SSL Certificate – IBM

Installation Guide

webnic
accelerate your business

Please select your version

Installation Instructions for IBM AS 400 / iSeries server

Installation Instructions for IBM HTTP Server running IKEYMAN GUI

Installation Instructions for IBM WebSphere using IKEYMAN GUI (Version 7)

Installation Instructions for IBM Websphere using the command line

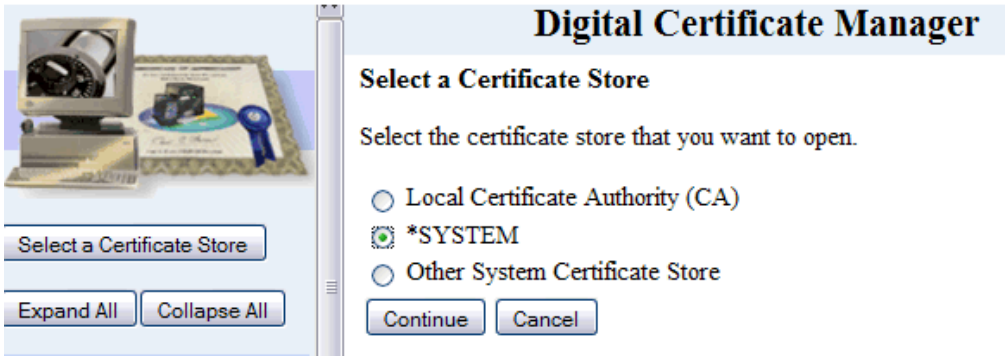
Installation Instructions for IBM AS 400 / iSeries server

Step 1: Download the Symantec Intermediate CA Certificate

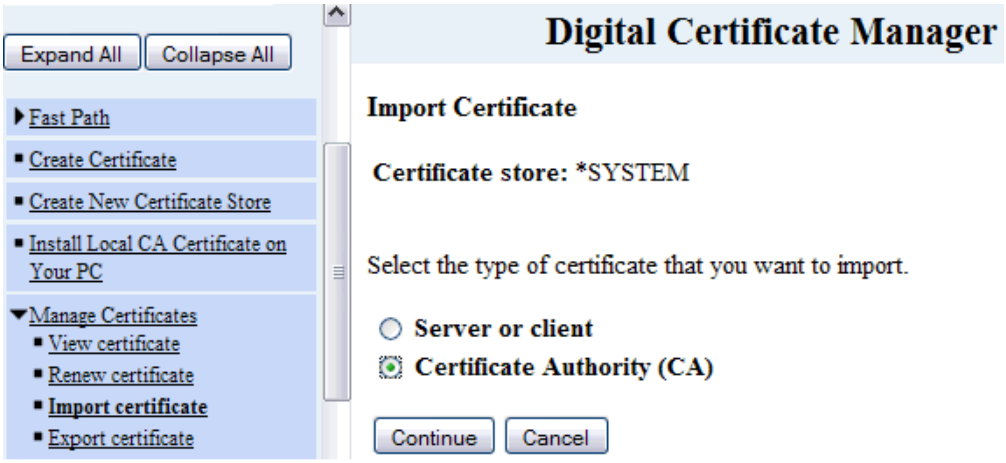
1. Download the Intermediate CA certificate from here
2. Select the appropriate Intermediate CA certificate for your SSL Certificate type.
3. Copy the Intermediate CA certificate and paste it on a Notepad.
4. Save the file as **intermediate.txt**

Step 2: Install the Symantec Intermediate CA Certificate

1. Start Digital Certificate Manager (DCM).
2. From navigation panel, click **Select a Certificate Store** > select ***SYSTEM**

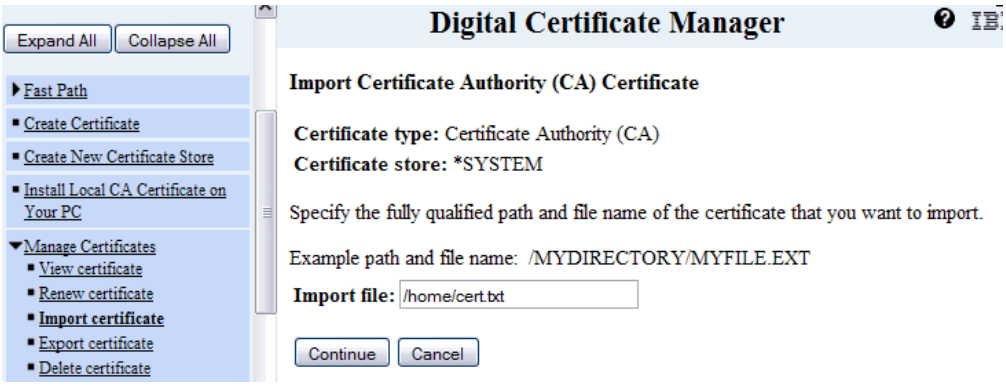


3. Enter in password for Certificate Store > click **Continue**
4. From navigation panel, select **Manage Certificates**
5. From the list, select **Import Certificate** > **Certificate Authority (CA)** > click **Continue**



