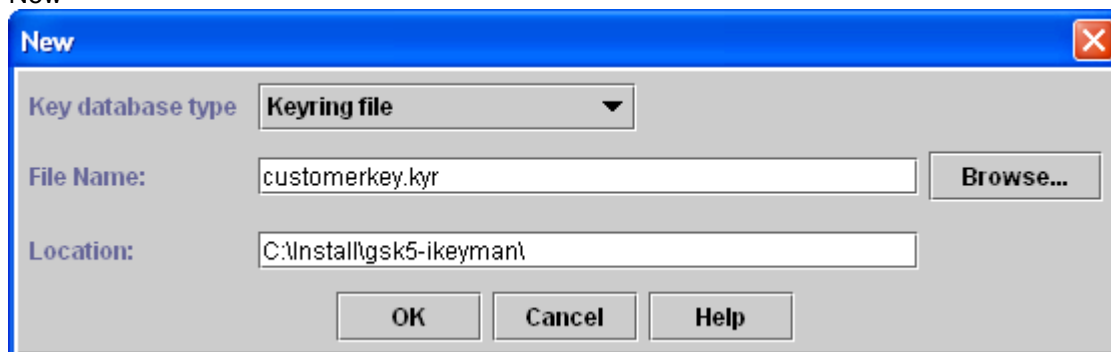
C:\Install\gsk5-ikeyman>C:\Install\gsk5-ikeyman\gsk5\bin\gsk5ikm.exe -cp "C:\Install\gsk5-ikeyman\ssl\ikeyman";"C:\Install\gsk5-ikeyman\ssl\ikeyman\sguide.zip";
```

Could take a while to start




Key Database File

New



OK



**Password Prompt** 

**Password:**

**Confirm Password:**

☐ **Set expiration time?**  Days

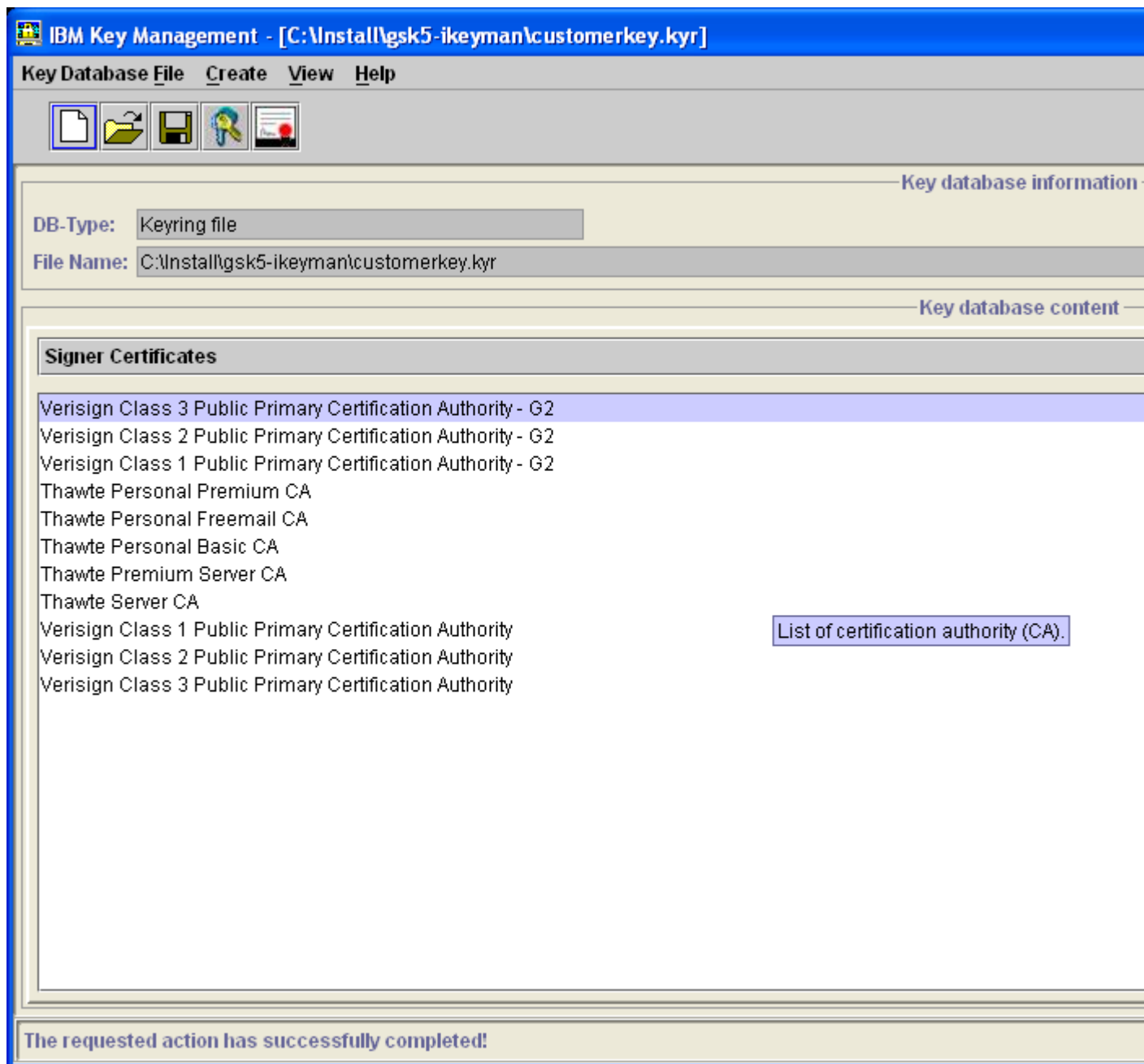
**Password Strength:**

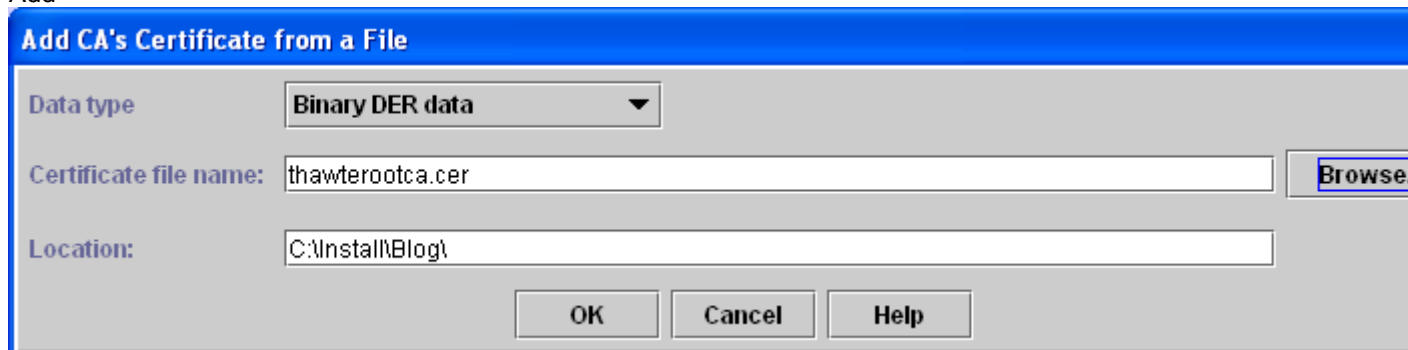
---

OK





Add



OK

Use the label that you wrote down earlier

**Enter a Label**

Enter a label for the certificate:

thawte Primary Root CA

OK Cancel

OK

**IBM Key Management - [C:\Install\gsk5-ikeyman\customerkey.kyr]**

Key Database File Create View Help

Key database information

DB-Type: Keyring file

File Name: C:\Install\gsk5-ikeyman\customerkey.kyr

Key database content

**Signer Certificates**

thawte Primary Root CA

Verisign Class 3 Public Primary Certification Authority - G2

Verisign Class 2 Public Primary Certification Authority - G2

Verisign Class 1 Public Primary Certification Authority - G2

Thawte Personal Premium CA

Thawte Personal Freemail CA

Thawte Personal Basic CA

Thawte Premium Server CA

Thawte Server CA

Verisign Class 1 Public Primary Certification Authority

Verisign Class 2 Public Primary Certification Authority

Verisign Class 3 Public Primary Certification Authority

The requested action has successfully completed!

