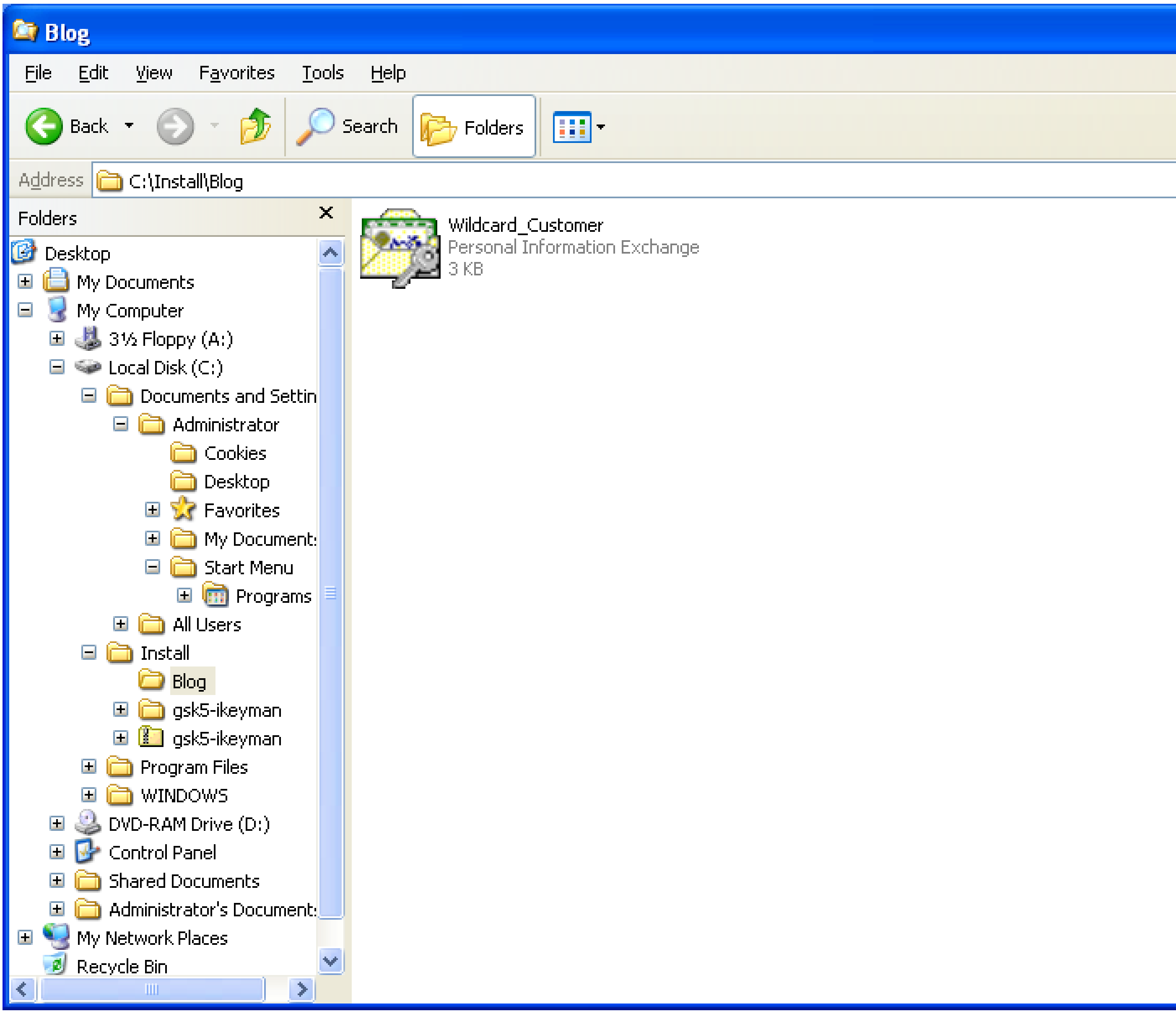
Contents

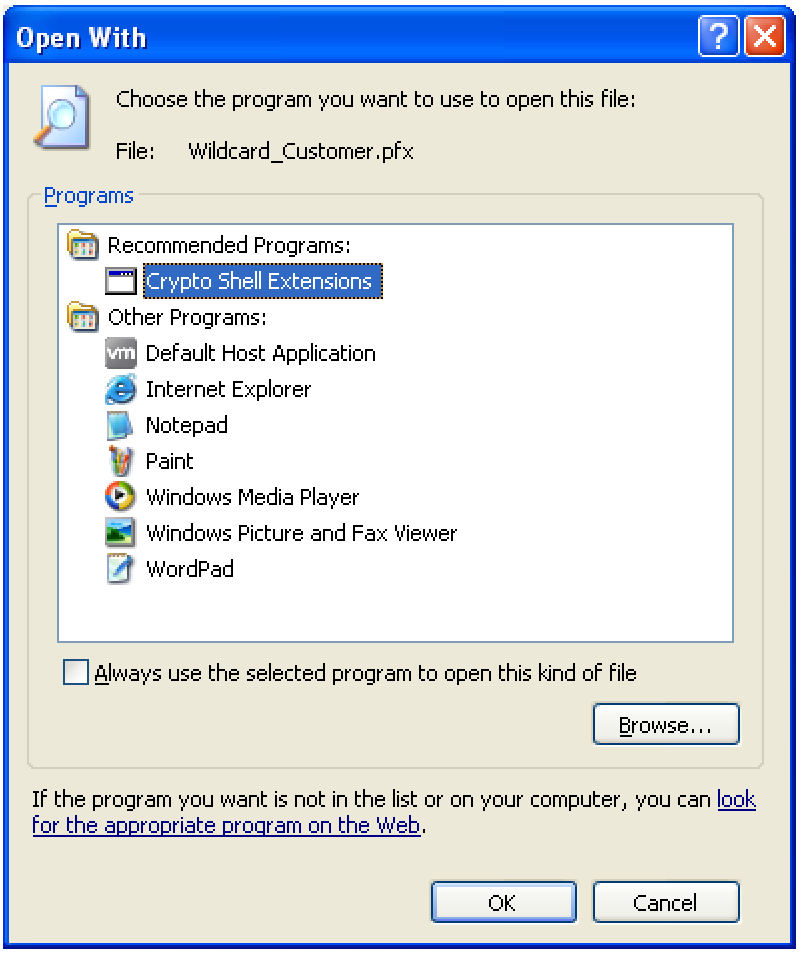
What do I need:

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...



Open With

Choose the program you want to use to open this file:

File: Wildcard_Customer.pfx

Programs

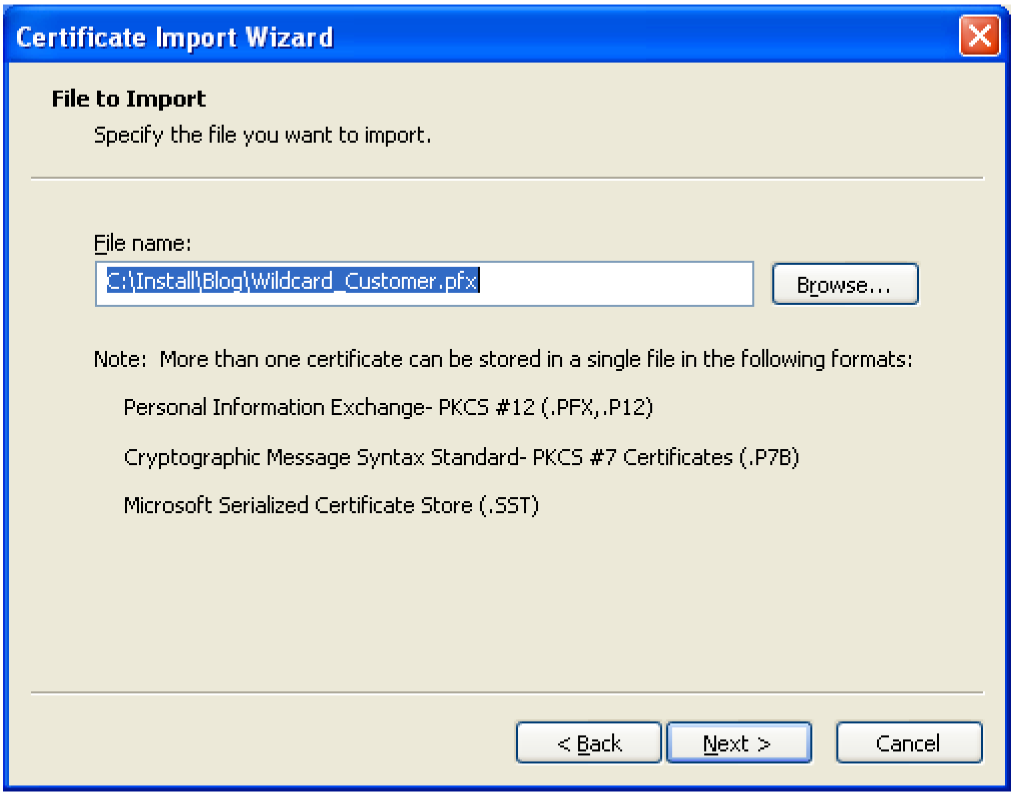
- Recommended Programs:
  - Crypto Shell Extensions
- Other Programs:
  - Default Host Application
  - Internet Explorer
  - Notepad
  - Paint
  - Windows Media Player
  - Windows Picture and Fax Viewer
  - WordPad

□ Always use the selected program to open this kind of file

If the program you want is not in the list or on your computer, you can look for the appropriate program on the Web.

OK

Next >



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name: C:\Install\Blog\Wildcard_Customer.pfx

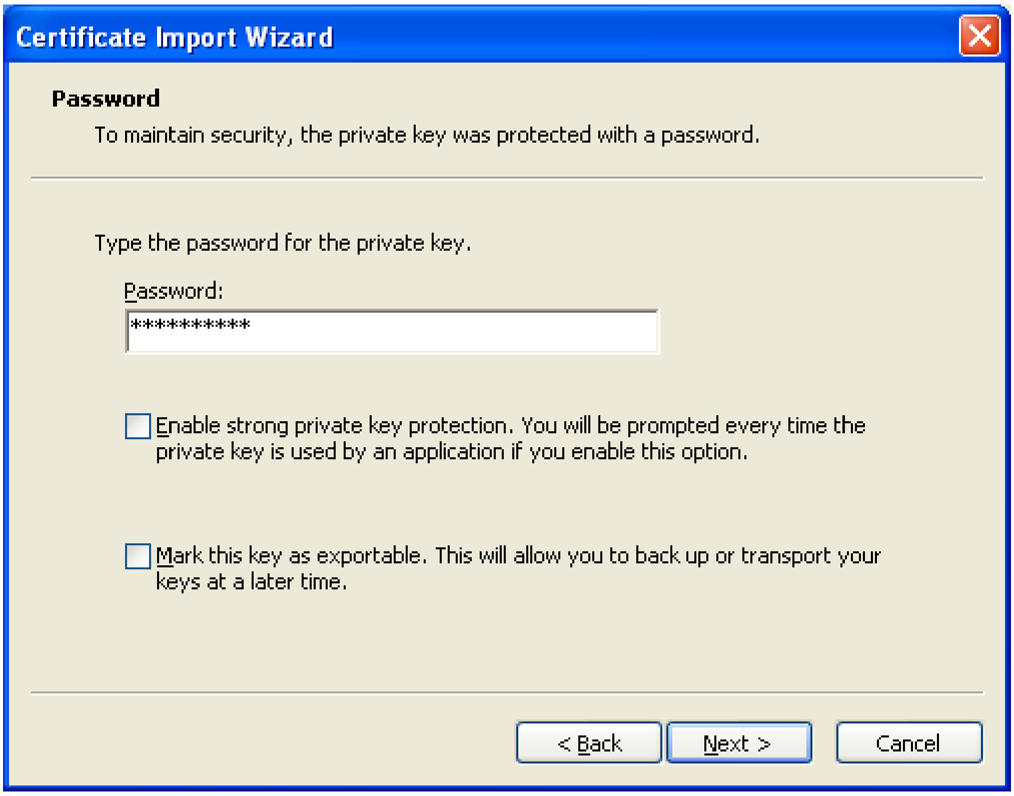
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

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

Microsoft Serialized Certificate Store (.SST)

Next >



Certificate Import Wizard

Password

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

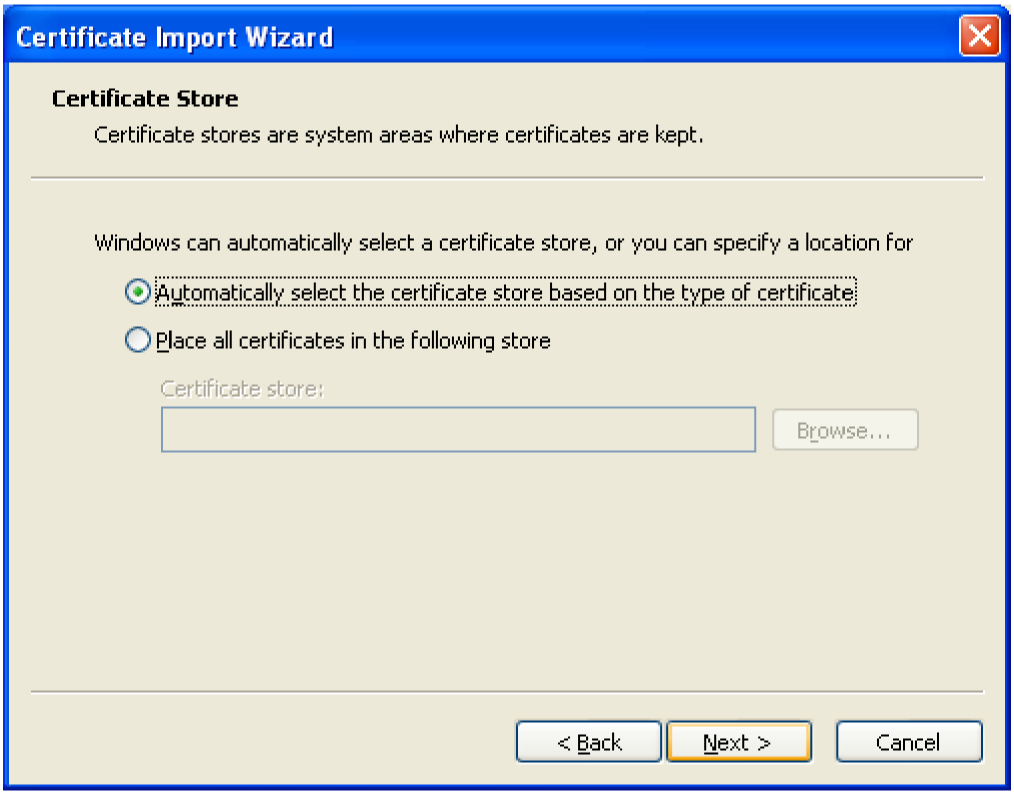
Type the password for the private key.

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.

Next >



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

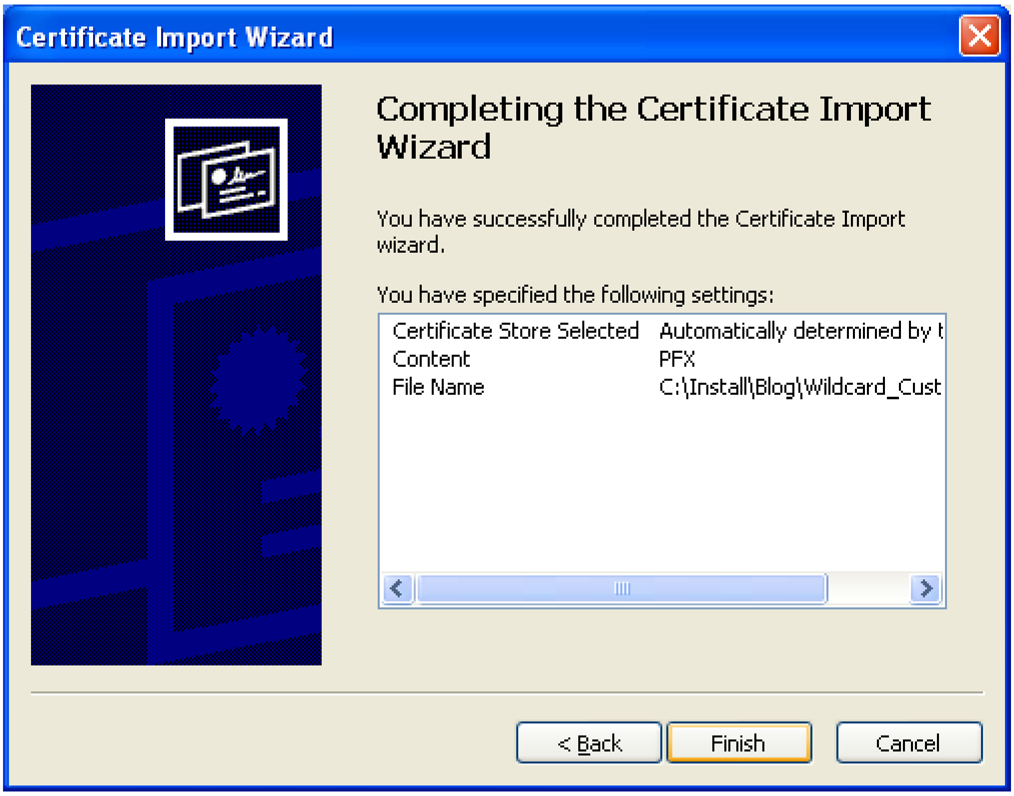
Windows can automatically select a certificate store, or you can specify a location for