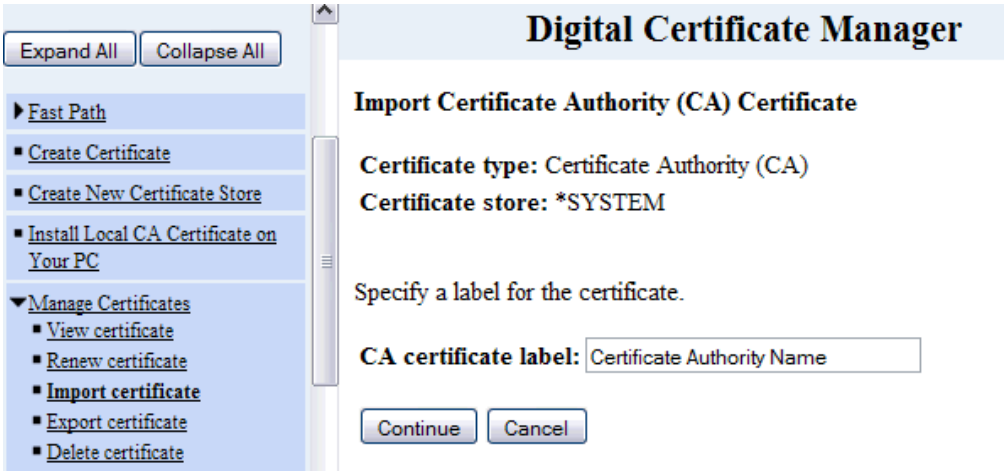
6. On the next screen, specify the path and file name of intermediate ca certificate. This is the location and name of the intermediate ca file on the IFS of the iSeries.

   Example: The file is stored in the /home directory and the intermediate ca file was called 'cert.txt' you would put in a path and file name of /home/cert.txt.

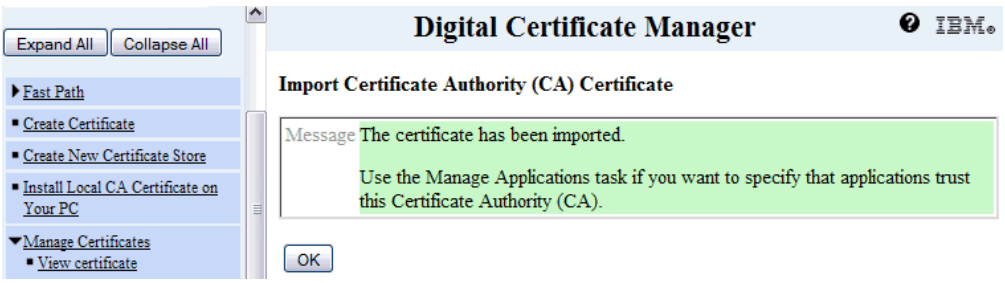


7. Click **Continue**
8. Create a CA certificate label. This can be any name desired as long as it is unique (should not match any labels for any other certificates).

   Example: CA certificate label: Certificate Authority Name



9. Click **Continue**
10. A message stating the intermediate ca certificate has been imported. Click **OK**



Step 3: Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad
   The text file should look like:
   -----BEGIN CERTIFICATE-----

   [encoded data]

   -----END CERTIFICATE-----

3. Save the file with extansion **.txt**

Step 4: Install the SSL Certificate

1. Start Digital Certificate Manager (DCM).
2. From navigation panel, click **Select a Certificate Store** > select ***SYSTEM**
3. Enter in password for Certificate Store > click **Continue**
4. From navigation panel, select **Manage Certificates**
5. From the list, select **Import Certificate** > select **Server or Client**
6. Select the certificate file and complete wizard
7. Verify certificate installation using the Symantec Installation Checker.

Installation Instructions for IBM HTTP Server running IKEYMAN GUI

Step 1: Download the Symantec Intermediate CA Certificate

1. Download the Intermediate CA certificate.
2. Select the appropriate Intermediate CA certificate for your SSL Certificate type.
3. Copy the Intermediate CA certificate and paste it on a Notepad.
4. Save the file as **intermediate.cer**

Step 2: Install Symantec Intermediate CA Certificate

1. Start the key management utility (iKeyman):

   On Windows: Go to the start UI and select **Start Key Management Utility**

   On AIX, Linux or Solaris: Type **ikeyman** on the command line

2. Open the key database file that was used to create the certificate request.
3. Enter the password, then click **OK.**
4. Click on the "down arrow" to the right, to display a list of three choices.
5. Select **Signer Certificates**, then click **Add**.
6. Click **Data Type** and select a data type, such as Base64-encoded ASCII data.
   NOTE: This data type must match the data type of the importing certificate.
7. Enter a file name and location for **intermediate.cer** digital certificate or click **Browse** to select a file name and location.
8. Click **OK.**
9. Enter a label for importing certificate, for example: **Intermediate CA**
10. Click **OK**.
11. The Signer Certificates field displays the label of the signer certificate you added.

Step 3: Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad
   The text file should look like:

-----BEGIN CERTIFICATE-----

[encoded data]