Add

**Add CA's Certificate from a File**

Data type: **Binary DER data** ▼


Certificate file name:

Location:

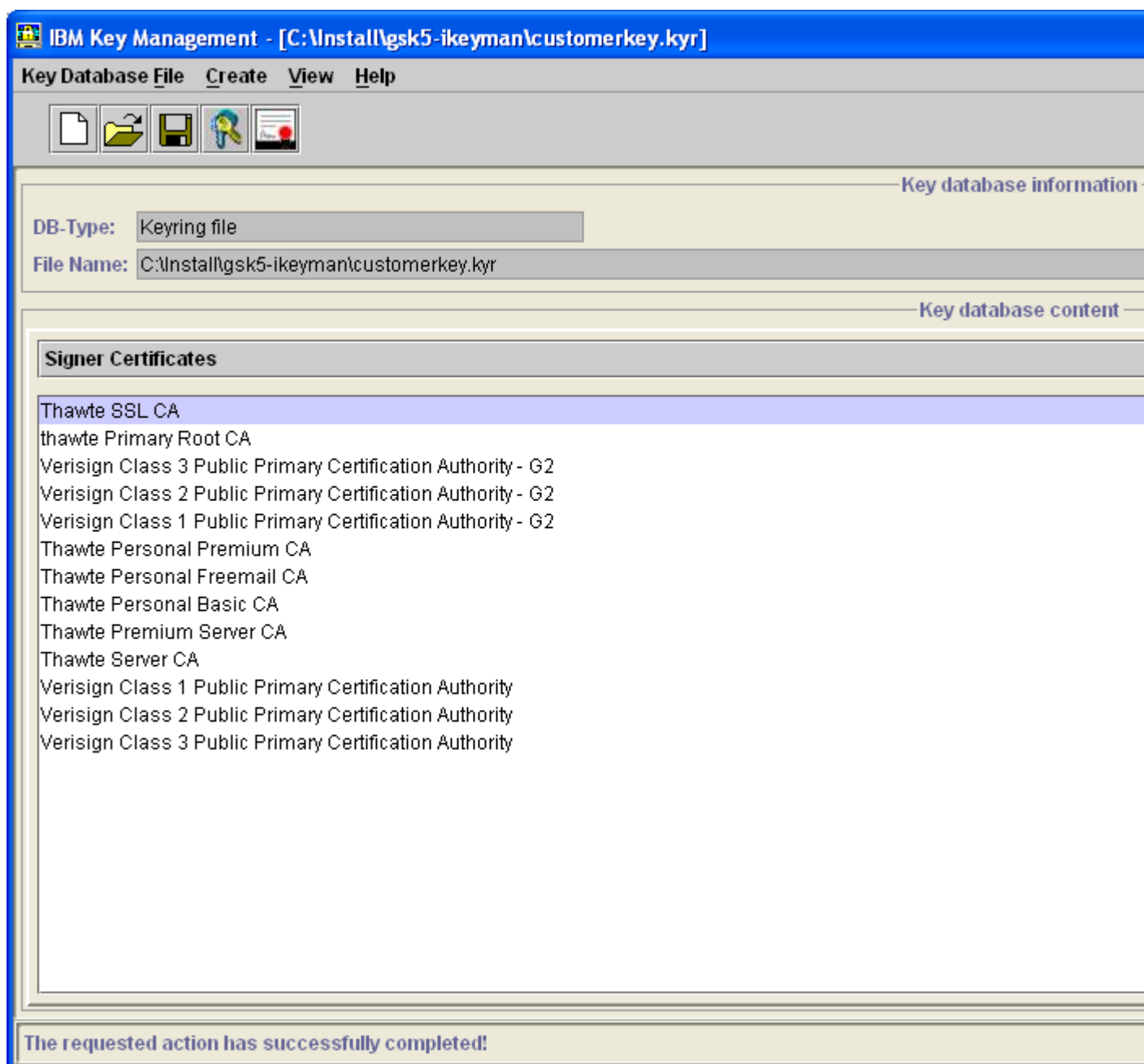
OK

Use the label that you wrote down earlier

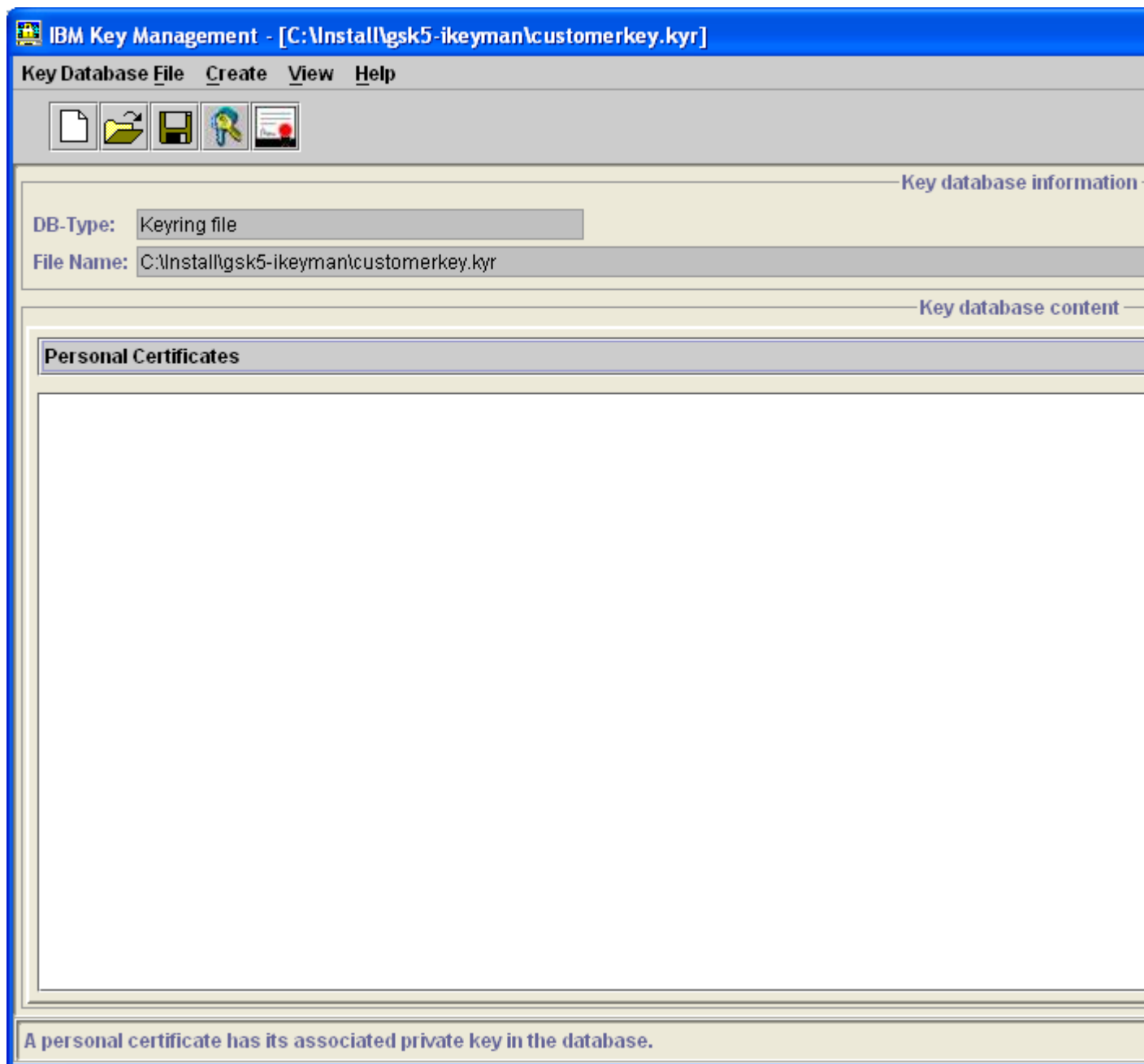
**Enter a Label**

 Enter a label for the certificate:

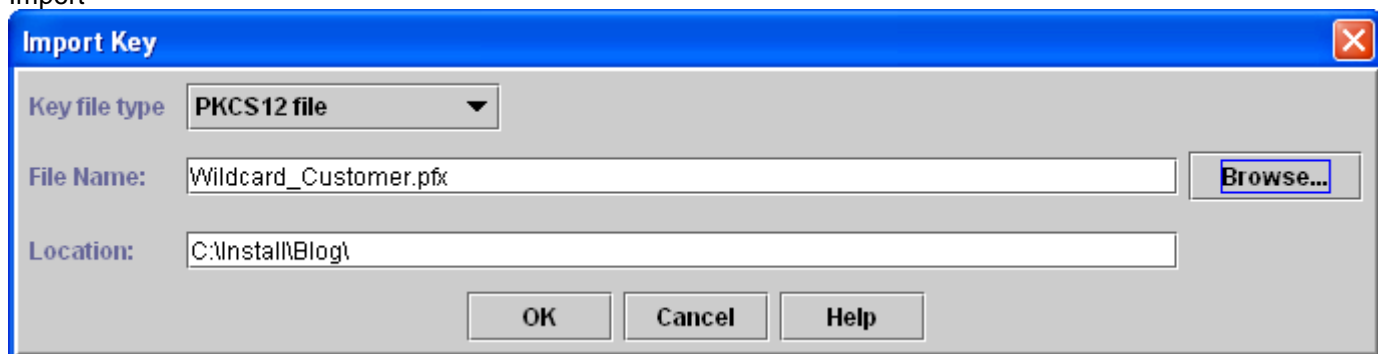
OK



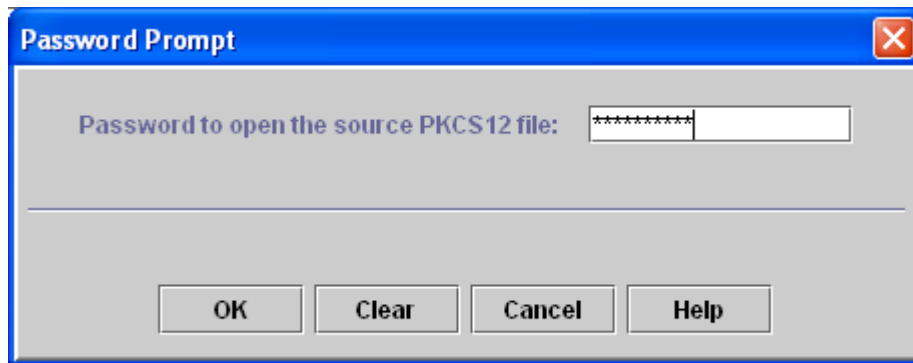
Switch to... Personal Certificates



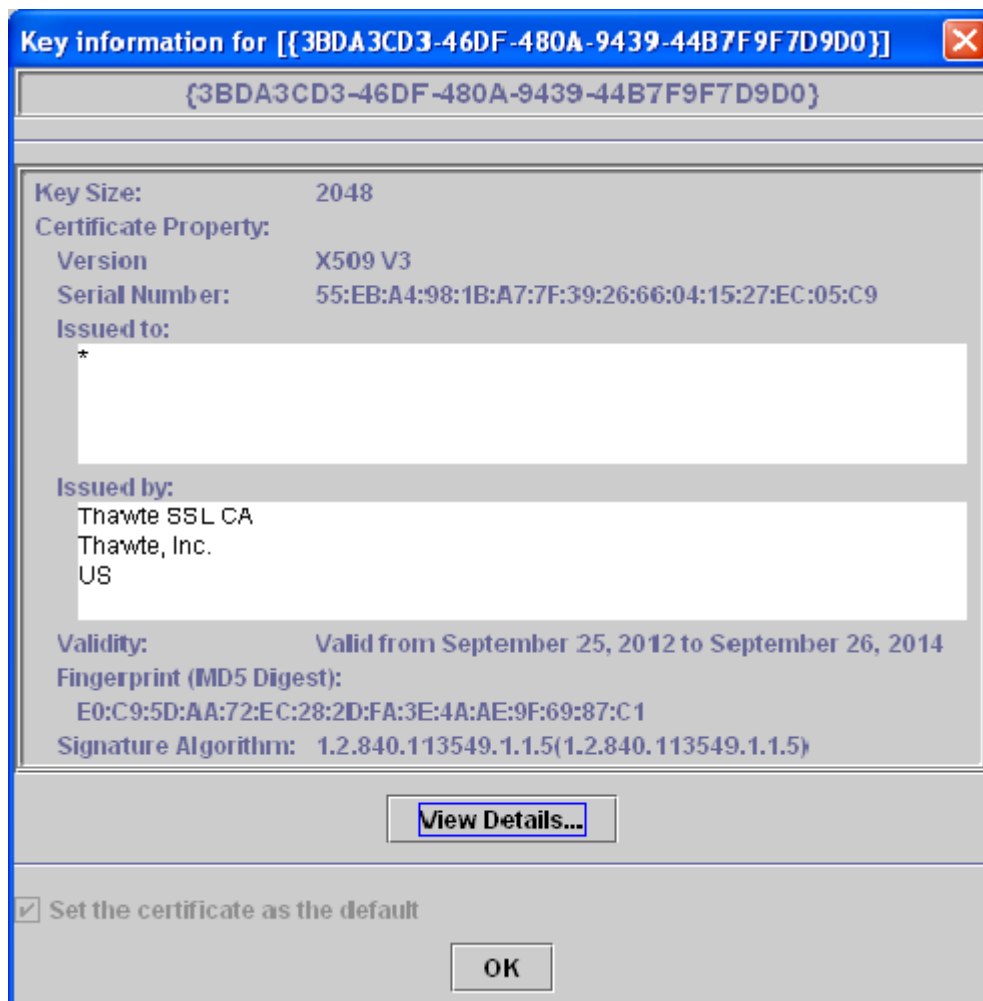
Import



OK



OK  
View/Edit