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

○ Place all certificates in the following store

Certificate store:

Next >



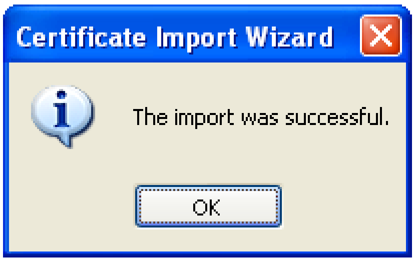
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	C:\Install\Blog\Wildcard_Cust

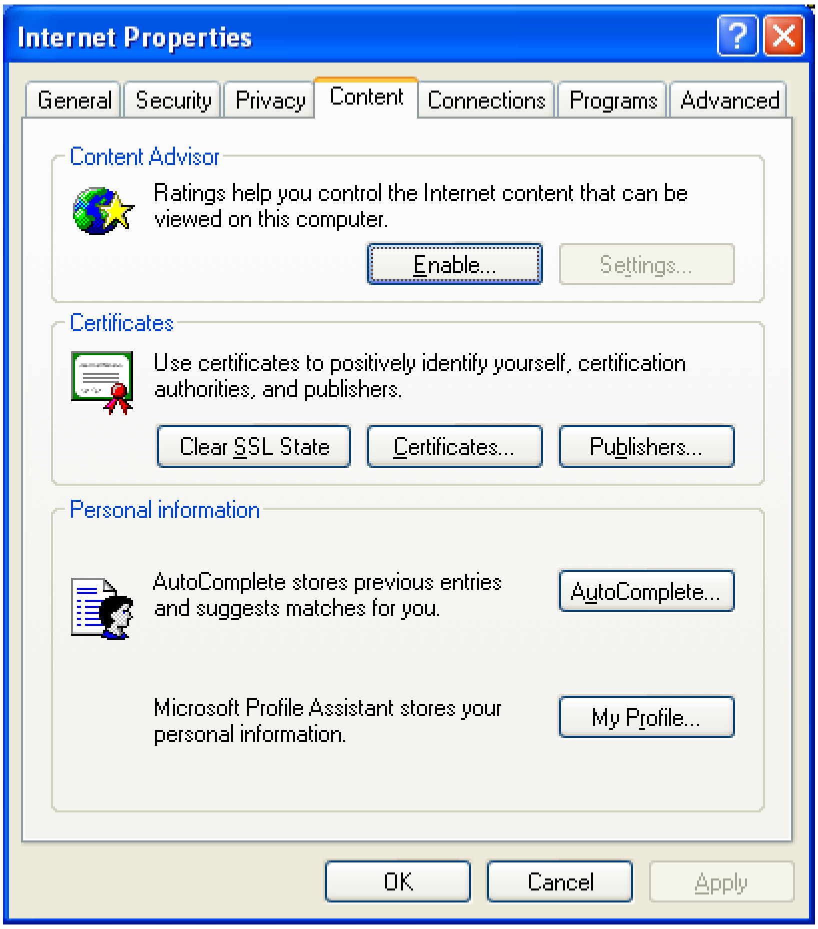
Finish



The import was successful.

OK

2. Check your imported certificate(s)



Content Advisor

Ratings help you control the Internet content that can be viewed on this computer.

Certificates

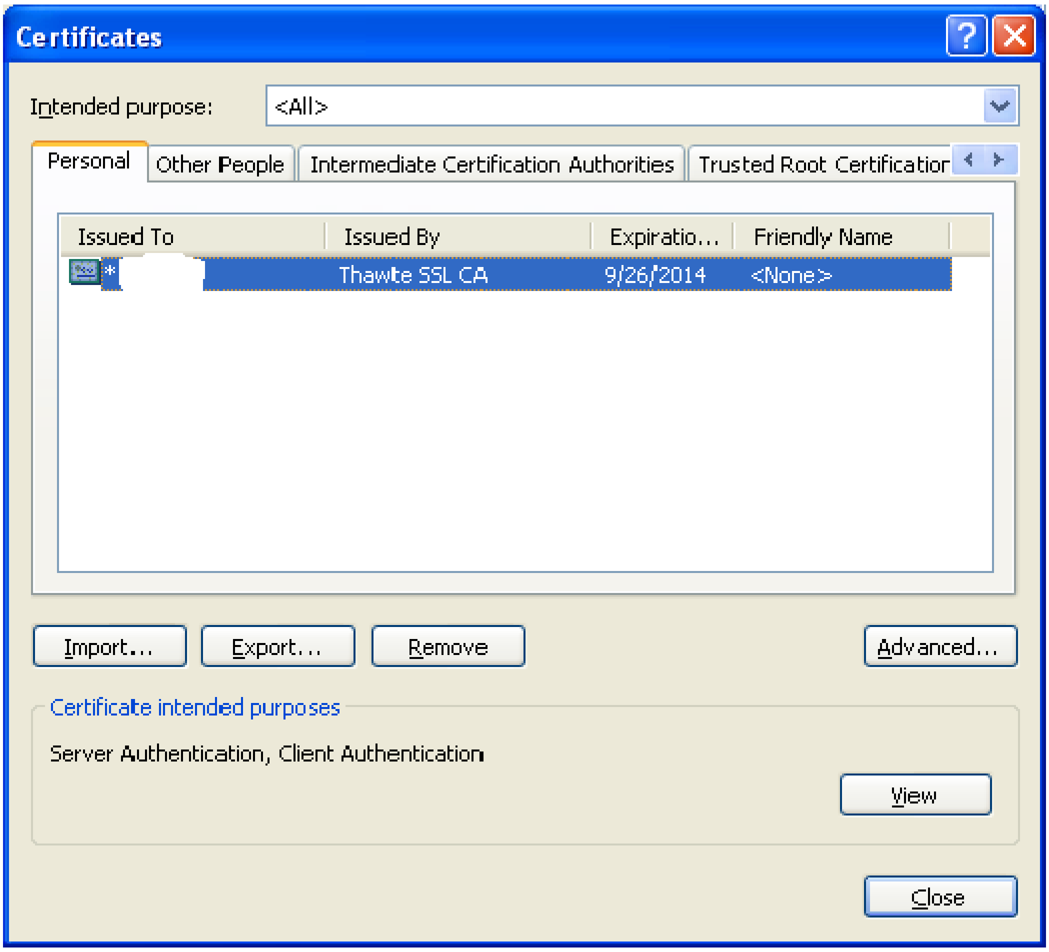
Use certificates to positively identify yourself, certification authorities, and publishers.

Personal information

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Certificates



Certificates

Intended purpose: <All>

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification

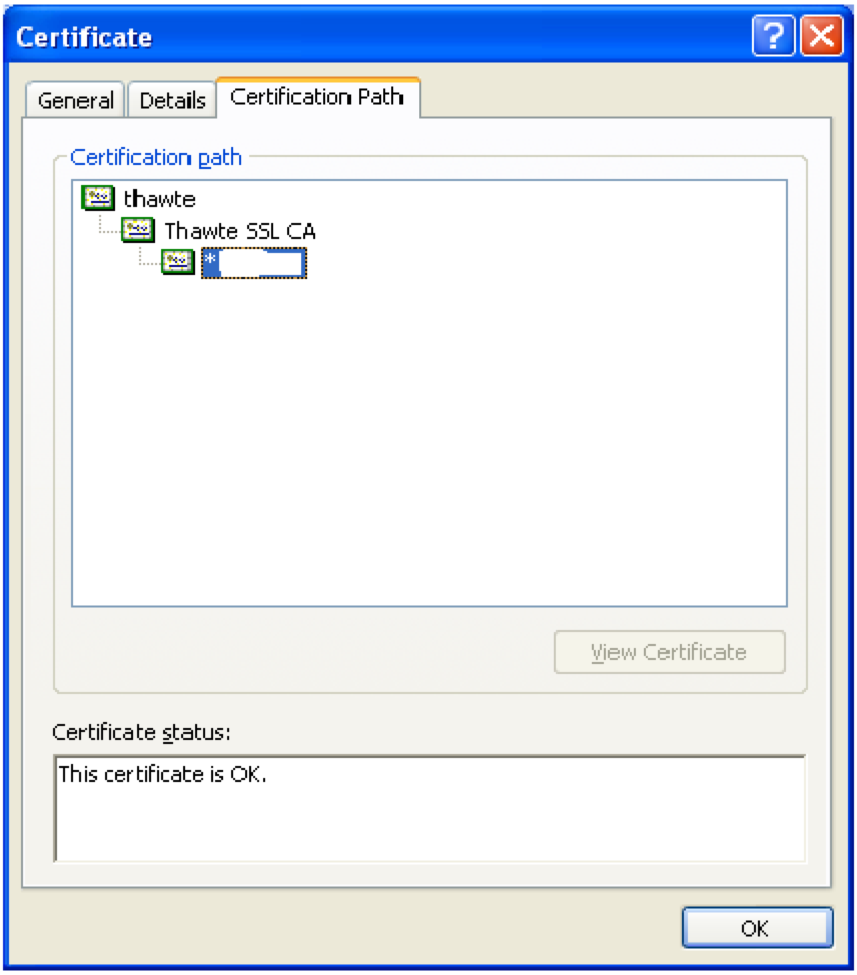
Issued To	Issued By	Expiratio...	Friendly Name
*[redacted]	Thawte SSL CA	9/26/2014	<None>

Import...
Export...
Remove
Advanced...

Certificate intended purposes

Server Authentication, Client Authentication

View

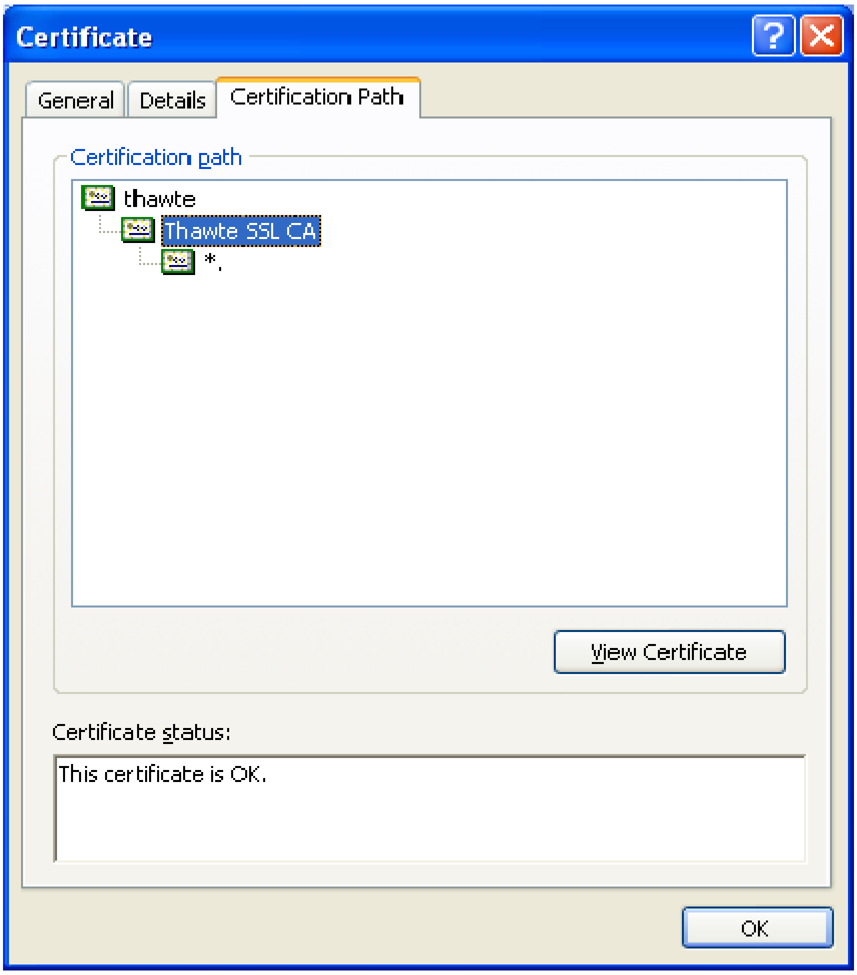


Certification path

- thawte
  - Thawte SSL CA
    - * [redacted]

Certificate status:

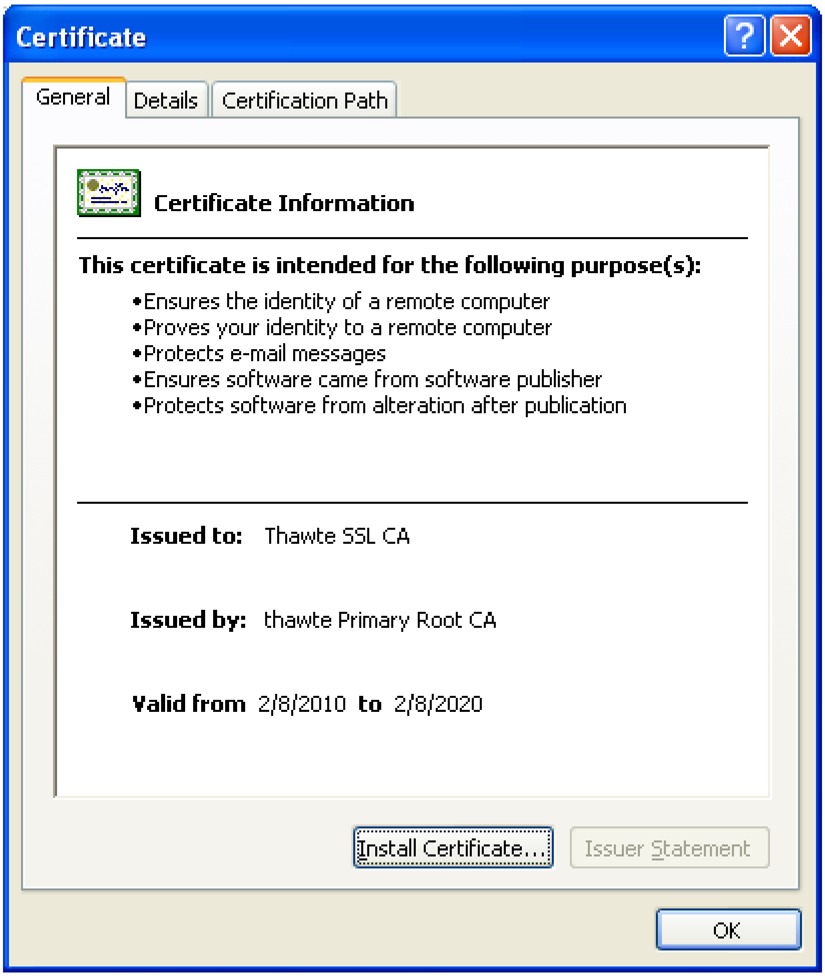
This certificate is OK.



Certificate status:

This certificate is OK.

View Certificate



Certificate Information

This certificate is intended for the following purpose(s):

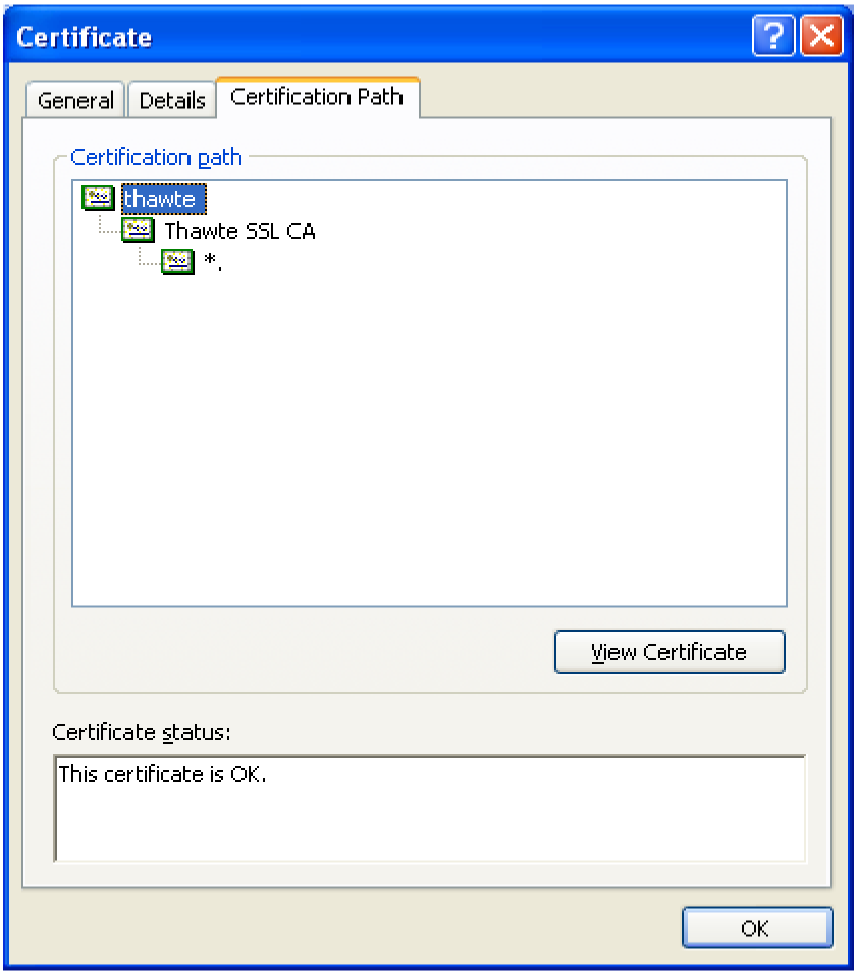
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: Thawte SSL CA