-----END CERTIFICATE-----

3. Save the file with extension **.cer**

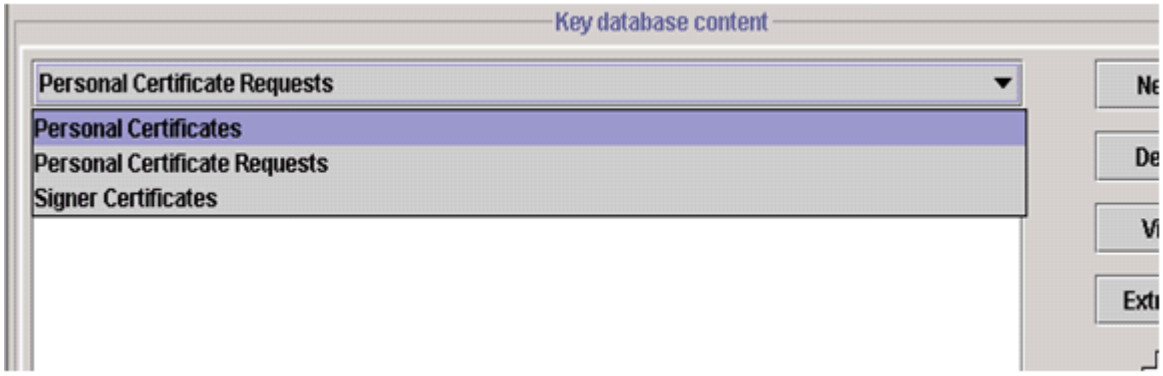
Step 4: Install the SSL Certificate

1. Open the .kdb file using the iKeyman utility:

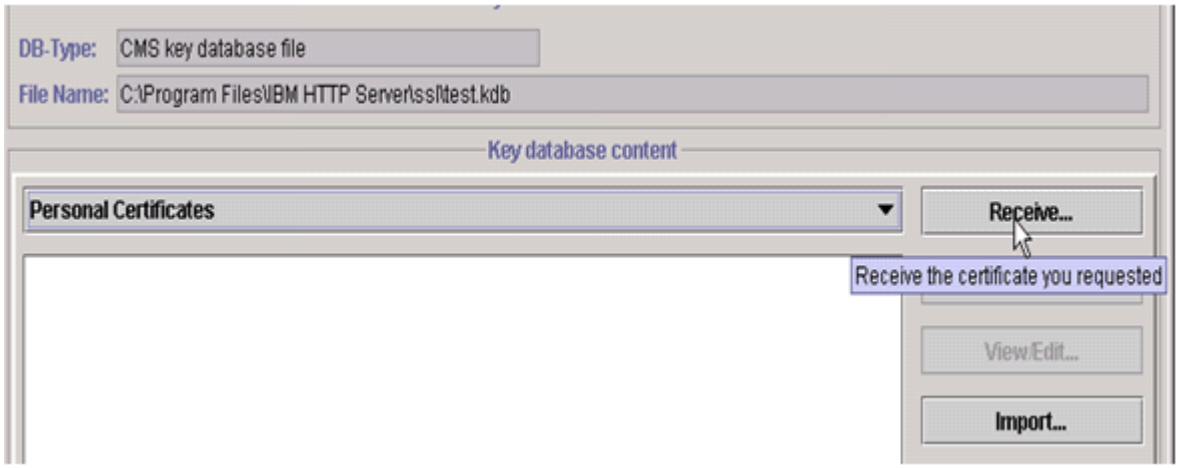
   On Windows: Go to the start UI and select **Start Key Management Utility**

   On AIX, Linux or Solaris: Type **ikeyman** on the command line

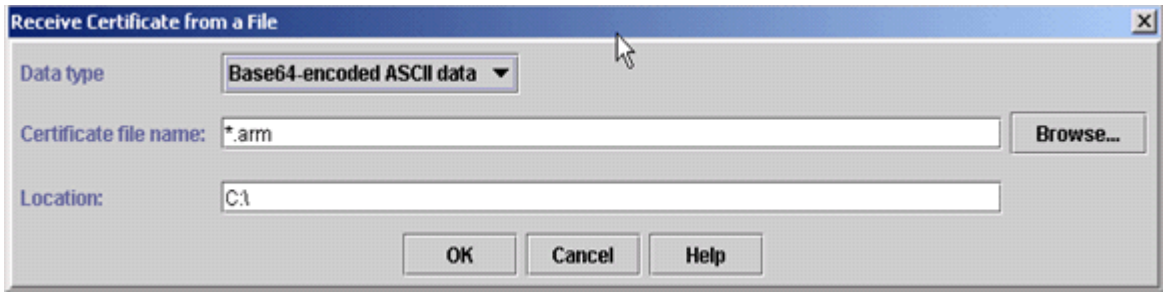
2. In the middle of the iKeyman GUI you will see a section called **Key database content**
3. Click on the "down arrow" to the right, to display a list of three choices
4. Select **Personal Certificates**



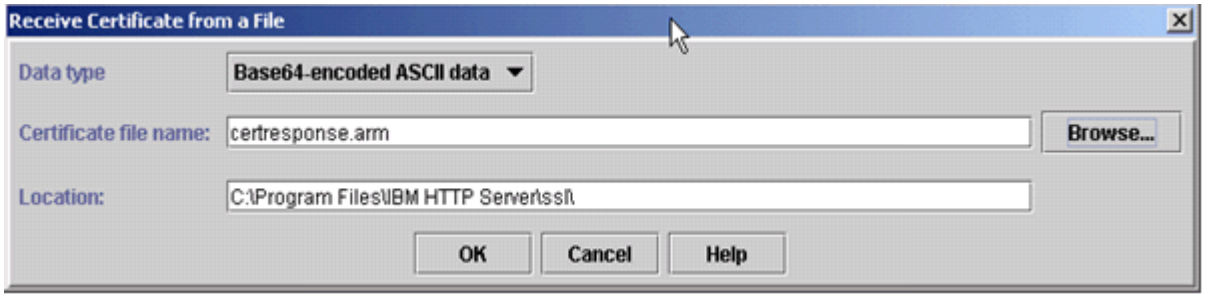
5. From the **Personal Certificates** section, click **Receive**



6. Data Type - leave the default of "Base64-encoded ASCII data"



7. Browse to the directory that contains the .cert or .arm file
8. Highlight the file and click **Open**.
9. Now click **OK** on this dialog box



Step 5. Transfer Certificate

1. To extract an SSL certificate from a key database file and store it in a CA key ring file, start the iKeyman graphical user interface

2. Run following command:

   On Windows: strmqikm

   On UNIX: gsk7ikm

3. Choose **Open** from the **Key Database File** menu. Click **Key database type**, and select **CMS**.
4. Click **Browse** to navigate to the directory containing the key database files
5. Select the key database file to which you want to add the certificate. For example, key.kdb.
6. Click **Open**
7. In the Password Prompt window, type the password you set when you created the key database and then click **OK**.
8. Select **Signer Certificates** in the Key database content field, and then select the certificate you want to extract.
9. Click **Extract**.
10. Select the **Data type** of the certificate. For example, **Base64-encoded ASCII**
11. Click **Browse** to select the name and location of the certificate file name.
12. Click **OK.** The certificate is written to the file you specified.
13. Verify certificate installation using the Symantec Installation Checker.