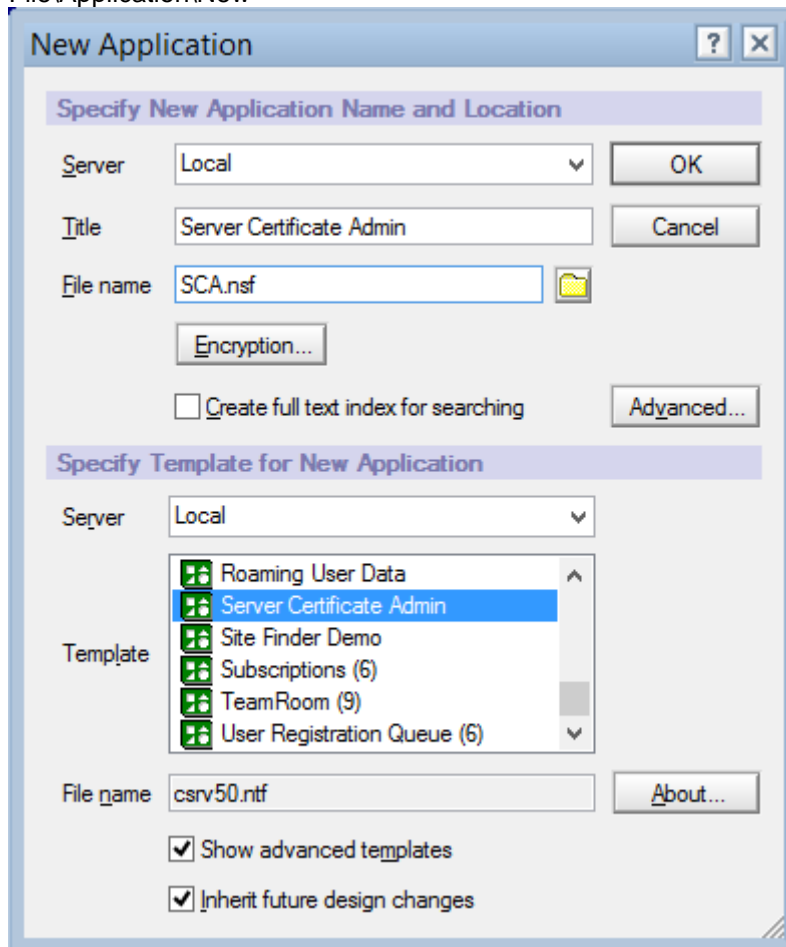
OK  
Key Database File  
Exit

## Check your file and add sth file to enable it for Domino use

Copy customerkey.kyr to your Notes Data directory on your client

From your Notes client use:

File\Application\New



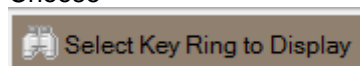
The 'New Application' dialog box is divided into two sections. The top section, 'Specify New Application Name and Location', contains fields for 'Server' (set to 'Local'), 'Title' (set to 'Server Certificate