Issued by: thawte Primary Root CA

Valid from 2/8/2010 **to** 2/8/2020

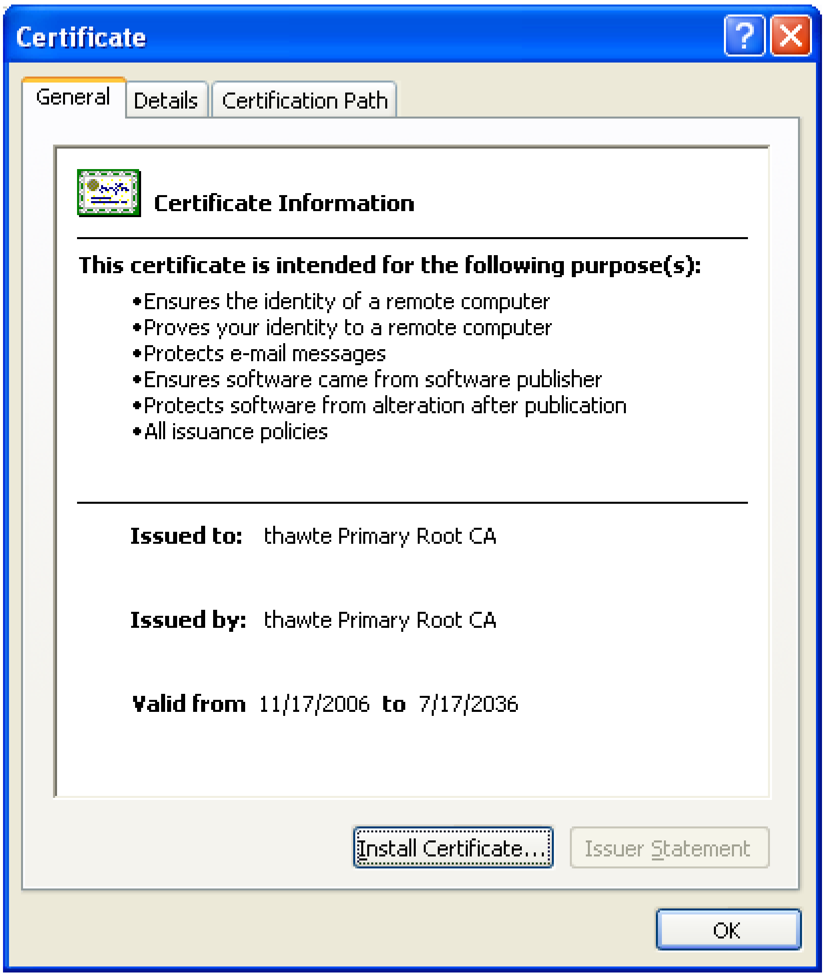
Write down the label on the right of **Issued to:** to use later on inside ikeyman in this case it is:
Thawte SSL CA
OK



Certificate status:

This certificate is OK.

View Certificate



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- All issuance policies

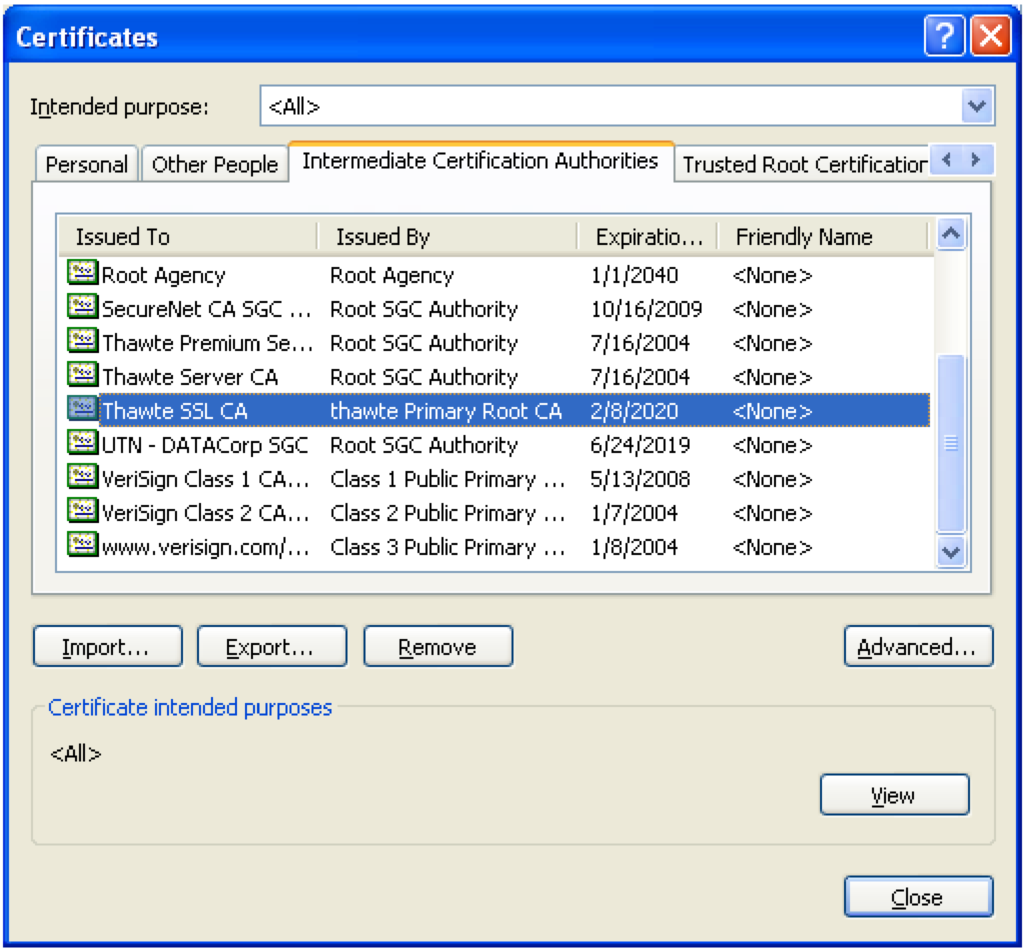
Issued to: thawte Primary Root CA

Issued by: thawte Primary Root CA

Valid from 11/17/2006 to 7/17/2036

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

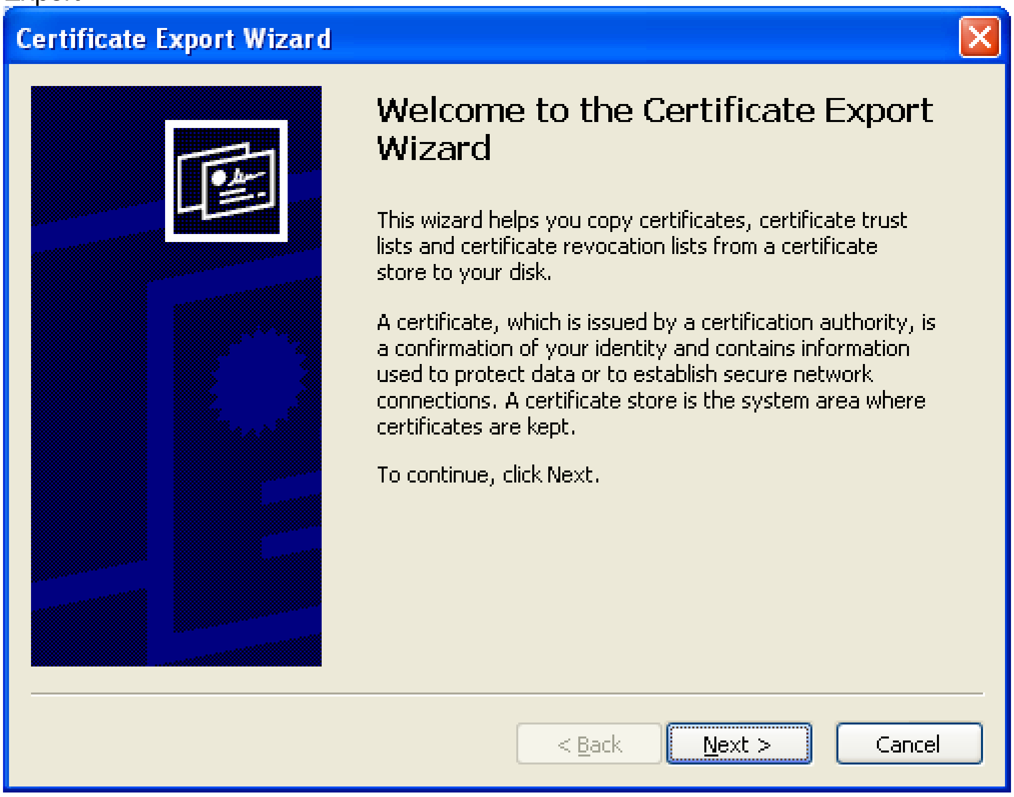

Certificates
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Root Agency	Root Agency	1/1/2040	<None>
SecureNet CA SGC ...	Root SGC Authority	10/16/2009	<None>
Thawte Premium Se...	Root SGC Authority	7/16/2004	<None>
Thawte Server CA	Root SGC Authority	7/16/2004	<None>
Thawte SSL CA	thawte Primary Root CA	2/8/2020	<None>
UTN - DATACorp SGC	Root SGC Authority	6/24/2019	<None>
VeriSign Class 1 CA...	Class 1 Public Primary ...	5/13/2008	<None>
VeriSign Class 2 CA...	Class 2 Public Primary ...	1/7/2004	<None>
www.verisign.com/...	Class 3 Public Primary ...	1/8/2004	<None>

<All>

Export



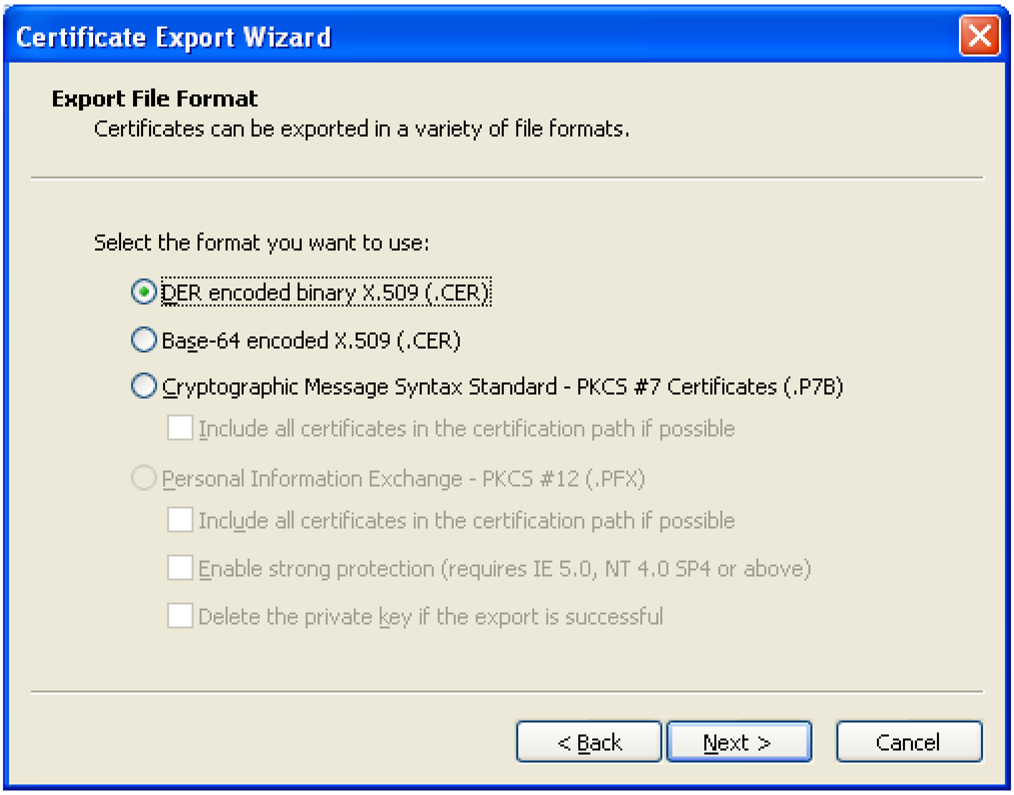
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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

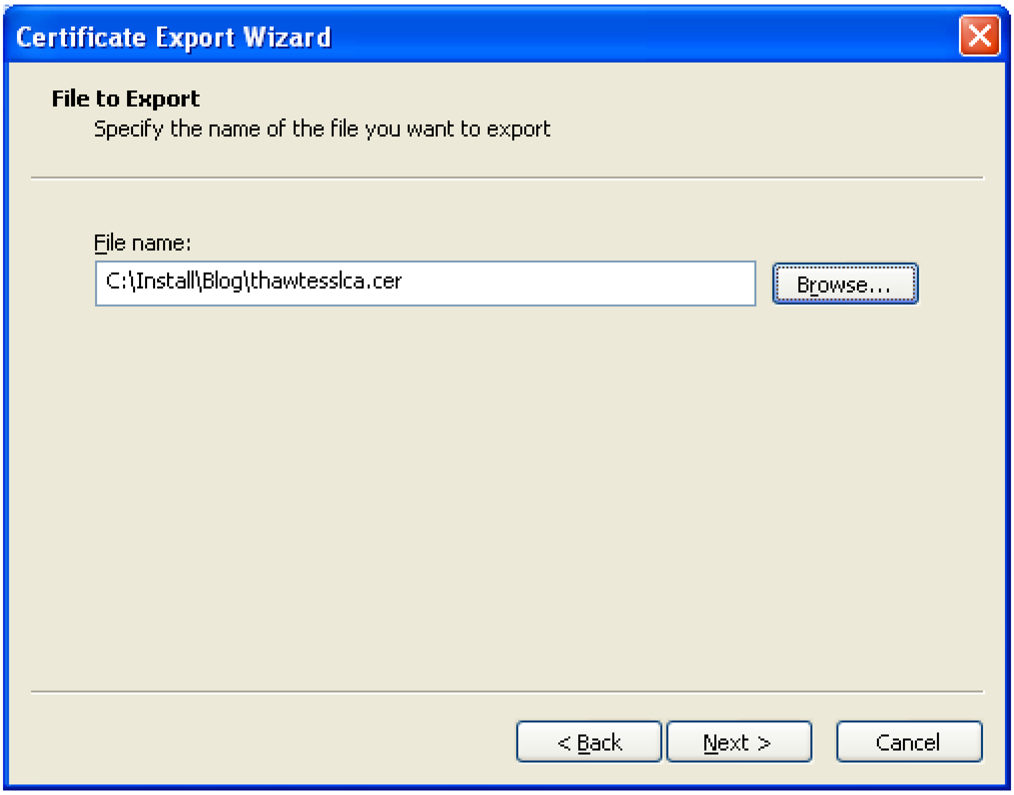
○ Personal Information Exchange - PKCS #12 (.PFX)

□ 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 >



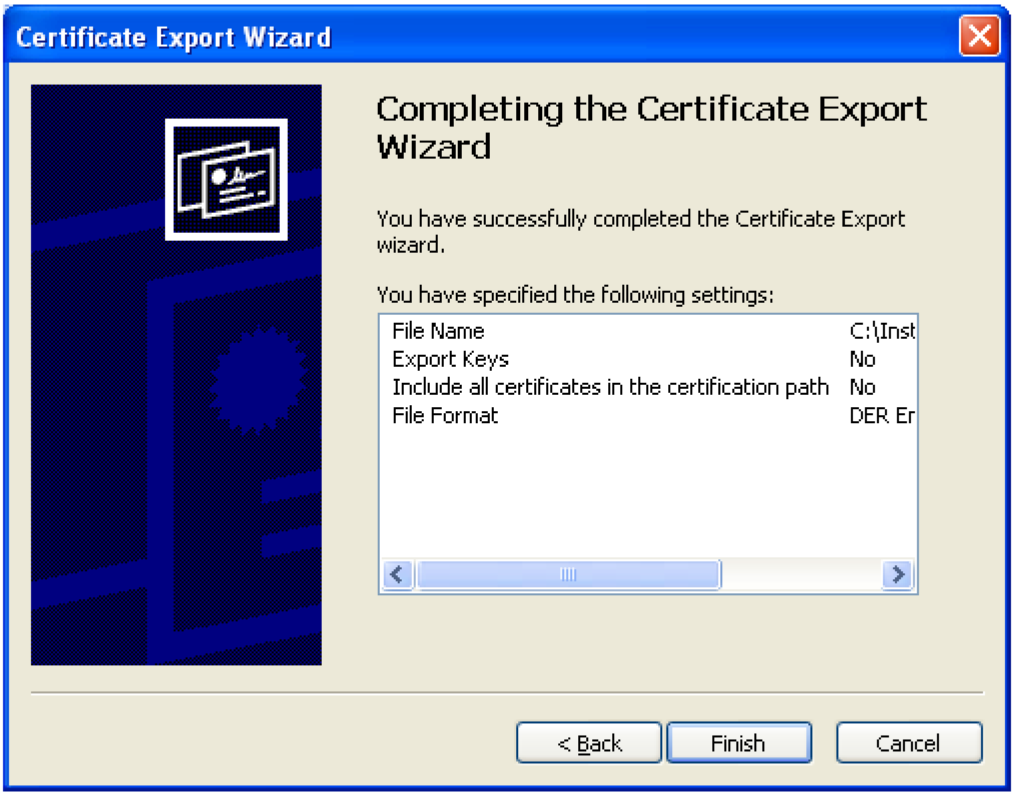
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: C:\Install\Blog\thawtesslca.cer

Next >



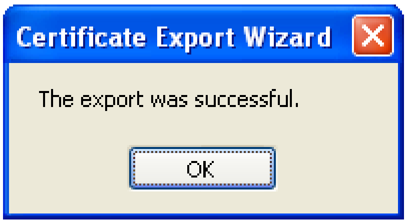
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