Installation Instructions for IBM WebSphere using IKEYMAN GUI (Version 7)

Step 1: Download the Symantec Intermediate CA Certificate

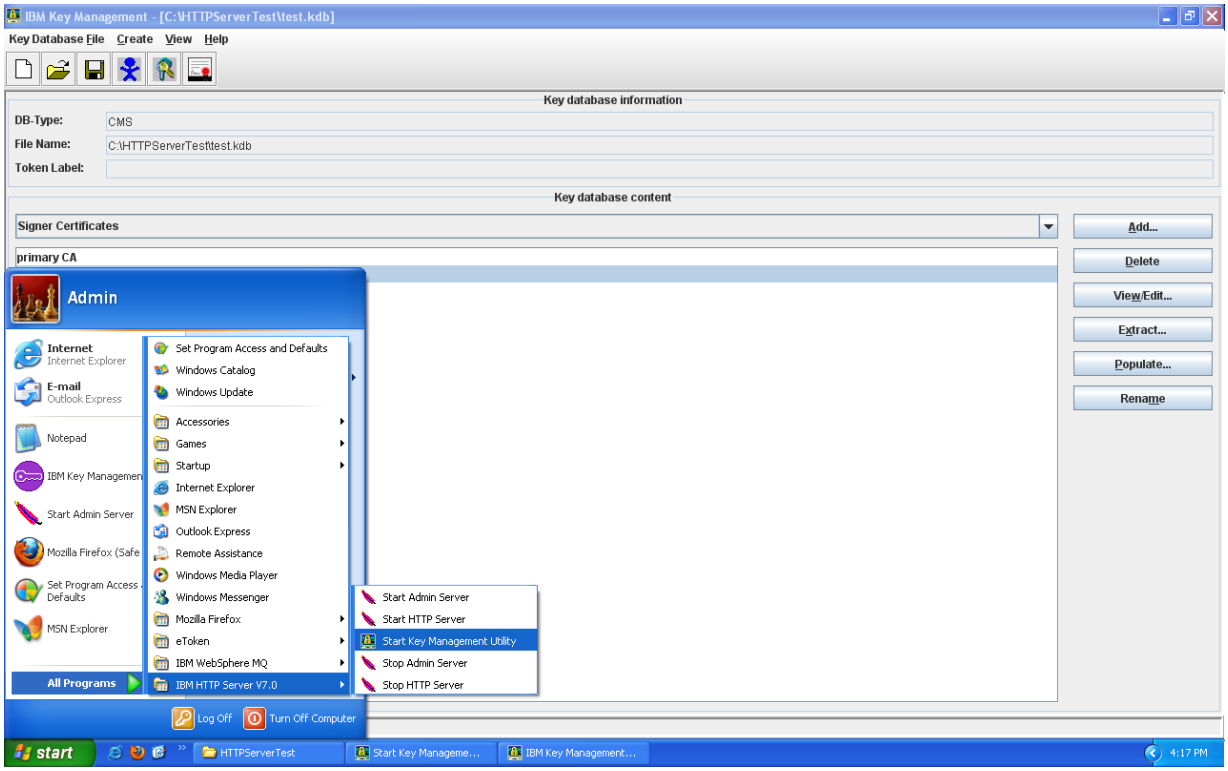
1. Download the Intermediate CA certificate.

   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
2. Copy the Intermediate CA certificate and paste it on a Notepad.
3. Save the file as **intermediate.cer**

Step 2: Install Symantec Intermediate CA Certificate

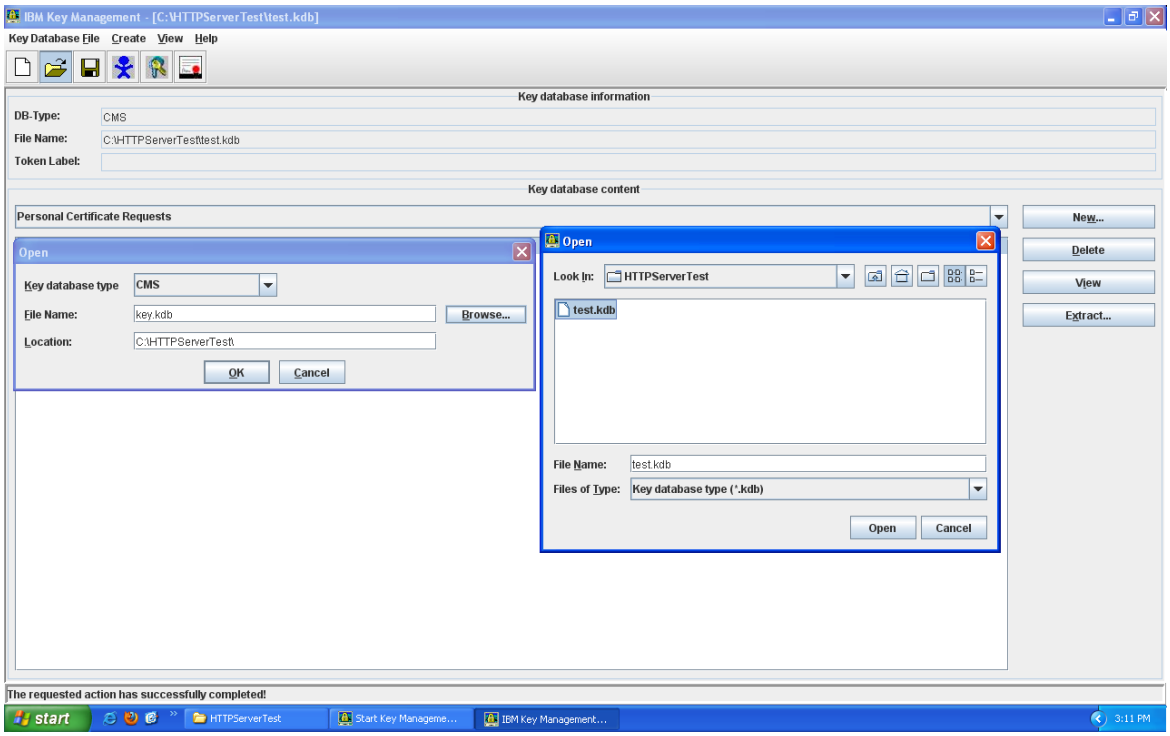
1. Start the key management utility (iKeyman):