Admin'), and 'File name' (set to 'SCA.nsf'). It also includes an 'Encryption...' button, a checkbox for 'Create full text index for searching' (unchecked), and 'OK', 'Cancel', and 'Advanced...' buttons. The bottom section, 'Specify Template for New Application', contains a 'Server' dropdown (set to 'Local'), a 'Template' list box with options: 'Roaming User Data', 'Server Certificate Admin' (selected), 'Site Finder Demo', 'Subscriptions (6)', 'TeamRoom (9)', and 'User Registration Queue (6)', a 'File name' field (set to 'csrv50.ntf'), and 'About...' button. At the bottom are checkboxes for 'Show advanced templates' and 'Inherit future design changes' (both checked).

OK

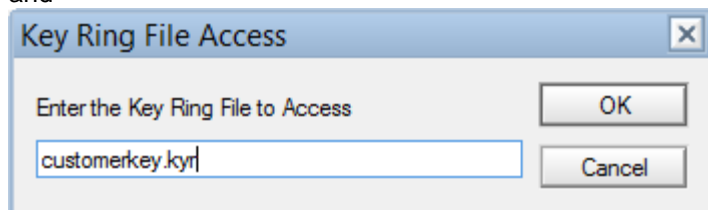
Open the newly created database  
and go to:



Choose



and



The 'Key Ring File Access' dialog box has a title bar with a close button. It contains a label 'Enter the Key Ring File to Access', a text input field containing 'customerkey.kyr', and 'OK' and 'Cancel' buttons.