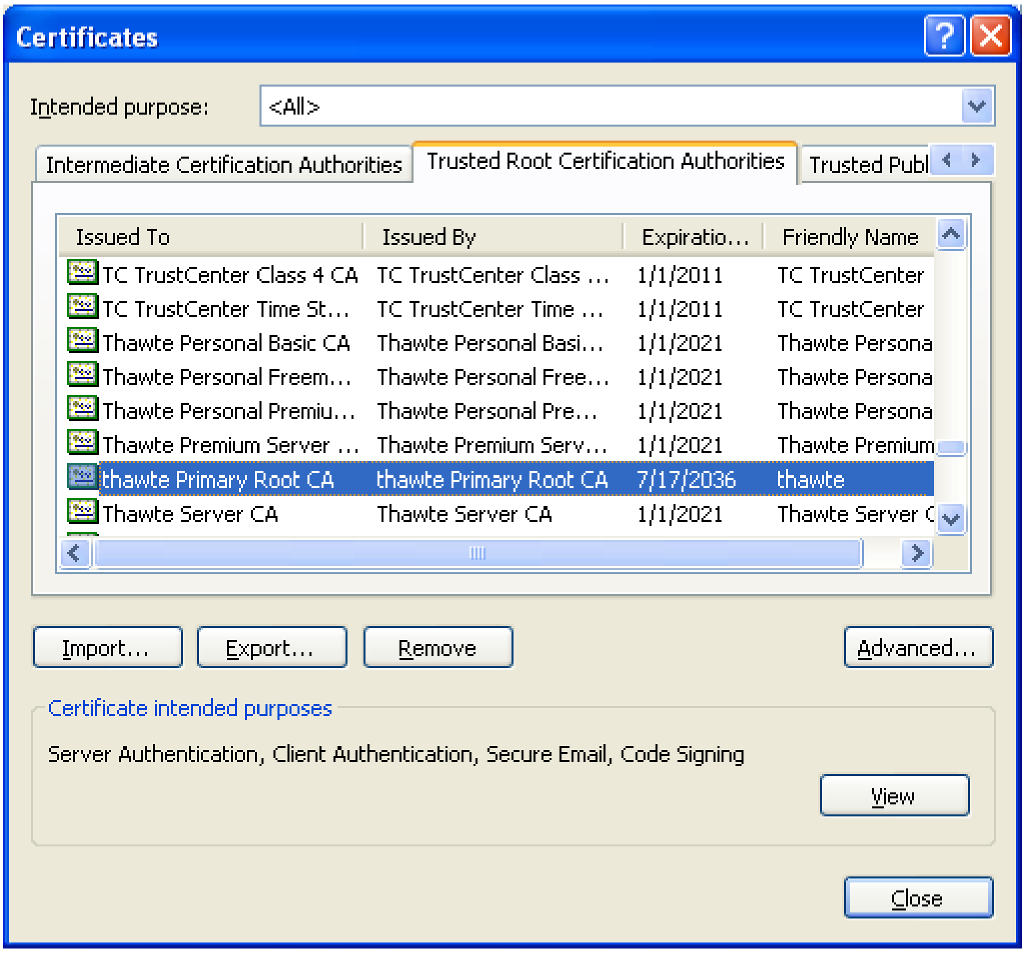
File Name	C:\Inst
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Er

Finish



The export was successful.

OK



Intended purpose: <All>

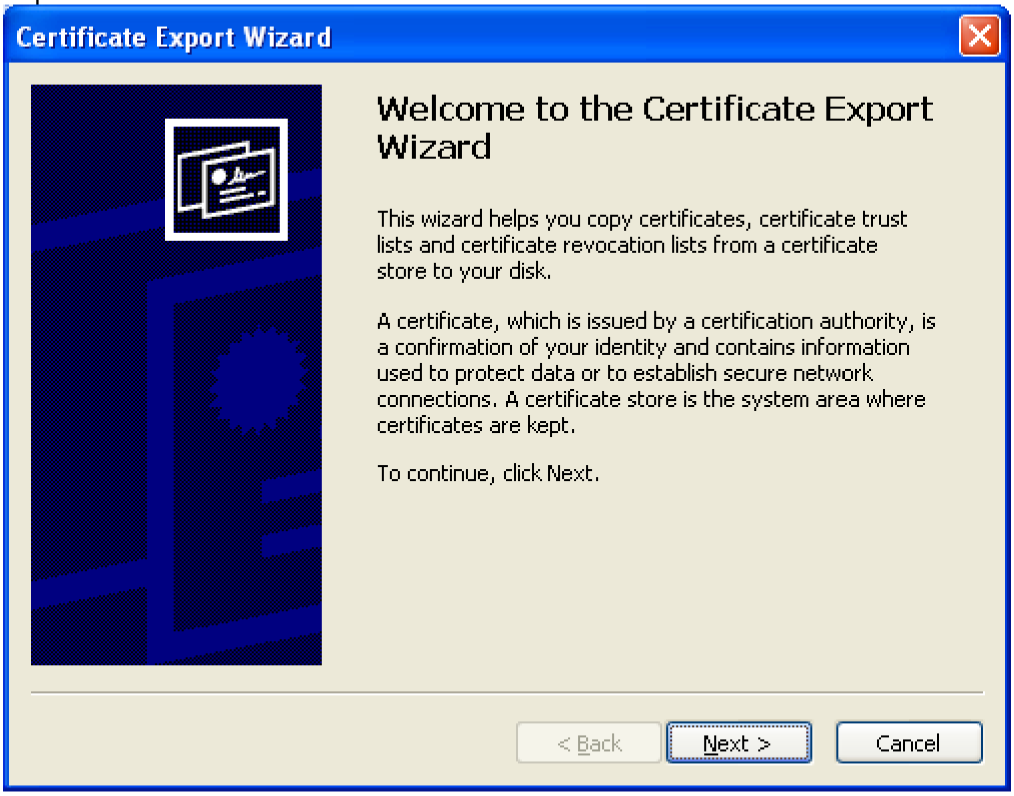
Intermediate Certification Authorities | Trusted Root Certification Authorities | Trusted Publ

Issued To	Issued By	Expiratio...	Friendly Name
TC TrustCenter Class 4 CA	TC TrustCenter Class ...	1/1/2011	TC TrustCenter
TC TrustCenter Time St...	TC TrustCenter Time ...	1/1/2011	TC TrustCenter
Thawte Personal Basic CA	Thawte Personal Basi...	1/1/2021	Thawte Persona
Thawte Personal Freem...	Thawte Personal Free...	1/1/2021	Thawte Persona
Thawte Personal Premiu...	Thawte Personal Pre...	1/1/2021	Thawte Persona
Thawte Premium Server ...	Thawte Premium Serv...	1/1/2021	Thawte Premium
thawte Primary Root CA	thawte Primary Root CA	7/17/2036	thawte
Thawte Server CA	Thawte Server CA	1/1/2021	Thawte Server C

Certificate intended purposes

Server Authentication, Client Authentication, Secure Email, Code Signing

Export



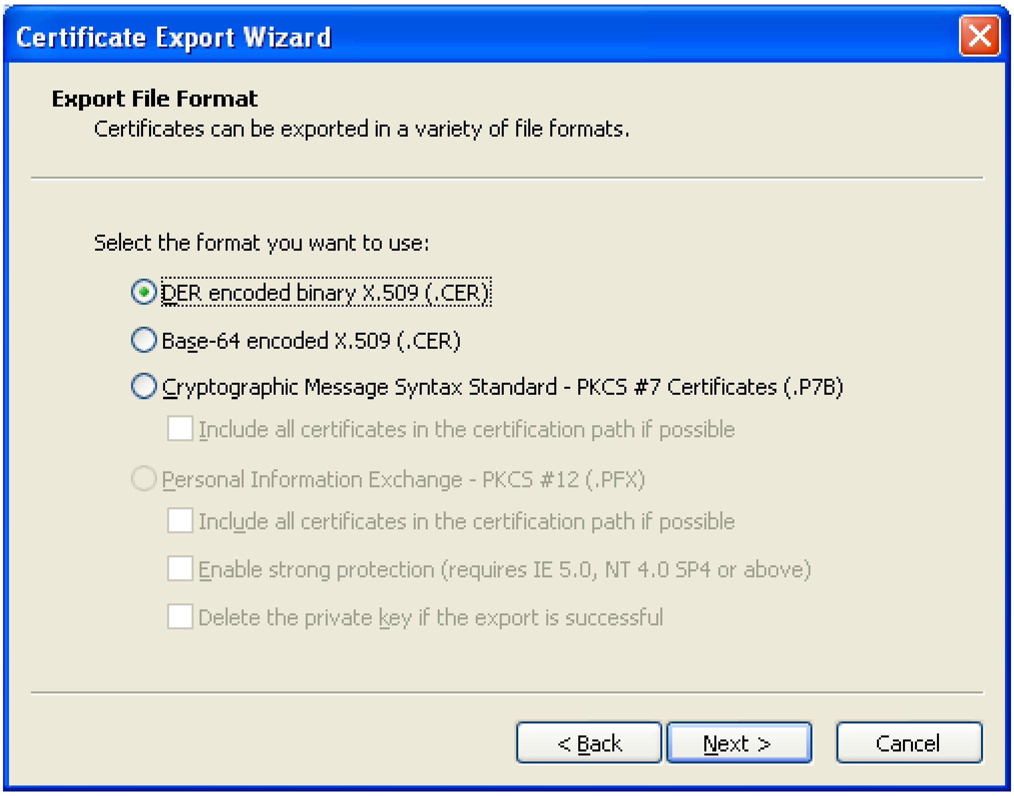
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Next >

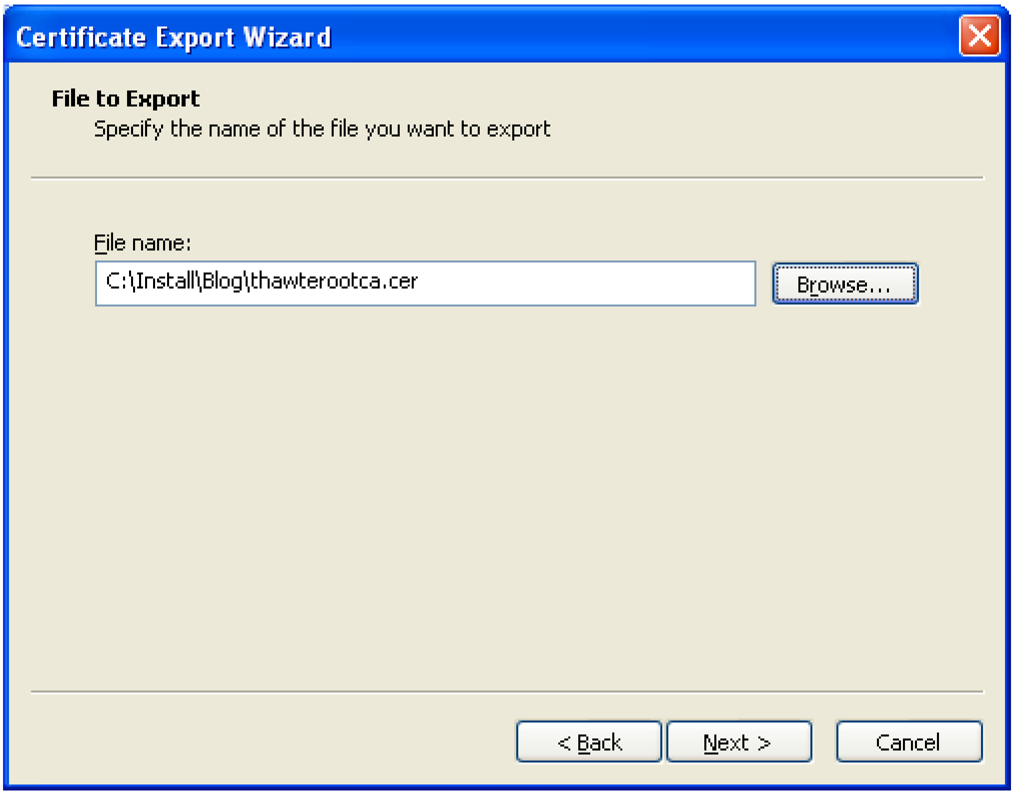

Certificate Export Wizard

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

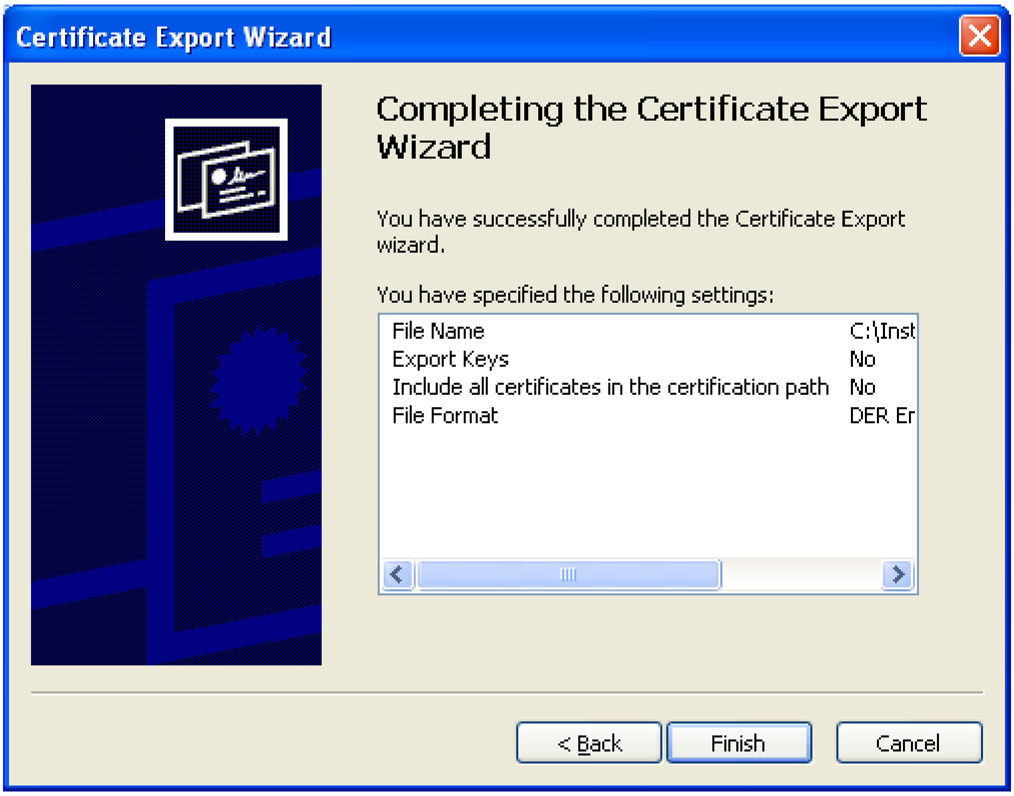
Next >


Certificate Export Wizard

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

File name: C:\Install\Blog\thawterootca.cer

Next >



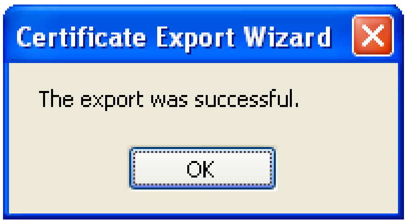
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

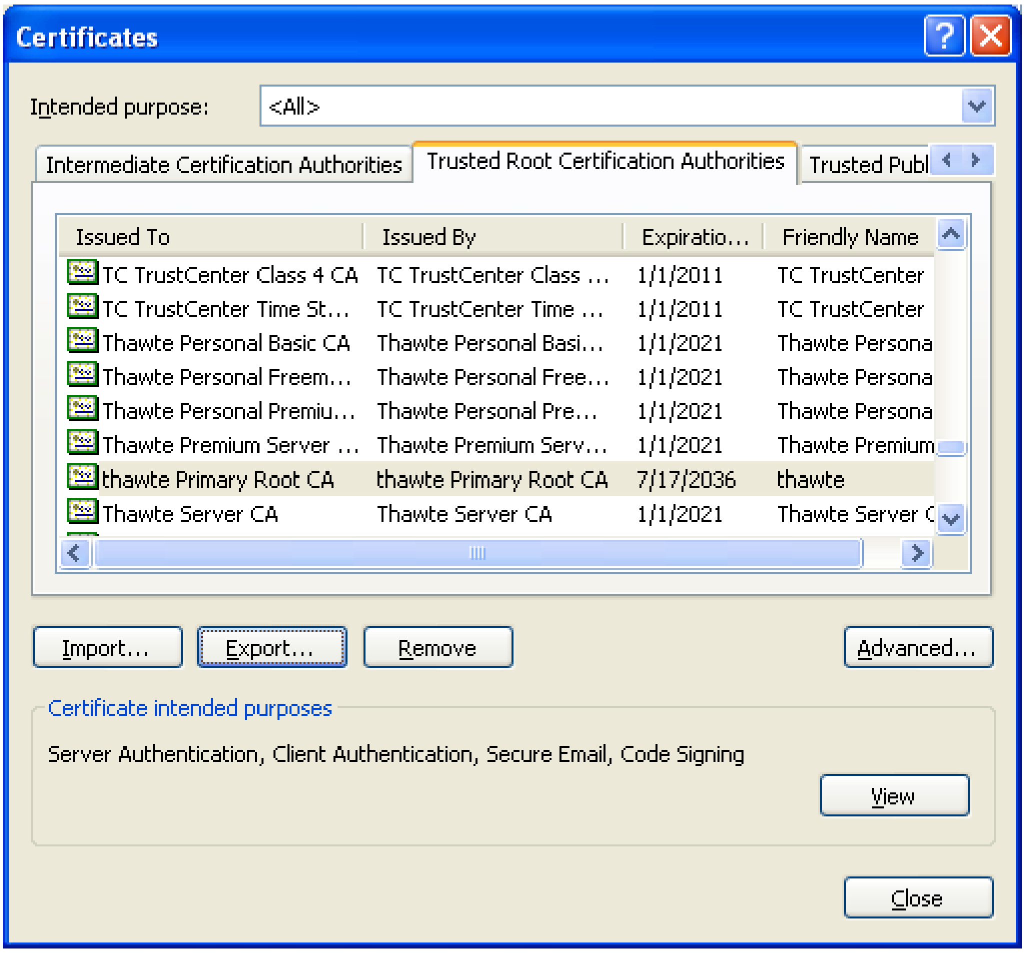
File Name	C:\Inst
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Er

Finish



The export was successful.