   On Windows: Go to the start UI and select **Start Key Management Utility**

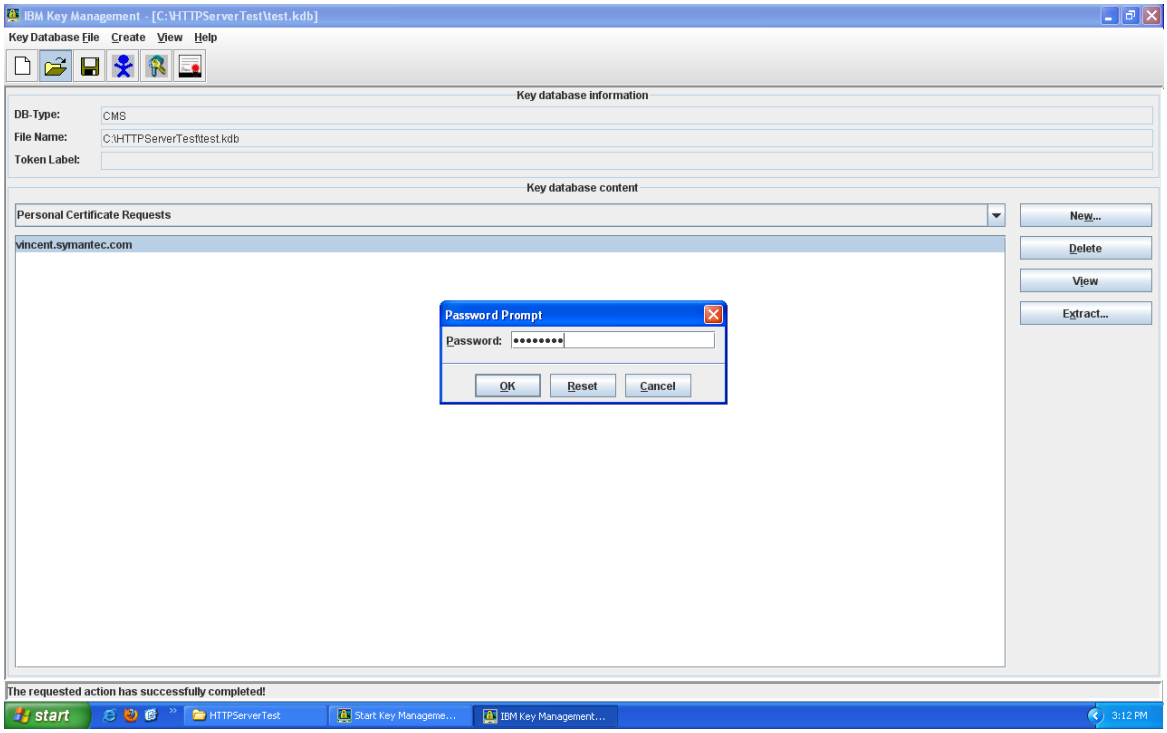


   On AIX, Linux or Solaris: Type **ikeyman** on the command line

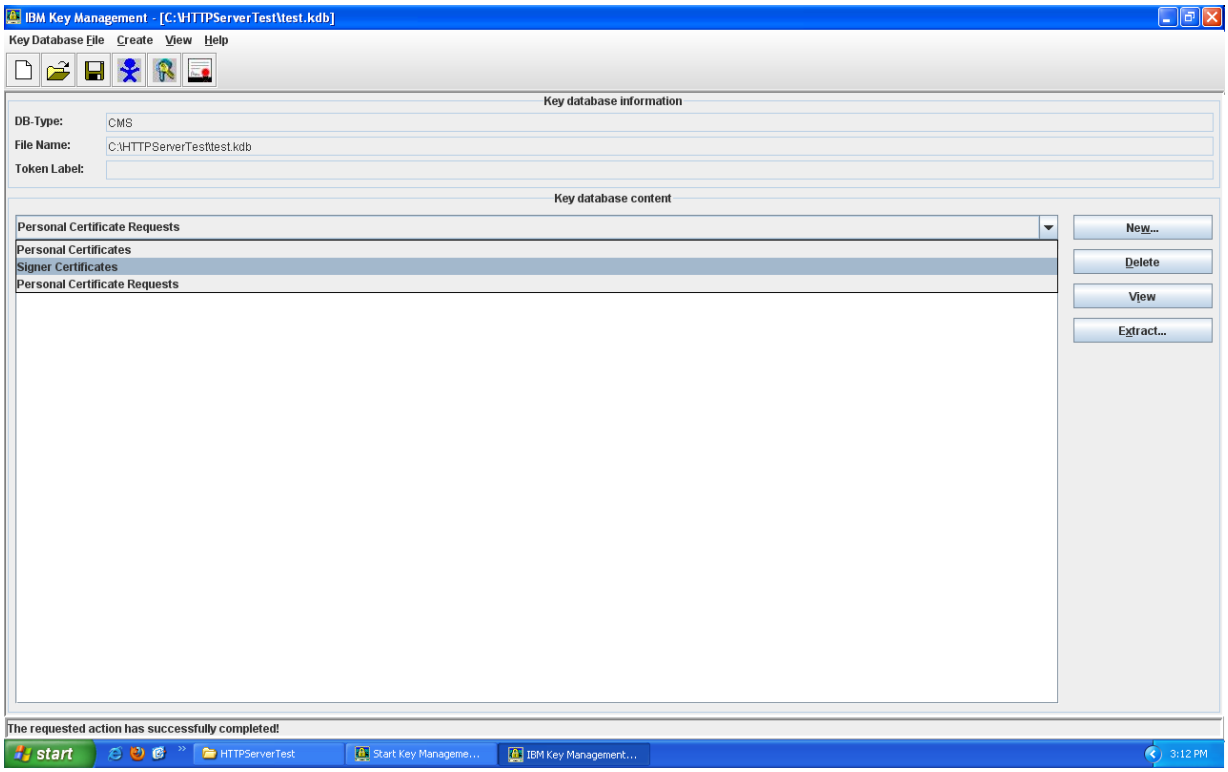
2. Open the key database file that was used to create the certificate request.