OK

Password Input

Input password for customerkey.kyr


\*\*\*\*\*

Warning: An application that is not IBM Notes or Domino may be prompting you for this password. If you do not know the source of this prompt, providing a password may be a security risk.

OK Cancel

OK

Choose

 Change Key Ring Password

and

Key Ring File Access

Enter the Key Ring File to Access

customerkey.kyr

OK Cancel

OK

Password Input

Input password for C:\IBM\Notes\Data\customerkey.kyr

\*\*\*\*\*

Warning: An application that is not IBM Notes or Domino may be prompting you for this password. If you do not know the source of this prompt, providing a password may be a security risk.

OK Cancel

OK

Password Input

Input New Password for C:\IBM\Notes\Data\customerkey.kyr

\*\*\*\*\*

Warning: An application that is not IBM Notes or Domino may be prompting you for this password. If you do not know the source of this prompt, providing a password may be a security risk.

OK Cancel

OK

Password Input

Enter the new password again  
C:\IBM\Notes\Data\customerkey.kyr

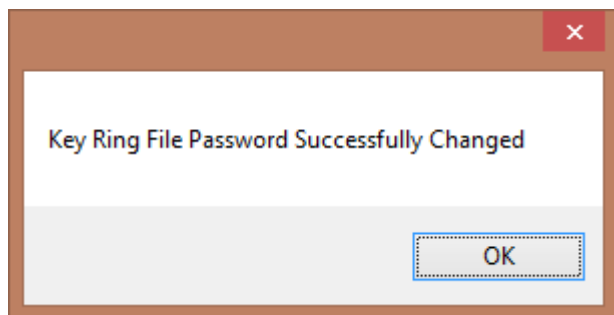
\*\*\*\*\*

Warning: An application that is not IBM Notes or Domino may be prompting you for this password. If you do not know the source of this prompt, providing a password may be a security risk.

OK Cancel

OK





You should now also have a customerkey.sth file in your data directory, please check that you have!  
If you don't you have not followed the instructions.  
Click on:

### Site Certificates

{3BDA3CD3-46DF-480A-9439-44B7F9F7D9D0}	No
--	----

should show something like this:

Certificate Information		
<b>Key Ring &amp; Certificate</b>		
Key Ring File Name	C:\IBM\Notes\Data\customerkey.kyr	
Certificate Label	{3BDA3CD3-46DF-480A-9439-44B7F9F7D9D0}	
Key Size	2048	
<b>Certificate Subject &amp; Issuer</b>		
	<b>Certificate Subject</b>	<b>Certificate Issuer</b>
Common Name	*.	Thawte SSL CA
Organization		Thawte, Inc.
Organizational Unit		
City		
State		
Country		US

## Implement the files on the server

Copy both kyr and sth files to the Servers Data Directory

Now in your Internet sites configuration

SSL Options	
Key file name:	<input type="text" value="customerkey.kyr"/>

Add the name of your kyr file as Key file name:

Also modify:

SSL Security	
SSL ciphers:	RC4 encryption with 128-bit key and MD5 MAC RC4 encryption with 128-bit key and SHA-1 MAC Triple DES encryption with 168-bit key and SHA-1 MAC DES encryption with 56-bit key and SHA-1 MAC RC4 encryption with 40-bit key and MD5 MAC
<input type="button" value="Modify"/>	

and uncheck

- ☐ DES encryption with 56-bit key and SHA-1 MAC
- ☐ RC4 encryption with 40-bit key and MD5 MAC

Save to avoid messages on the server console and in the log.

If you are not using internet sites change in the corresponding sections in your server document.

Also, in the server document, make sure that you have enabled SSL in the Internet Ports.... section.