OK

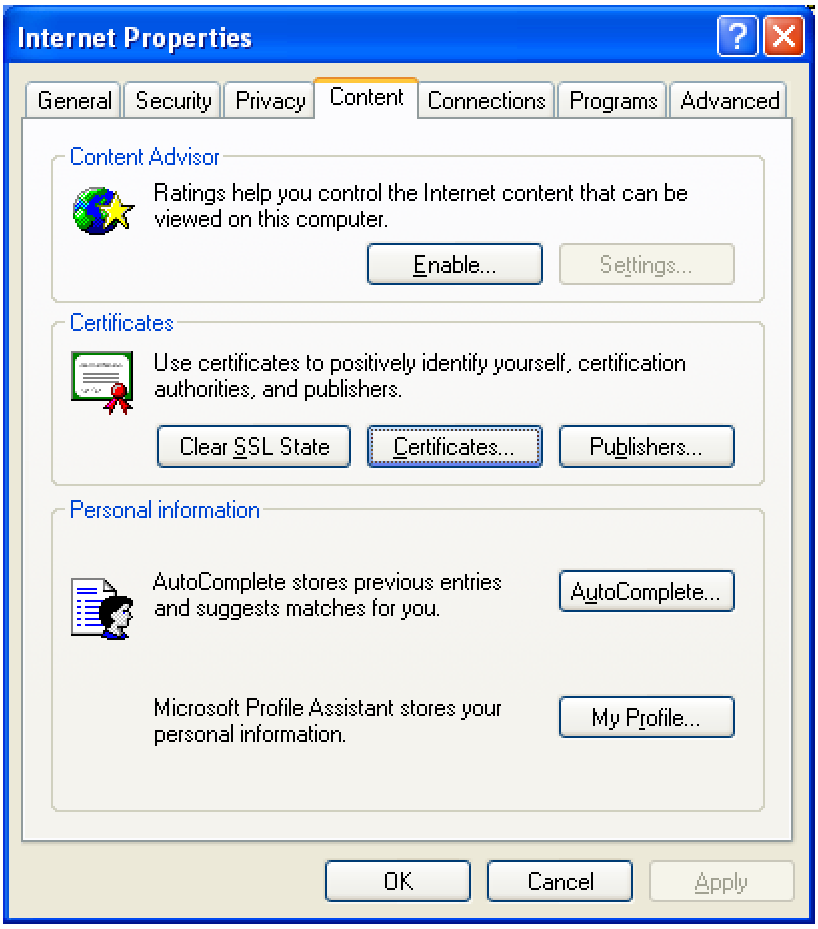

Certificates
Intended purpose:
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
TC TrustCenter Class 4 CA	TC TrustCenter Class ...	1/1/2011	TC TrustCenter
TC TrustCenter Time St...	TC TrustCenter Time ...	1/1/2011	TC TrustCenter
Thawte Personal Basic CA	Thawte Personal Basi...	1/1/2021	Thawte Persona
Thawte Personal Freem...	Thawte Personal Free...	1/1/2021	Thawte Persona
Thawte Personal Premiu...	Thawte Personal Pre...	1/1/2021	Thawte Persona
Thawte Premium Server ...	Thawte Premium Serv...	1/1/2021	Thawte Premium
thawte Primary Root CA	thawte Primary Root CA	7/17/2036	thawte
Thawte Server CA	Thawte Server CA	1/1/2021	Thawte Server C

Server Authentication, Client Authentication, Secure Email, Code Signing

Close



Internet Properties

General | Security | Privacy | Content | Connections | Programs | Advanced

Content Advisor

Ratings help you control the Internet content that can be viewed on this computer.

Certificates

Use certificates to positively identify yourself, certification authorities, and publishers.

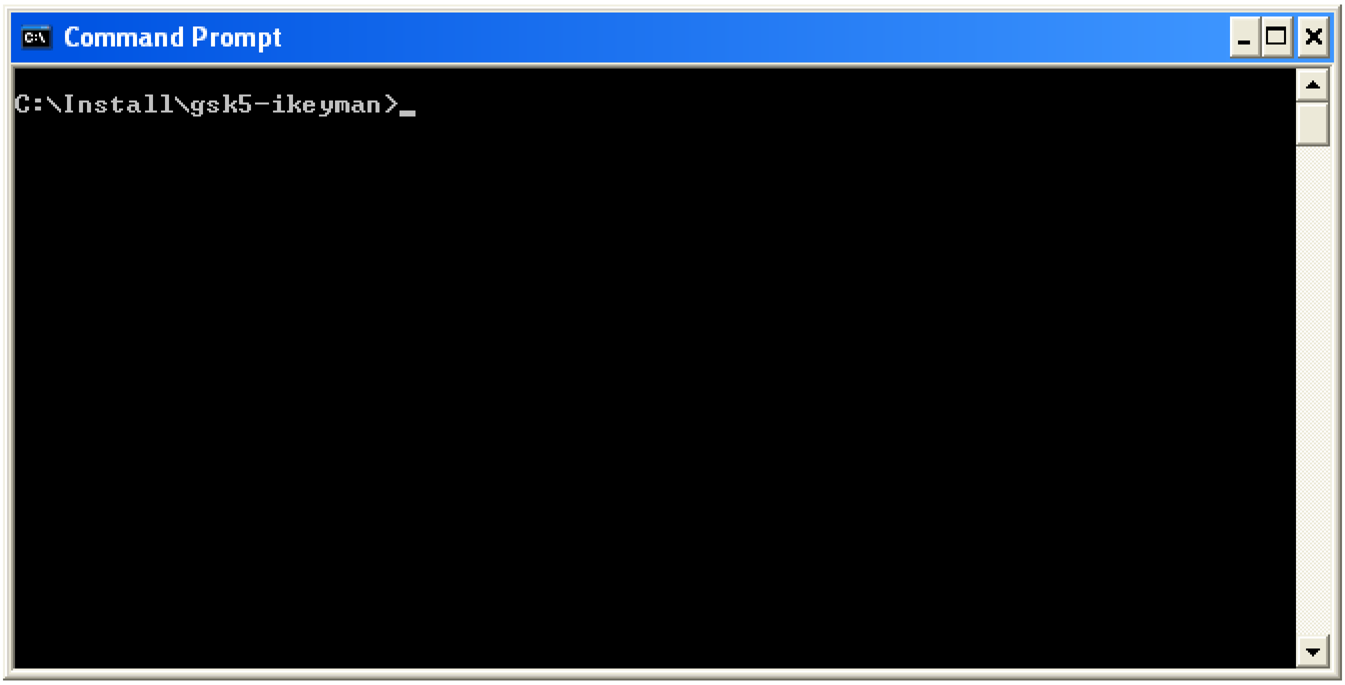
Personal information

AutoComplete stores previous entries and suggests matches for you.

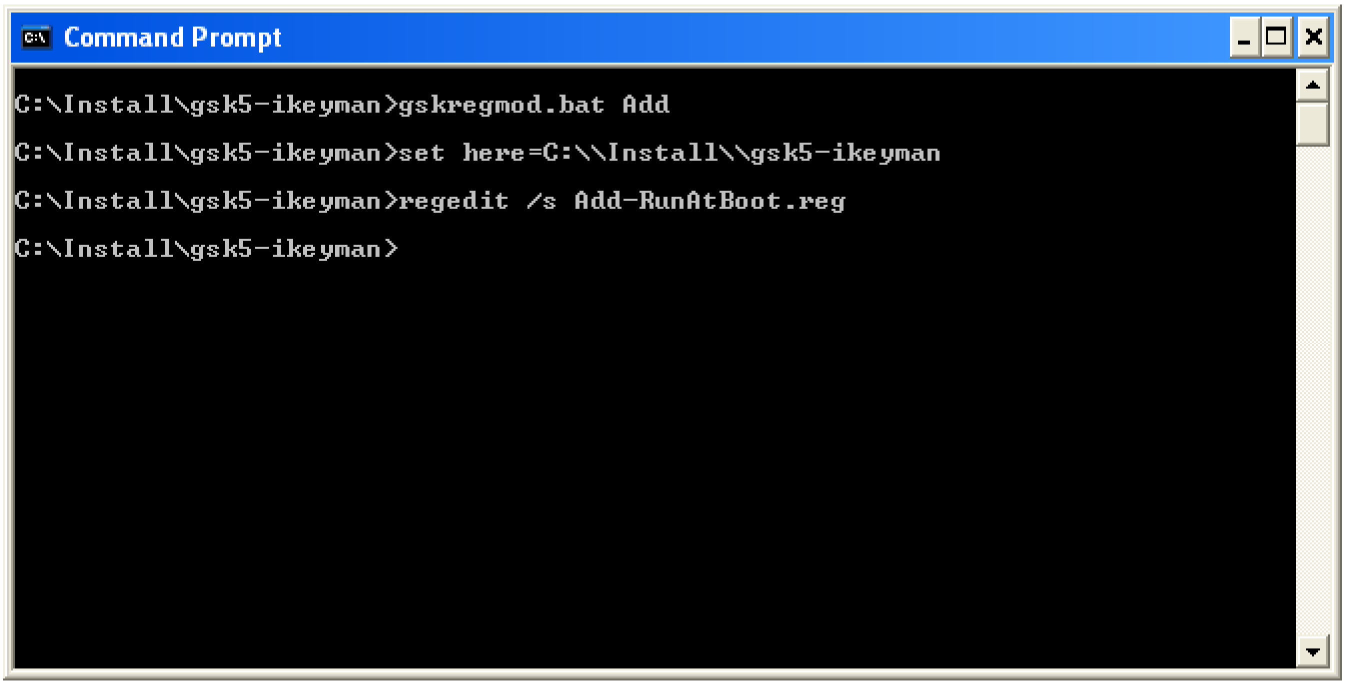
Microsoft Profile Assistant stores your personal information.

OK

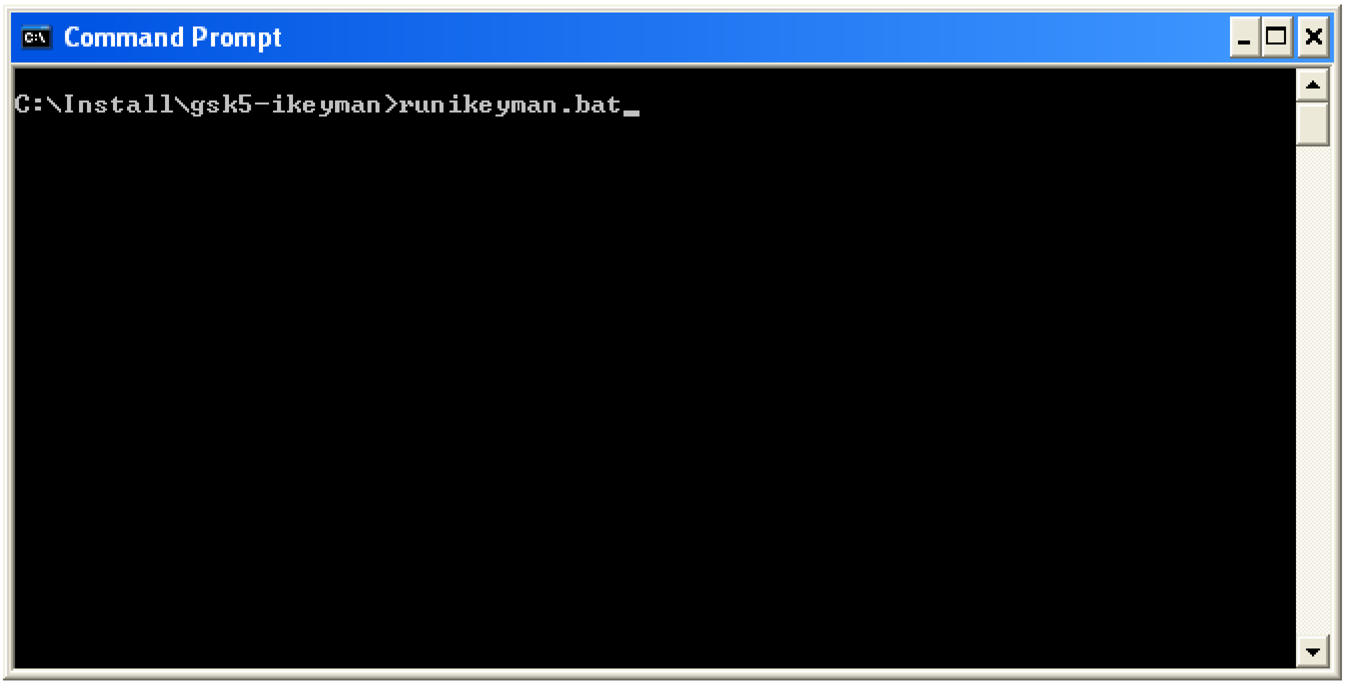
Run iKeyman to create new kyrfile and then Add and Import certificate information



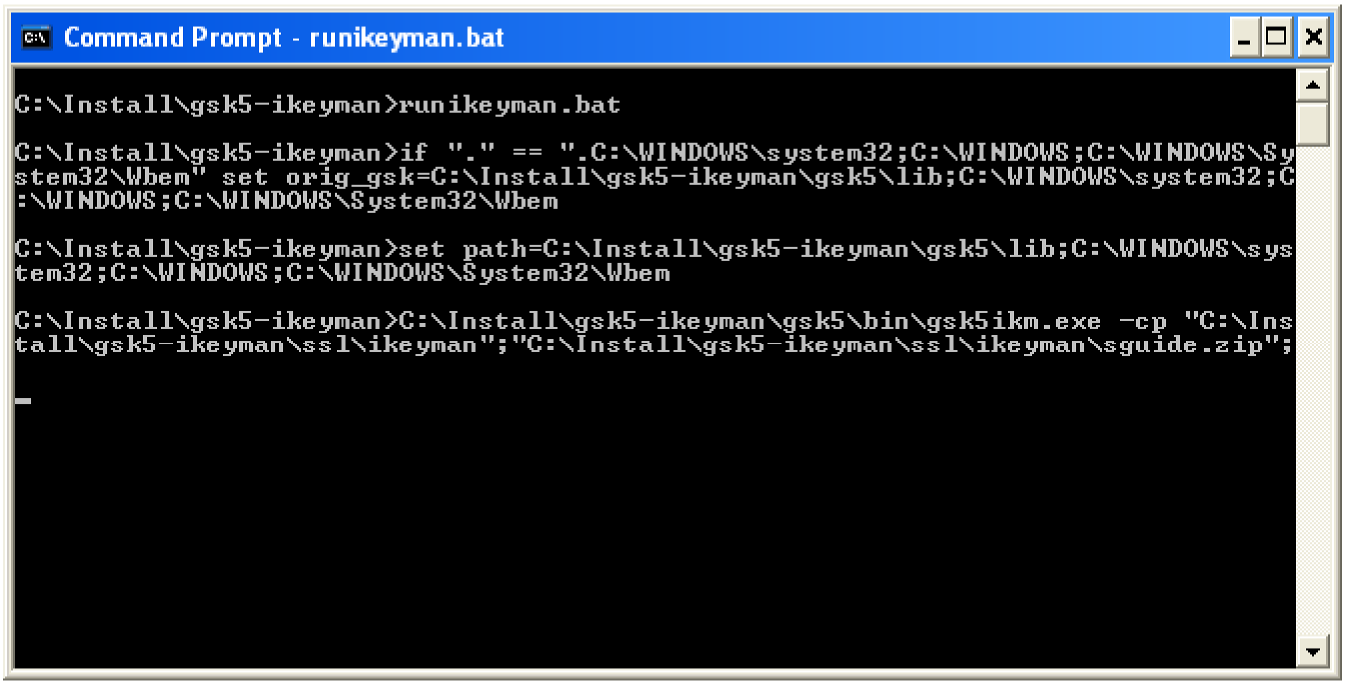
```
C:\Install\gsk5-ikeyman>_
```



```
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>
```