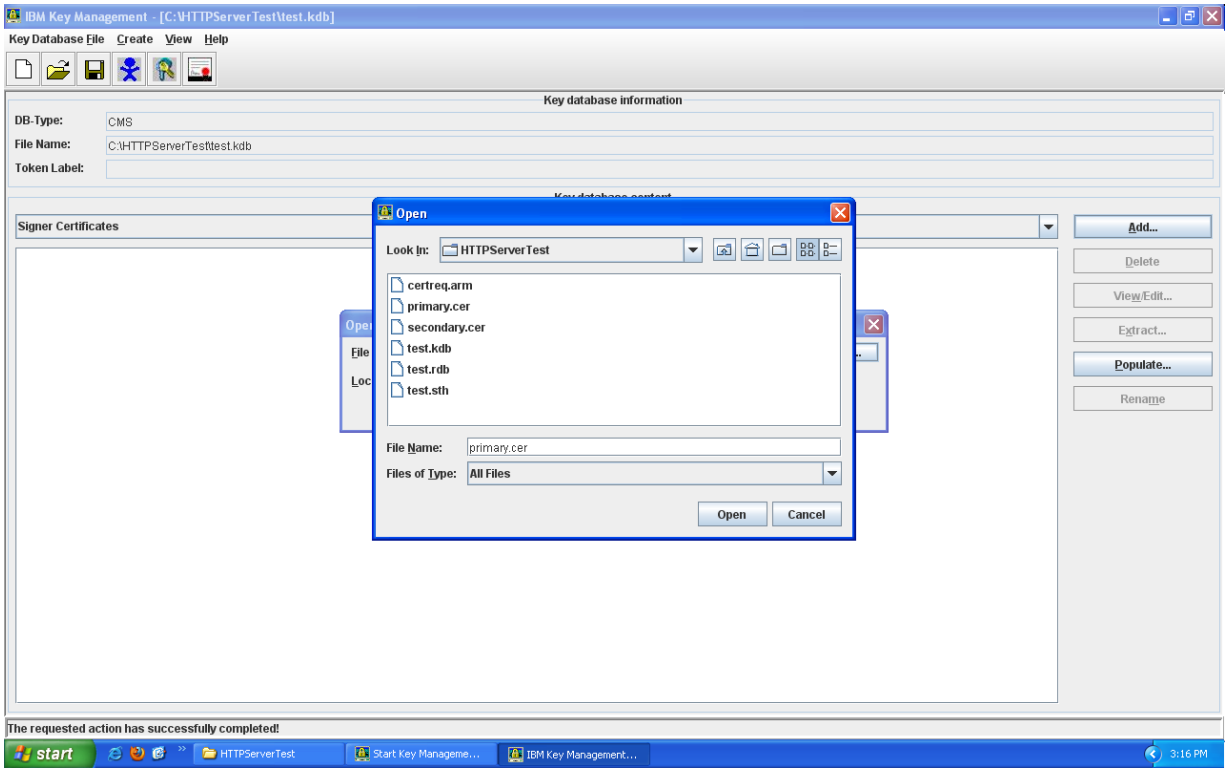
3. Enter the password, then click **OK.**



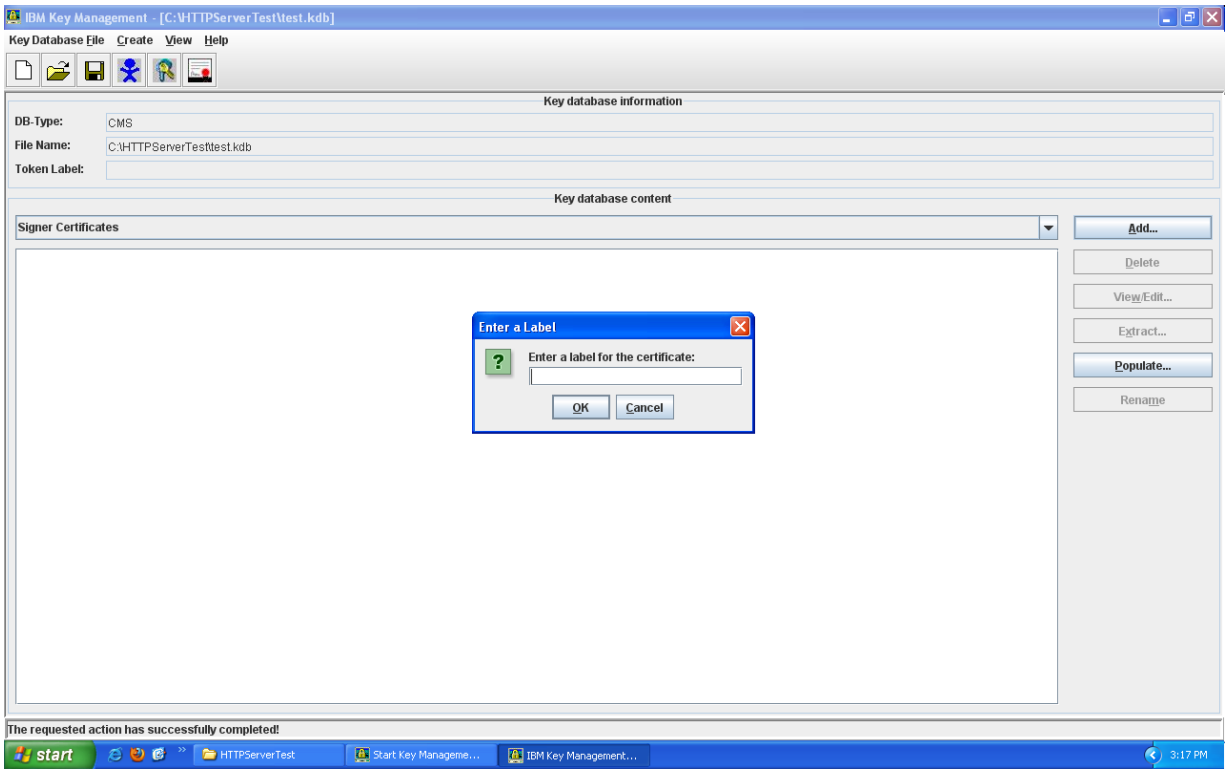
4. Select **Signer Certificates**, then click **Add**.