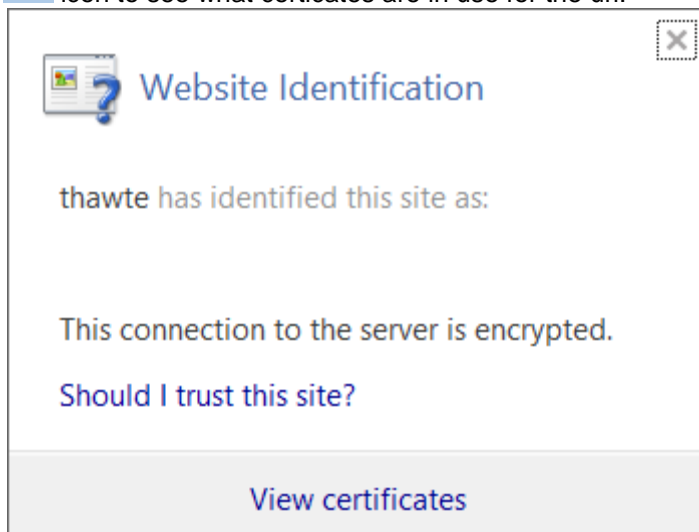
You could then restart your http with the following from the Live console on the server:  
restart task http

## Check out if it works

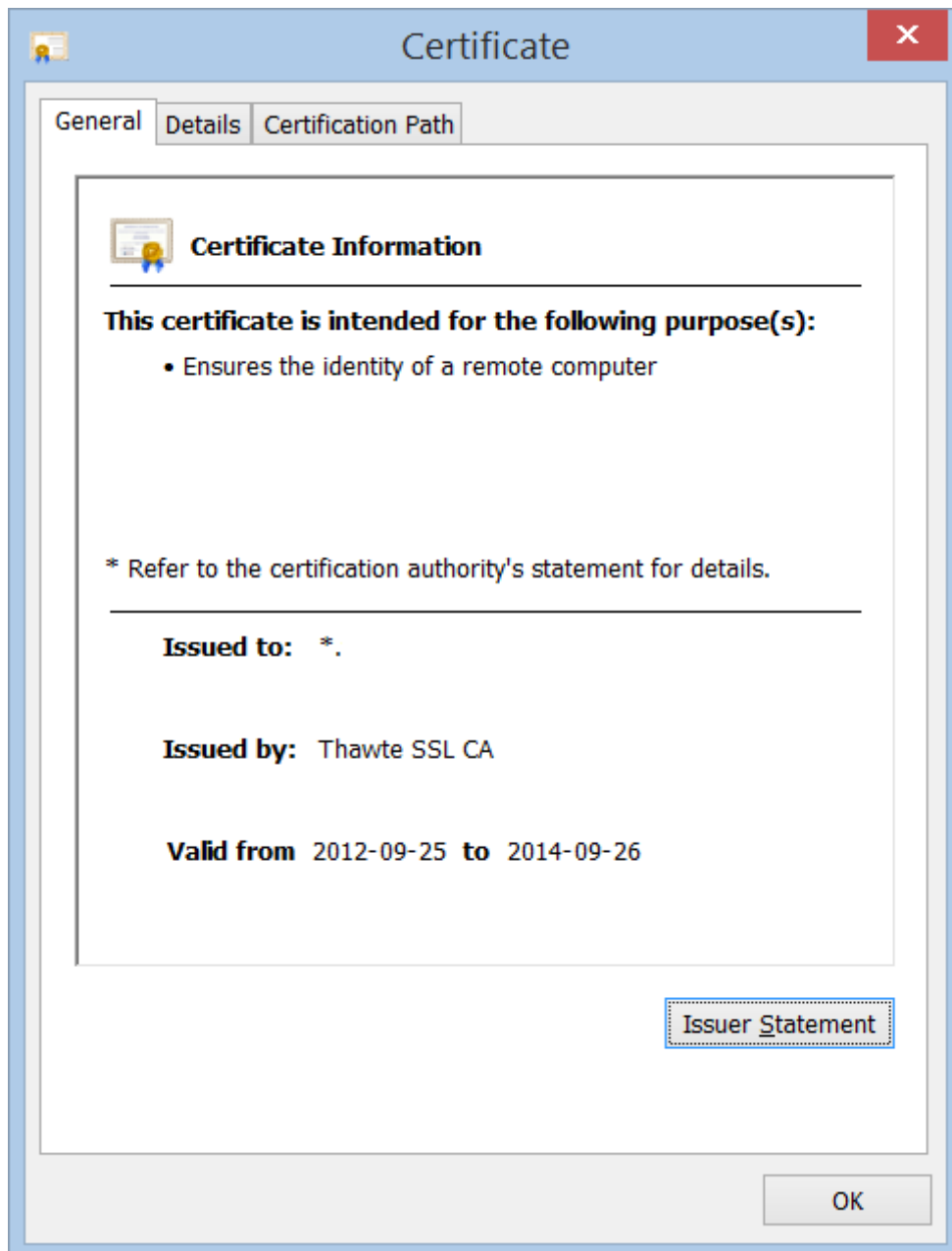
To check this out go to <https://yourserver.yourdomain.yoursuffix> and check that everything is OK.  
In Internet Explorer you can click on the



icon to see what certificates are in use for the url.



View certificates



If you are here now congratulations

## Conclusion