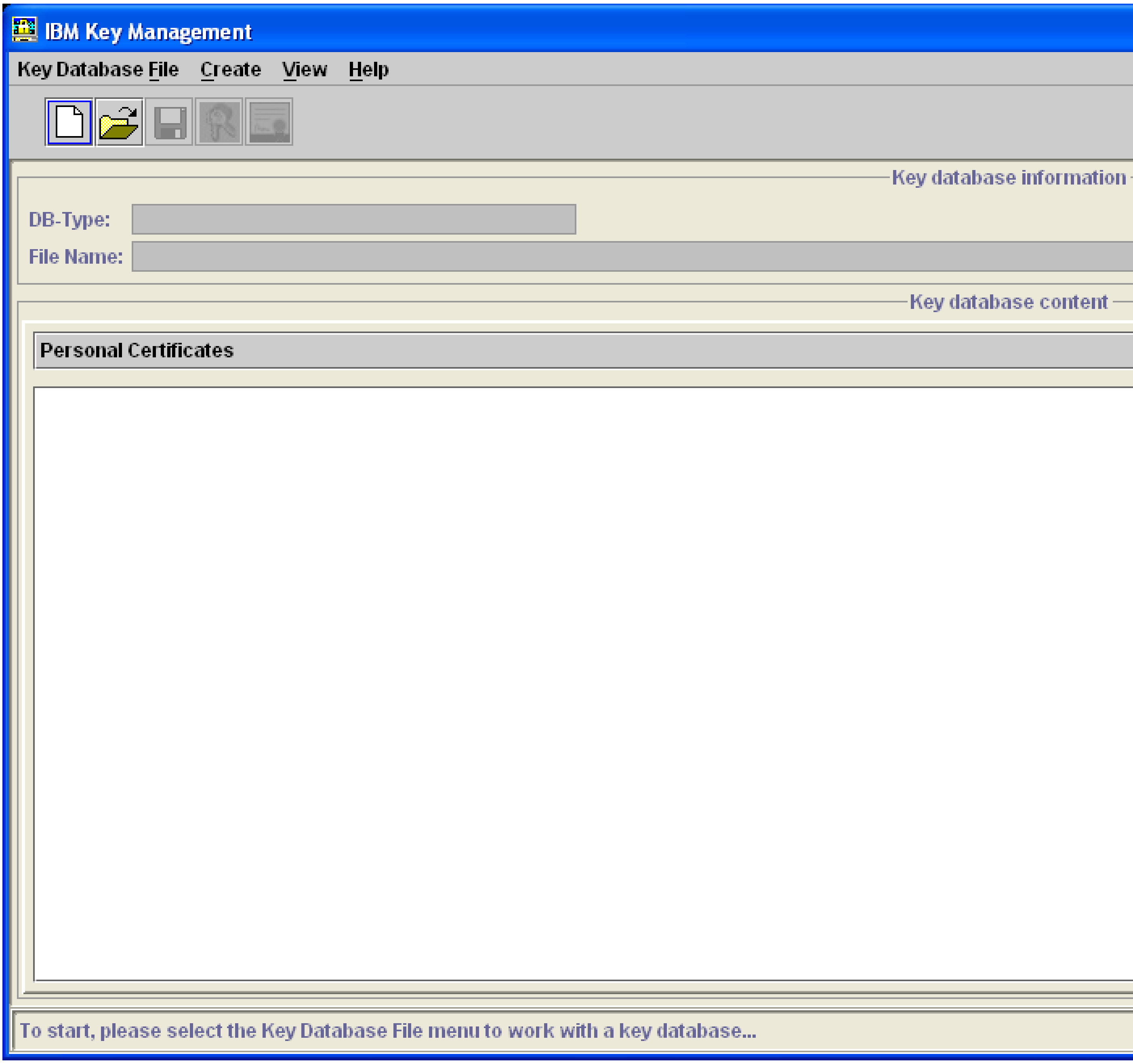


```
C:\Install\gsk5-ikeyman>runikeyman.bat_
```



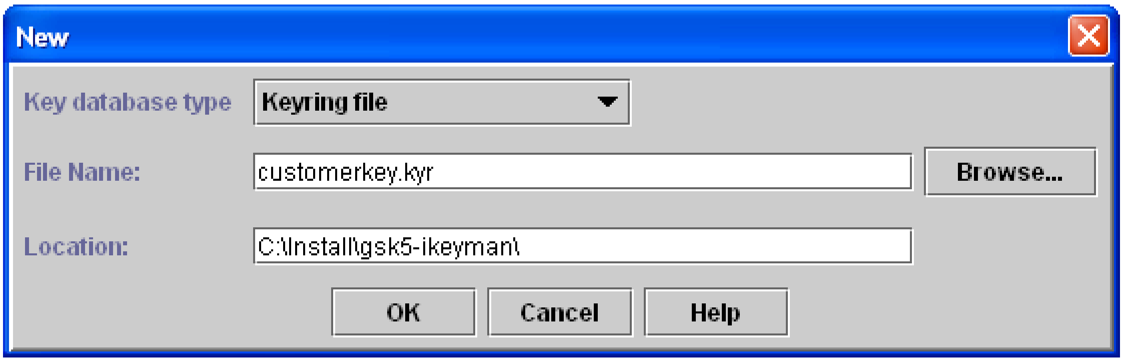
```
C:\Install\gsk5-ikeyman>runikeyman.bat

C:\Install\gsk5-ikeyman>if "." == ".C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\Sy
stem32\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\sys
tem32;C:\WINDOWS;C:\WINDOWS\System32\Wbem

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

_
```

Could take a while to start



To start, please select the Key Database File menu to work with a key database...

Key Database File
New

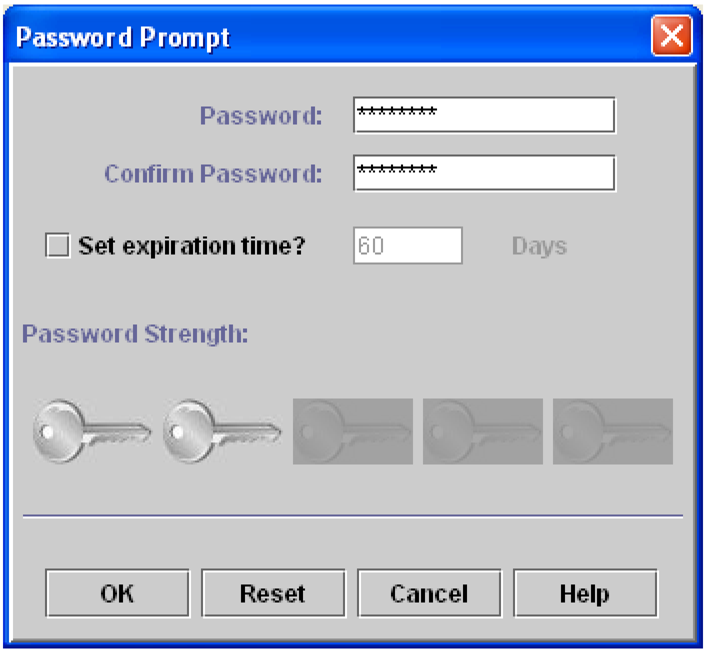


Key database type: Keyring file

File Name: customerkey.kyr

Location: C:\Install\gsk5-ikeyman\

OK



Password Prompt

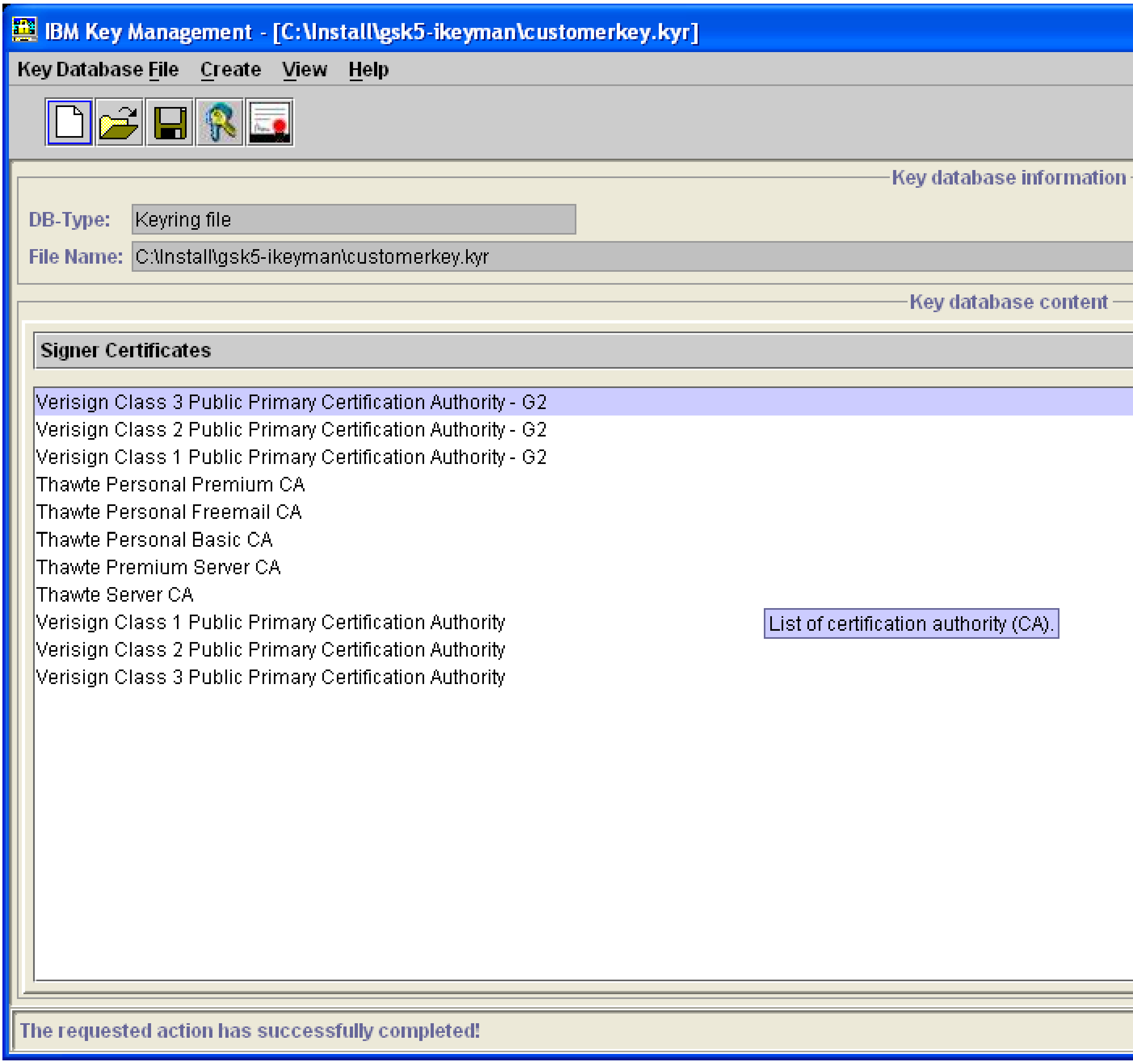
Password: *********

Confirm Password: *********

□ Set expiration time? 60 Days

Password Strength:

OK



DB-Type: Keyring file

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

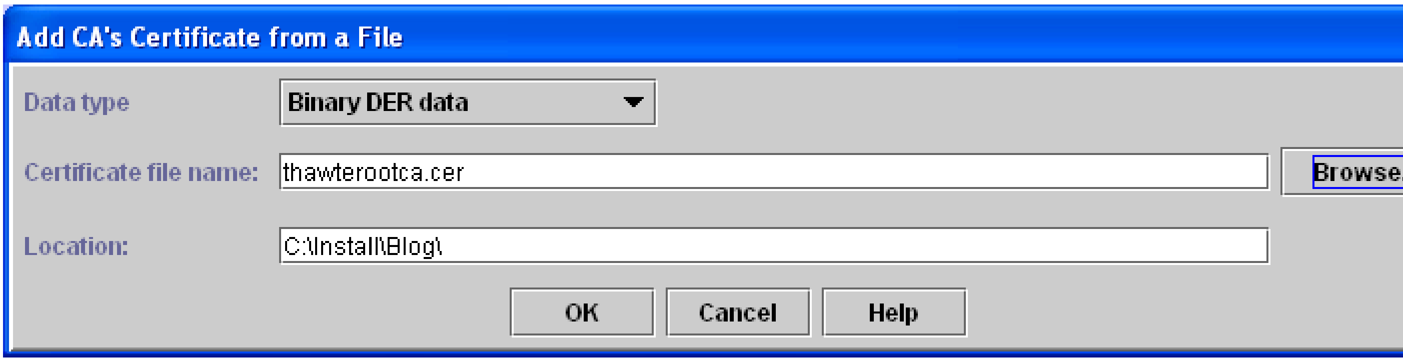
Signer Certificates

- 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

List of certification authority (CA).

The requested action has successfully completed!

Add



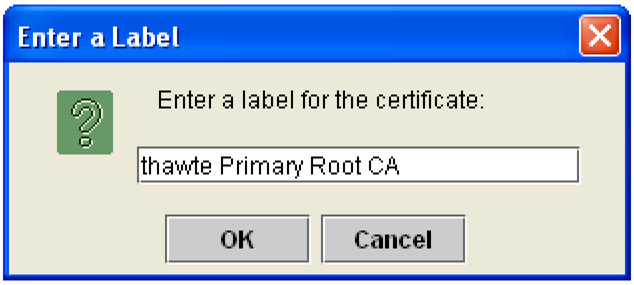
Data type: Binary DER data

Certificate file name: thawterootca.cer

Location: C:\Install\Blog\

OK

Use the label that you wrote down earlier

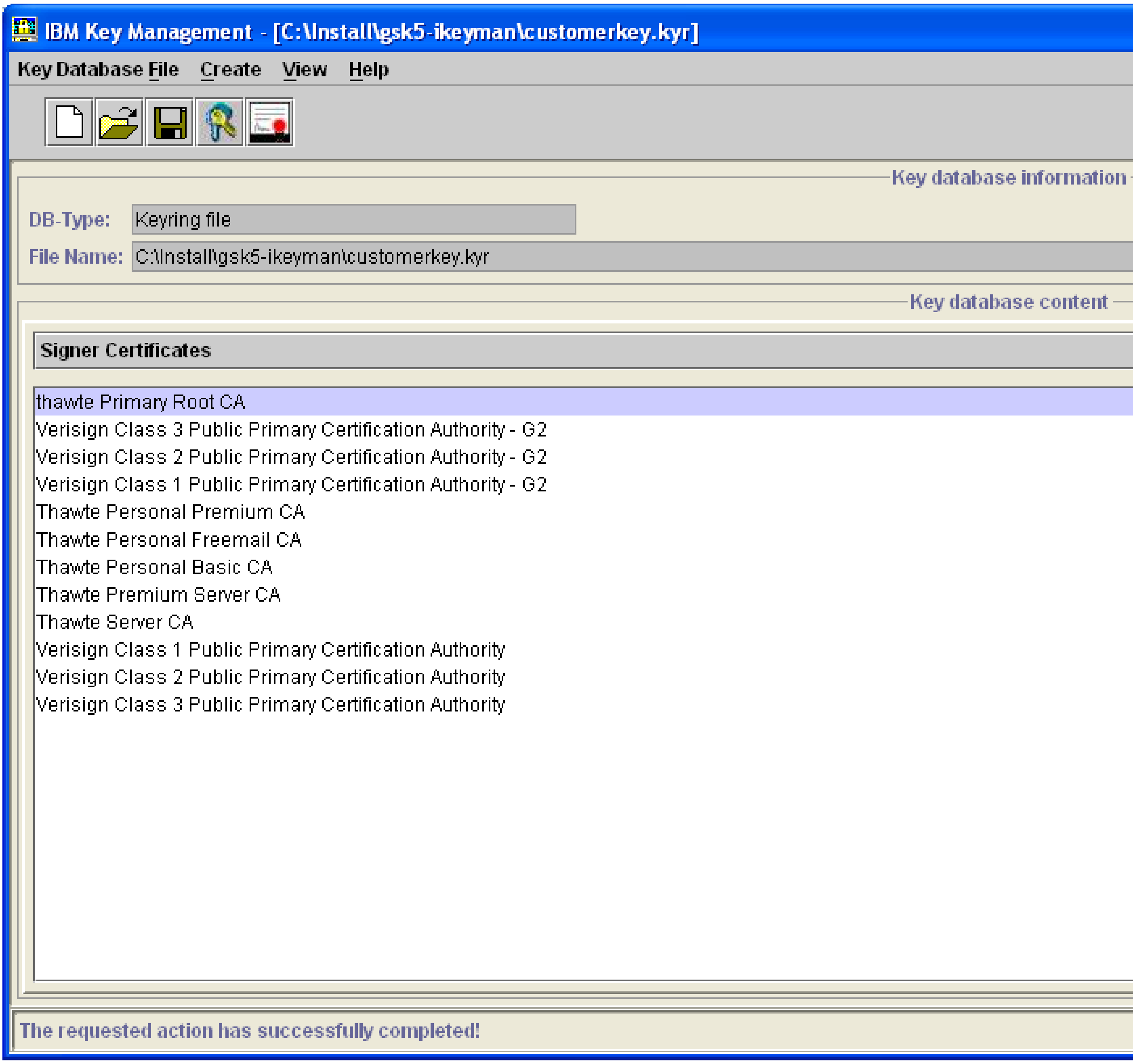


Enter a Label

Enter a label for the certificate:

thawte Primary Root CA

OK



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

Key database information

DB-Type: Keyring file

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

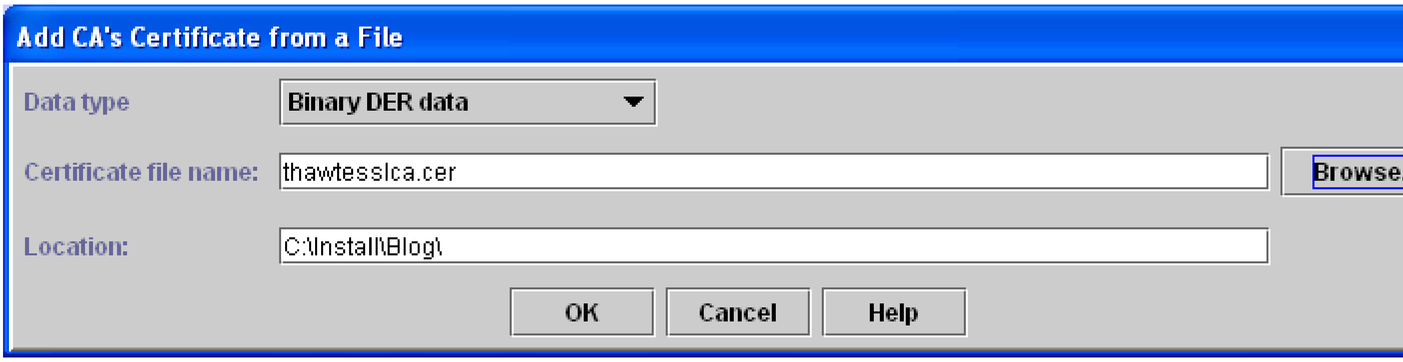
Key database content

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

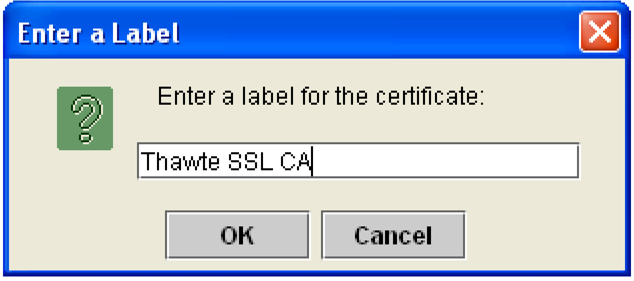
Data type: Binary DER data

Certificate file name: thawtesslca.cer

Location: C:\Install\Blog\

OK

Use the label that you wrote down earlier

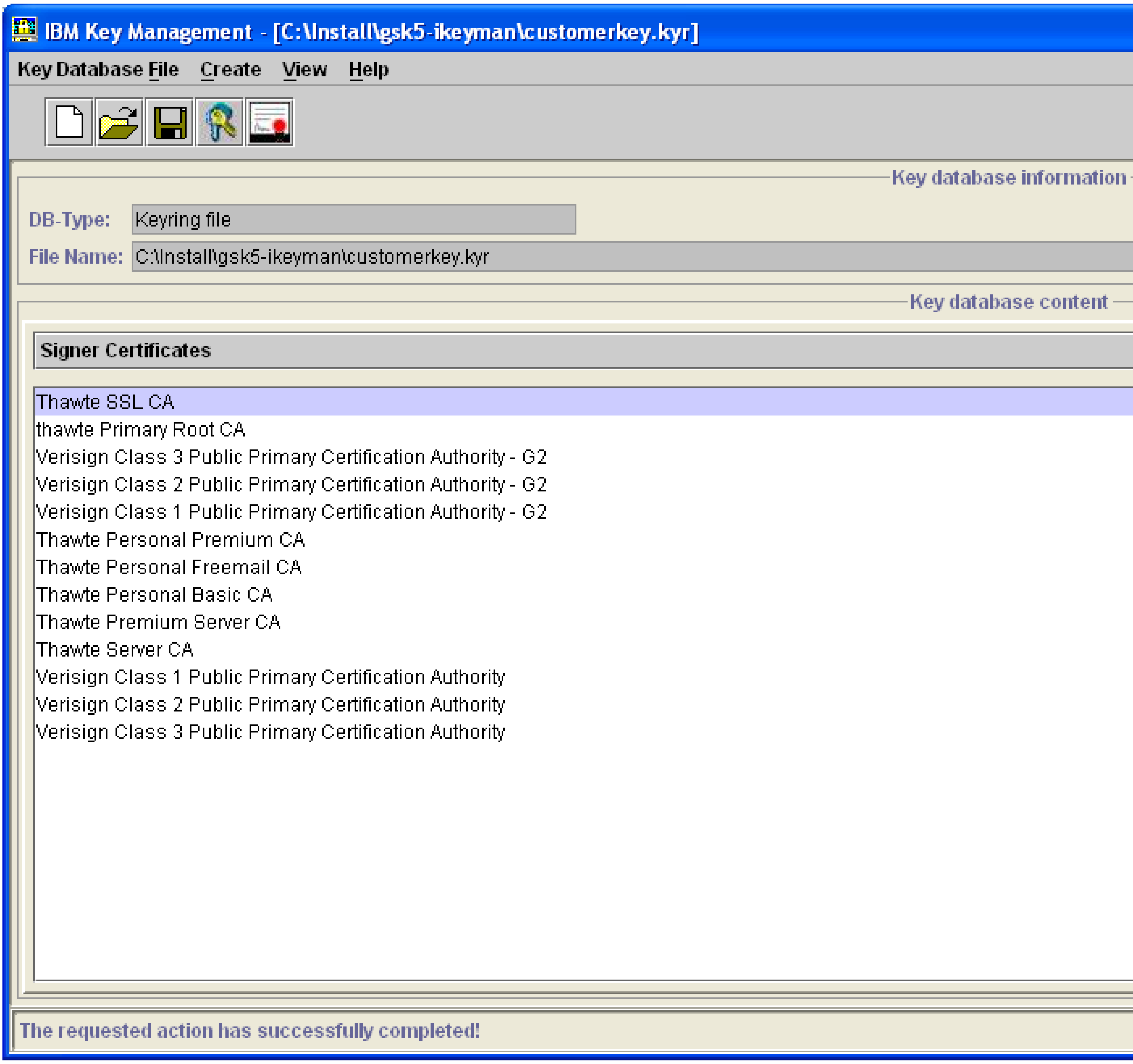


Enter a Label

Enter a label for the certificate:

Thawte SSL CA

OK



DB-Type: Keyring file

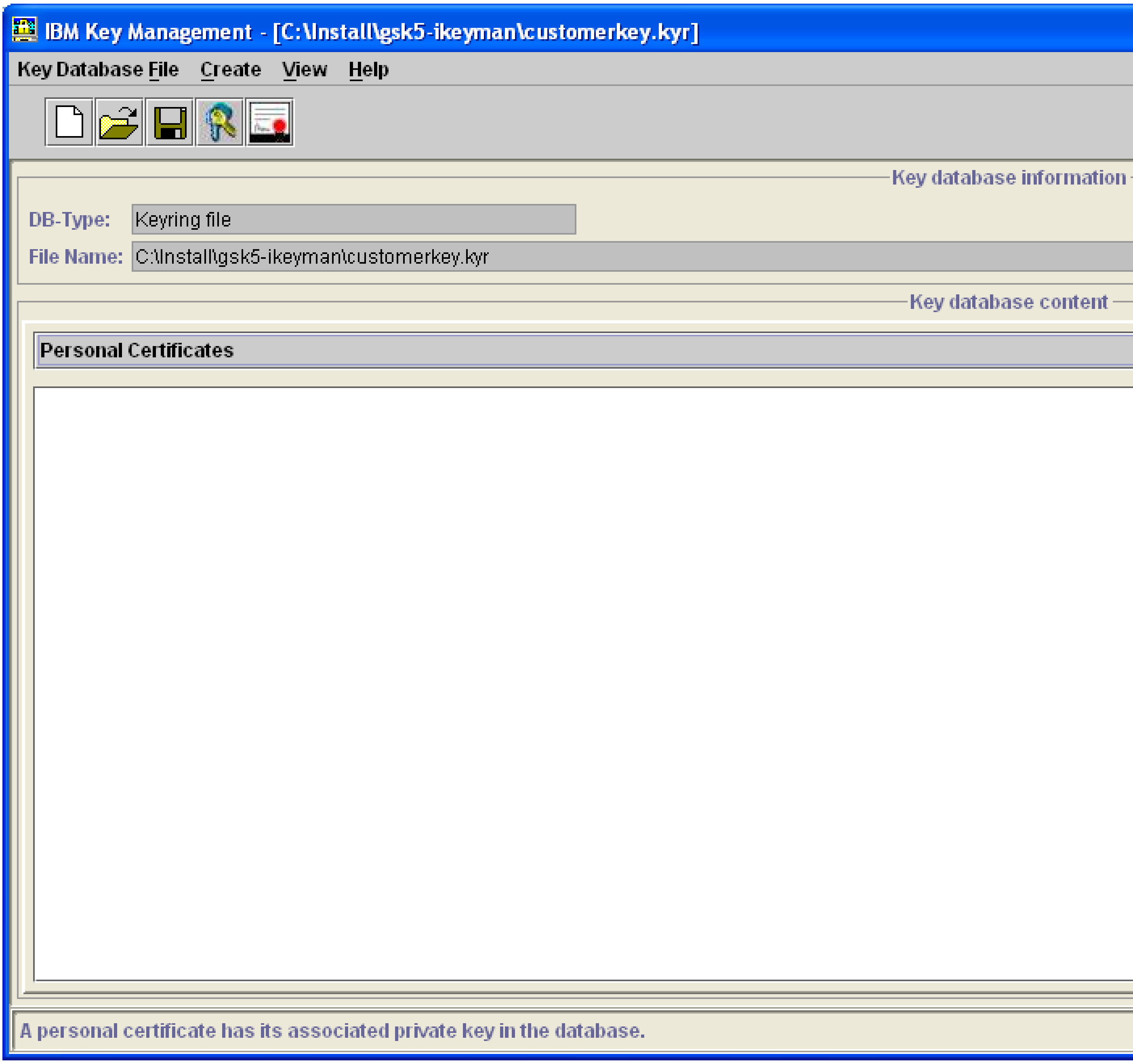
File Name: C:\Install\gsk5-ikeyman\customerkey.kyr

Signer Certificates

Thawte SSL CA
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!

Switch to... Personal Certificates



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

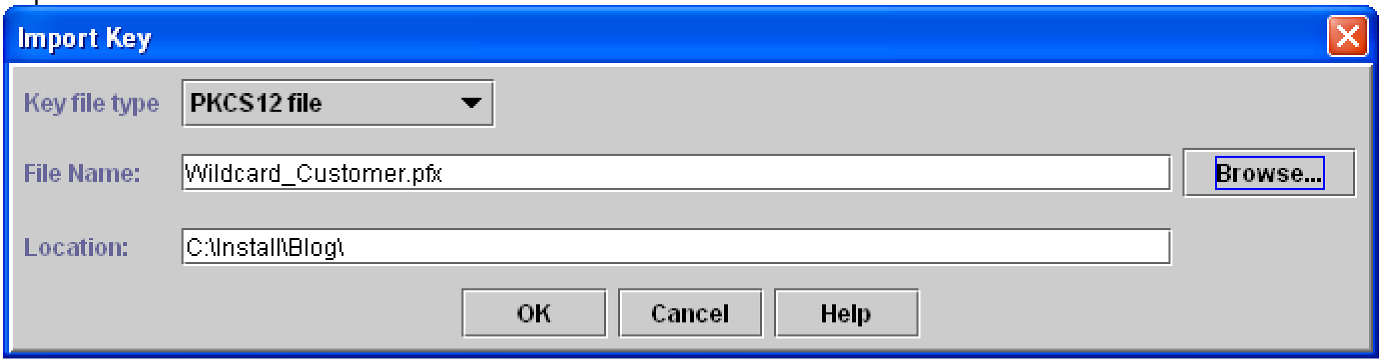
DB-Type: Keyring file

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

Personal Certificates

A personal certificate has its associated private key in the database.

Import



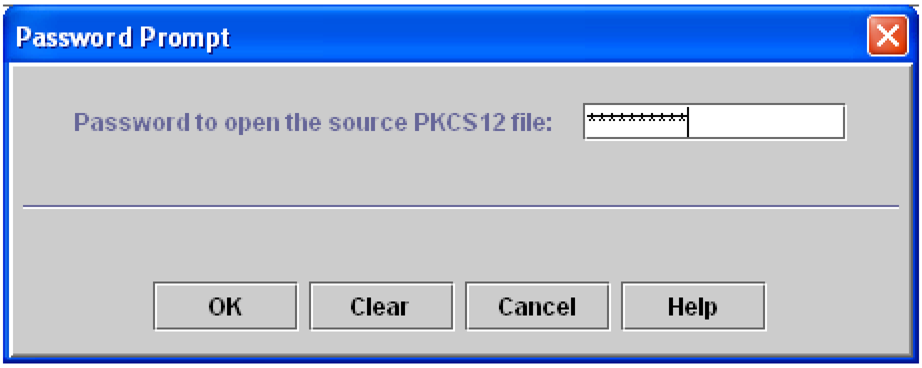
Import Key

Key file type: PKCS12 file

File Name: Wildcard_Customer.pfx

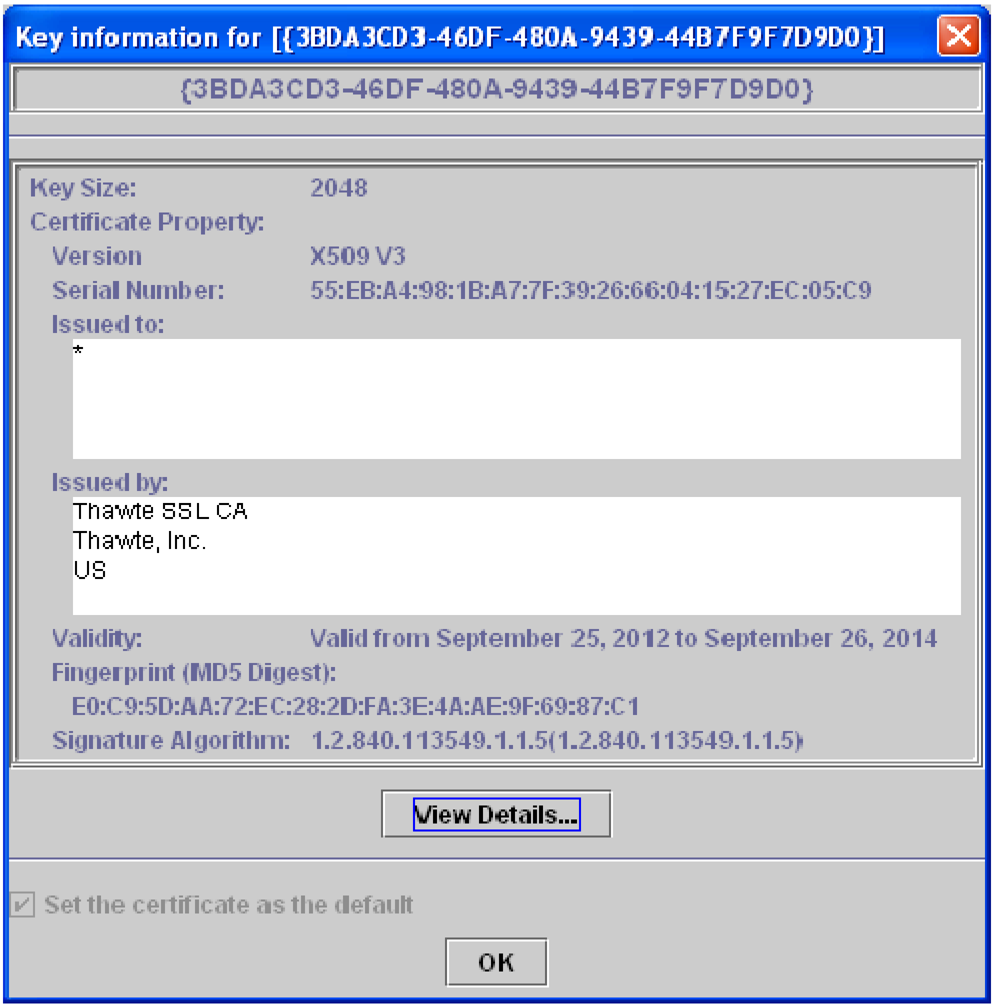
Location: C:\Install\Blog\

OK



Password to open the source PKCS12 file: ***********

OK
View/Edit



Key information for [{3BDA3CD3-46DF-480A-9439-44B7F9F7D9D0}]
{3BDA3CD3-46DF-480A-9439-44B7F9F7D9D0}
View Details...
OK

Key Size: 2048
Certificate Property:
Version X509 V3
Serial Number: 55:EB:A4:98:1B:A7:7F:39:26:66:04:15:27:EC:05:C9
Issued to:
*
Issued by:
Thawte SSL CA
Thawte, Inc.
US
Validity: Valid from September 25, 2012 to September 26, 2014
Fingerprint (MD5 Digest):
E0:C9:5D:AA:72:EC:28:2D:FA:3E:4A:AE:9F:69:87:C1
Signature Algorithm: 1.2.840.113549.1.1.5(1.2.840.113549.1.1.5)

☑ Set the certificate as the default

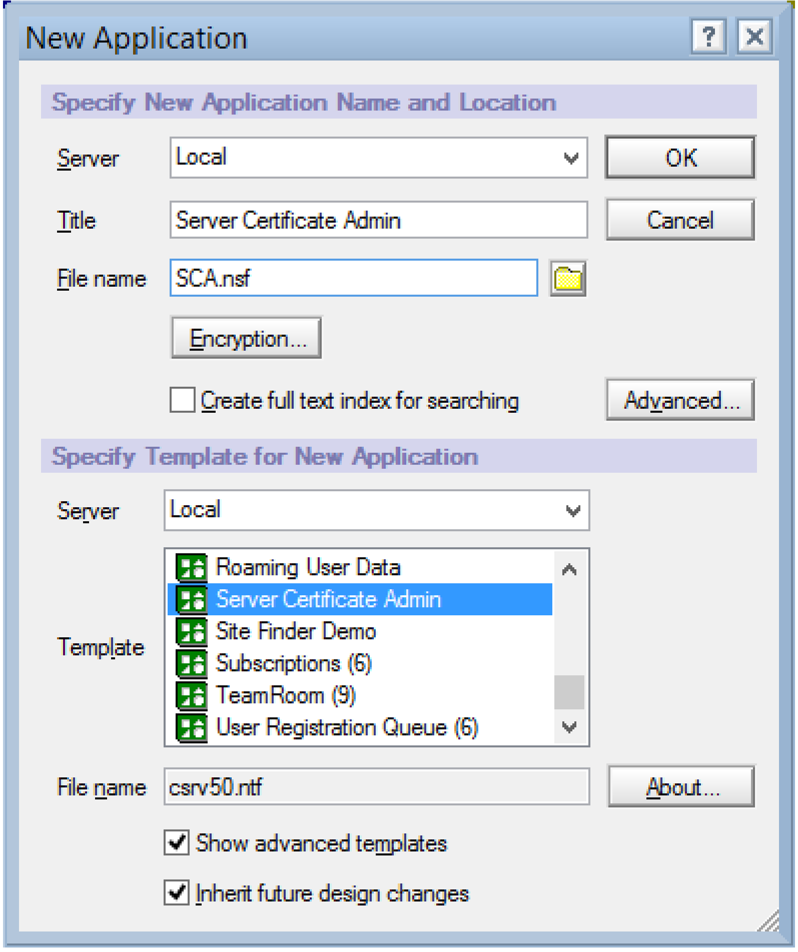
OK
Key Database File
Exit

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



New Application

Specify New Application Name and Location

Server: Local

Title: Server Certificate Admin

File name: SCA.nsf

□ Create full text index for searching

Specify Template for New Application

Server: Local

Template:
- Roaming User Data
- Server Certificate Admin
- Site Finder Demo
- Subscriptions (6)
- TeamRoom (9)
- User Registration Queue (6)

File name: csrv50.ntf

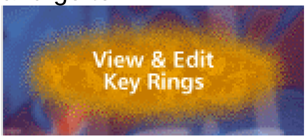
☑ Show advanced templates

☑ Inherit future design changes

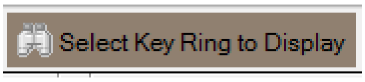
OK

Open the newly created database

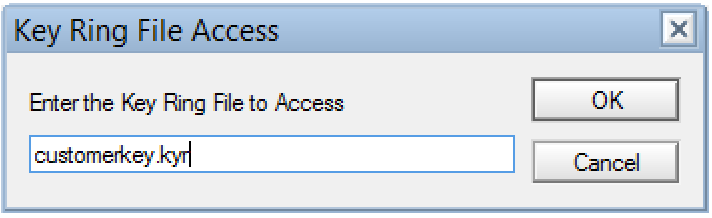
and go to:



Choose



and

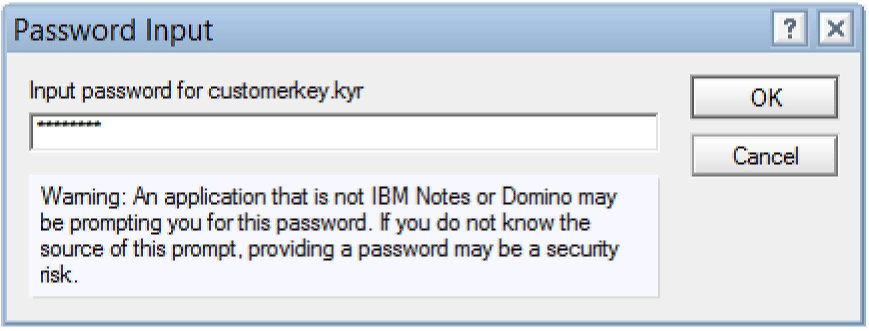


Key Ring File Access

Enter the Key Ring File to Access

customerkey.kyr

OK



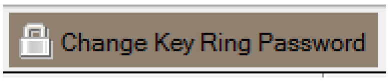
Input password for customerkey.kyr

****

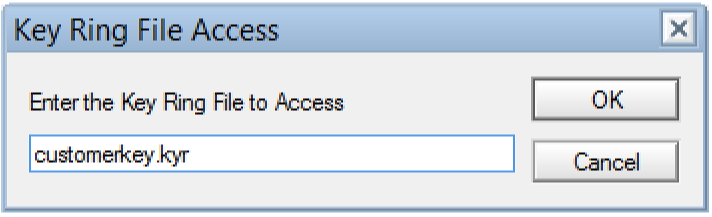
Warning: An application that is not IBM Notes or Domino may be prompting you for this password. If you do not know the source of this prompt, providing a password may be a security risk.

OK

Choose



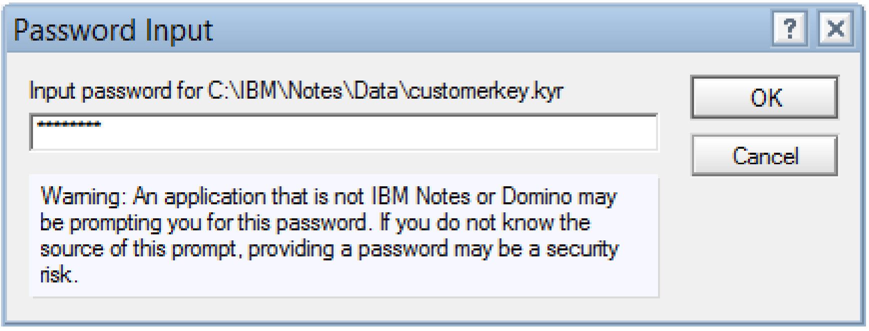
and



Enter the Key Ring File to Access

customerkey.kyr

OK

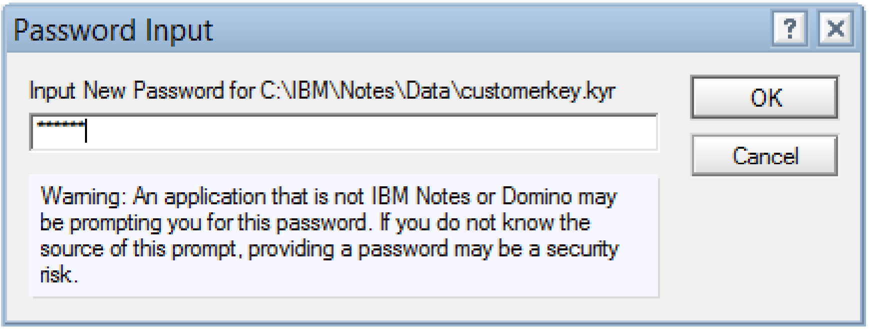


Input password for C:\IBM\Notes\Data\customerkey.kyr

****

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

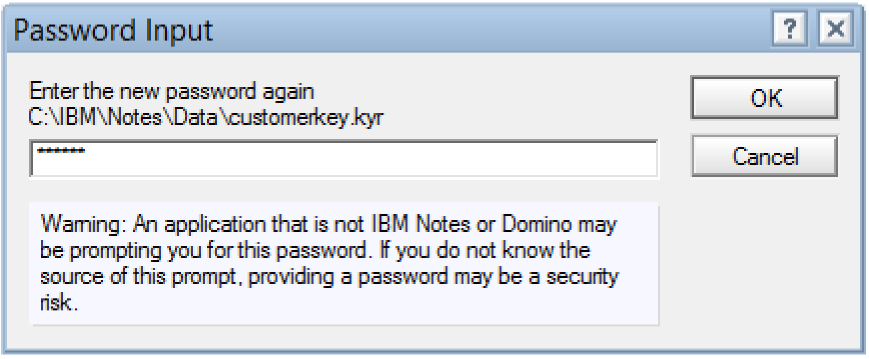


Input New Password for C:\IBM\Notes\Data\customerkey.kyr

****

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

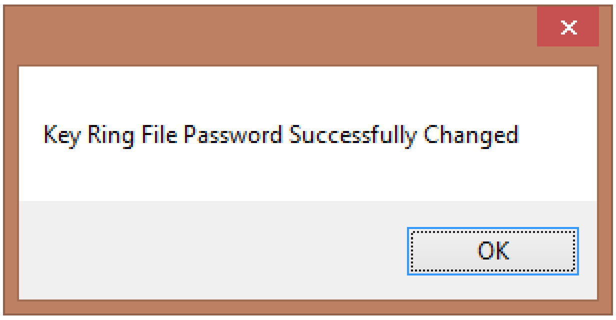


Enter the new password again
C:\IBM\Notes\Data\customerkey.kyr

****

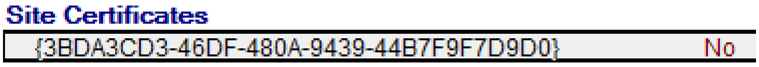
Warning: An application that is not IBM Notes or Domino may be prompting you for this password. If you do not know the source of this prompt, providing a password may be a security risk.

OK



Key Ring File Password Successfully Changed

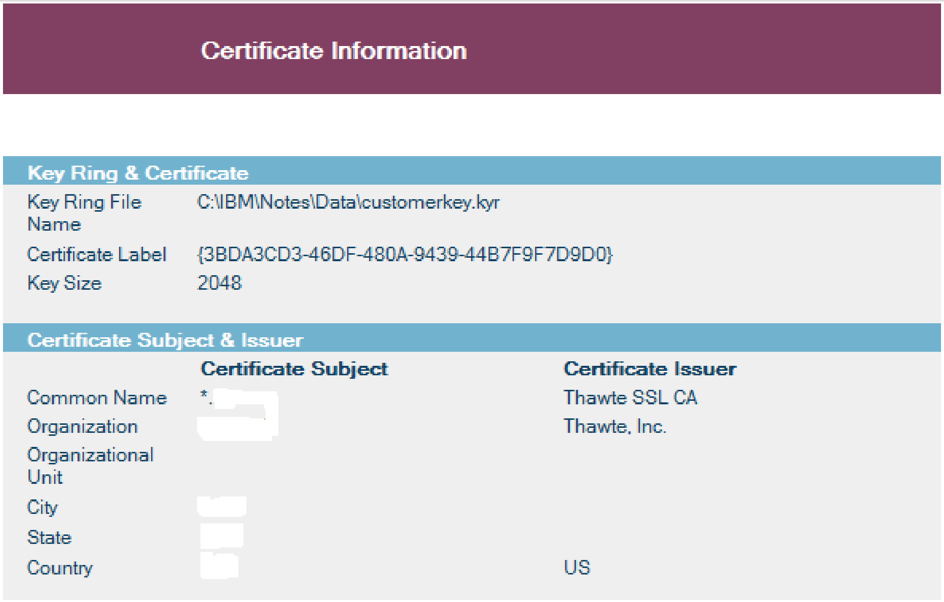
You should now also have a customerkey.sth file in your data directory, please check that you have!
If you don't you have not followed the instructions.
Click on:



Site Certificates

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

should show something like this:



Certificate Information

Key Ring & Certificate

Key Ring File Name	C:\IBM\Notes\Data\customerkey.kyr
Certificate Label	{3BDA3CD3-46DF-480A-9439-44B7F9F7D9D0}
Key Size	2048

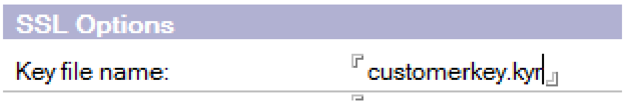
Certificate Subject & Issuer

	Certificate Subject	Certificate Issuer
Common Name	*.[redacted]	Thawte SSL CA
Organization	[redacted]	Thawte, Inc.
Organizational Unit		
City	[redacted]	
State	[redacted]	
Country	[redacted]	US

Implement the files on the server

Copy both kyr and sth files to the Servers Data Directory

Now in your Internet sites configuration

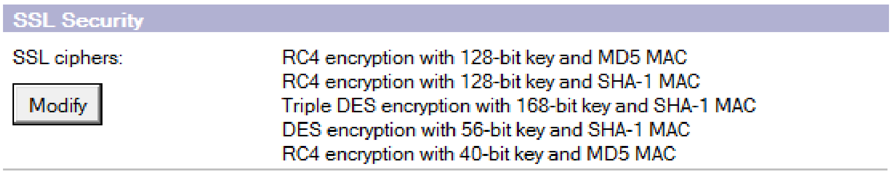


SSL Options

Key file name: customerkey.kyr

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

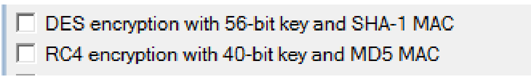
Also modify:



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

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.

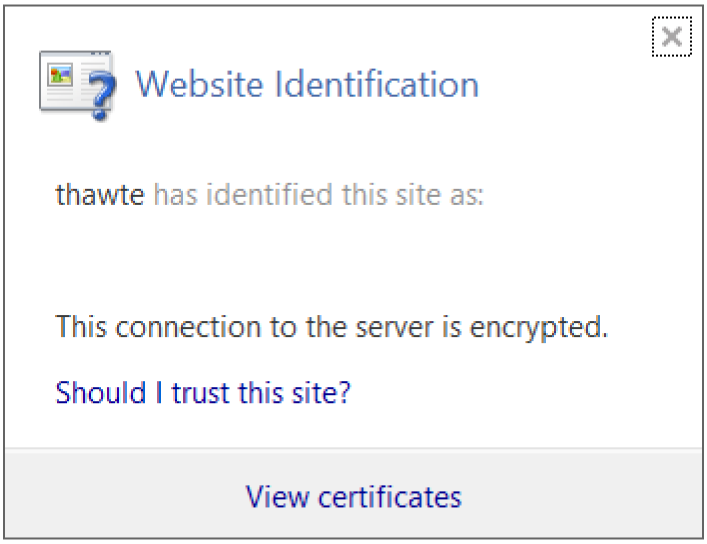
Also, in the server document, make sure that you have enabled SSL in the Internet Ports.... section.

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 certicates are in use for the url.

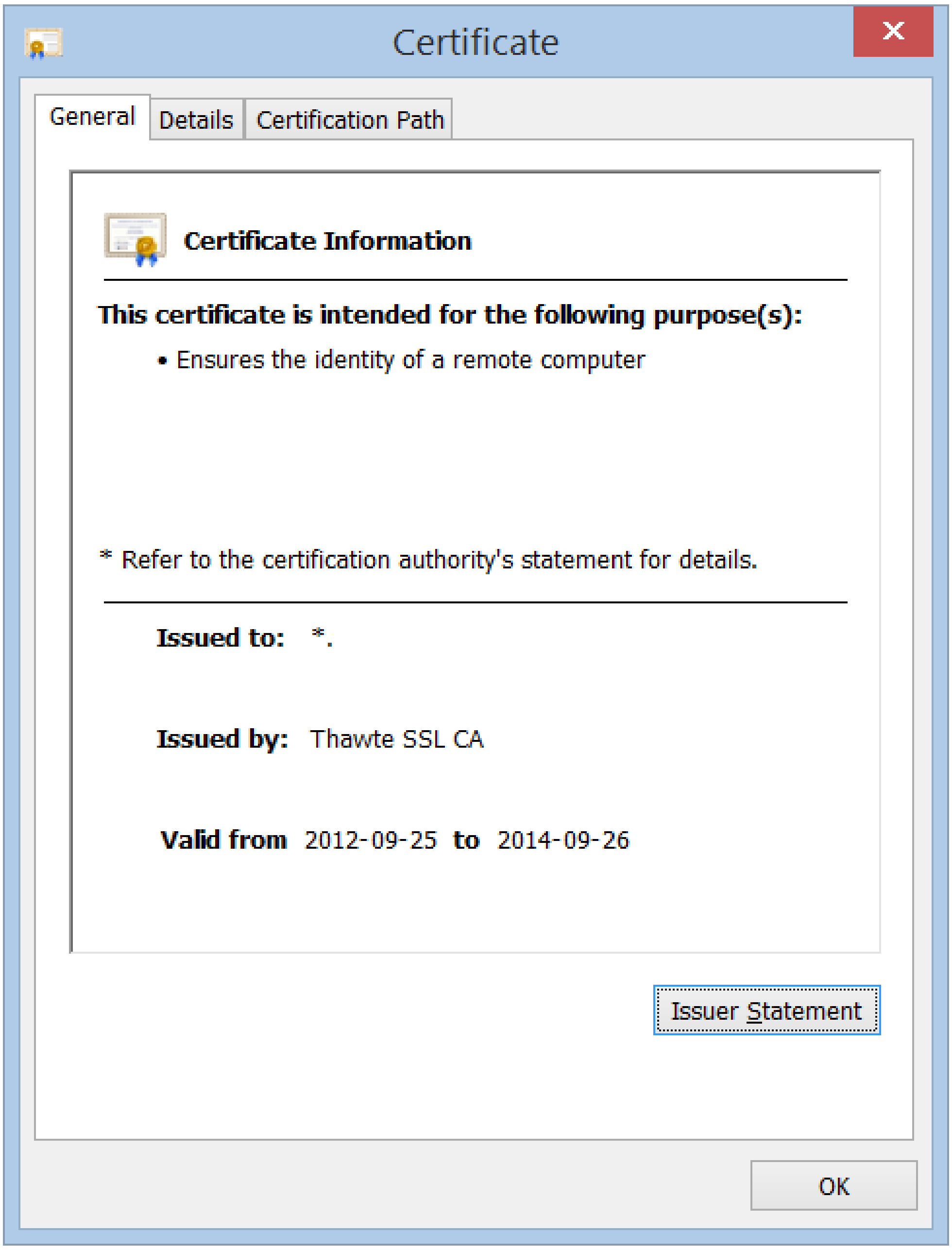


Website Identification

thawte has identified this site as:

This connection to the server is encrypted.

View certificates



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.

Issued by: Thawte SSL CA

Valid from 2012-09-25 to 2014-09-26

If you are here now congratulations

Conclusion