5. Click **Files of Type** and select **All Files**.
6. Enter a file name and location for **intermediate.cer** digital certificate or click **Browse** to select a file name and location.



7. Click **OK.**
8. Enter a label for importing certificate, for example: **Intermediate CA**



7. Click **OK**.
8. The Signer Certificates field displays the label of the signer certificate you added.

Step 3: Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad
   The text file should look like:
   -----BEGIN CERTIFICATE-----

   [encoded data]

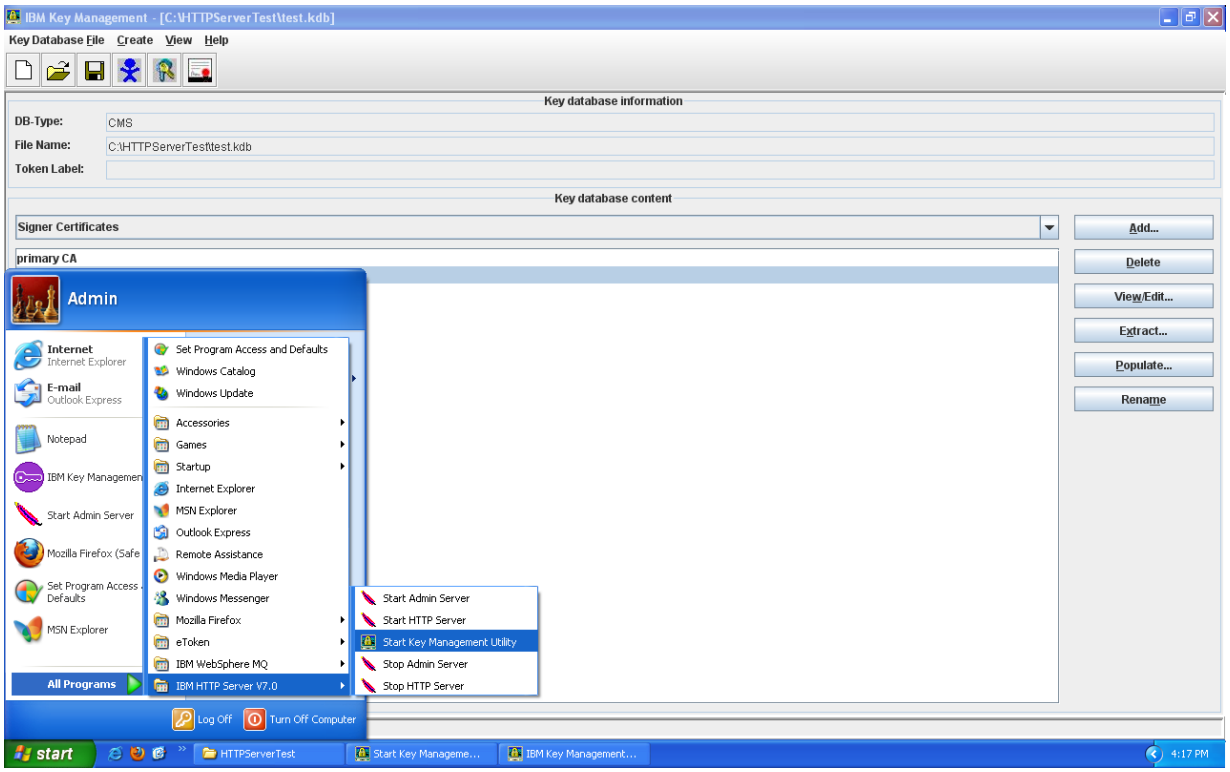
   -----END CERTIFICATE-----

3. Save the file with extension **.cer**

Step 4: Install the SSL Certificate

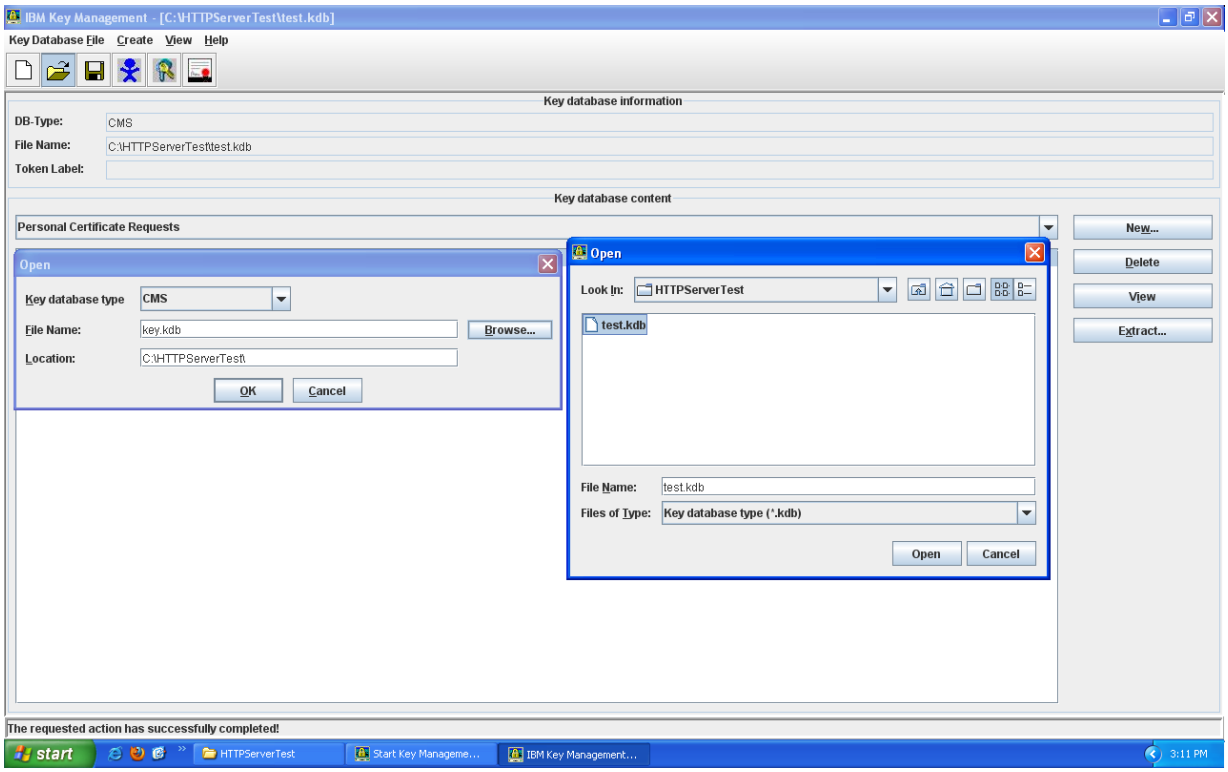
1. Start the key management utility (iKeyman):

   <u>On Windows:</u> Go to the start UI and select **Start Key Management Utility**

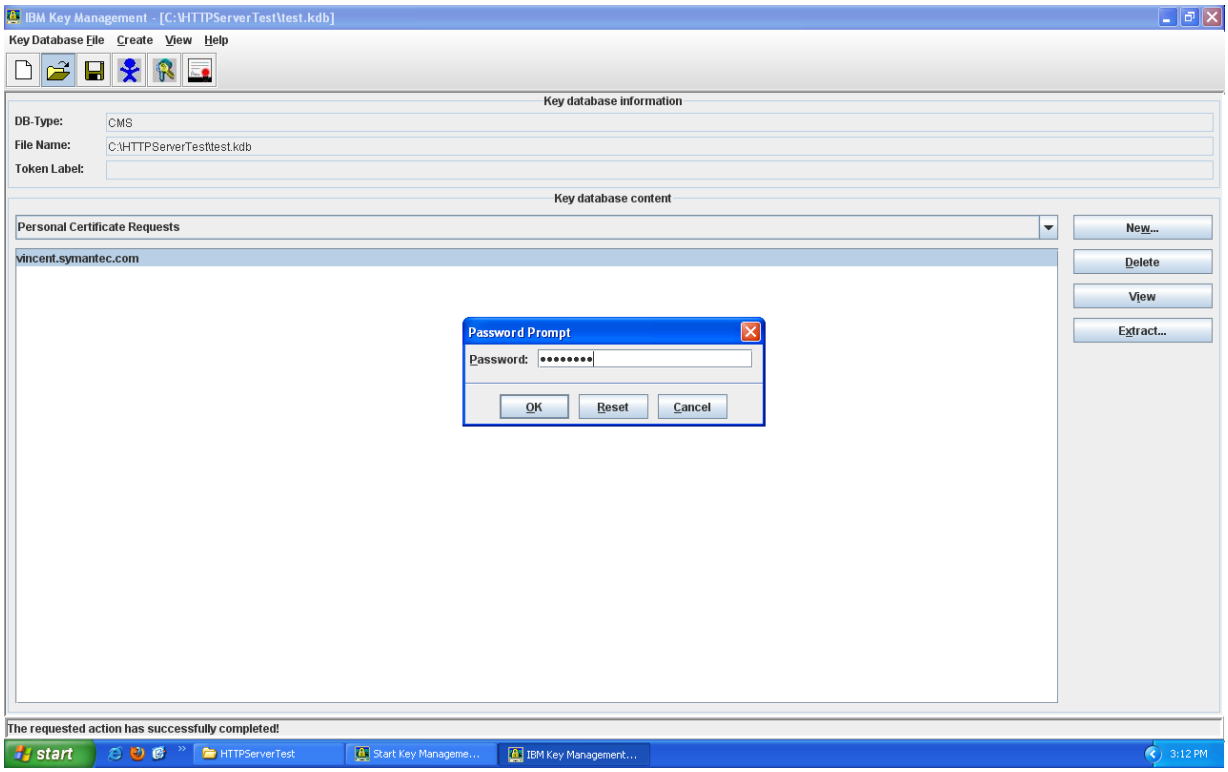


   <u>On AIX, Linux or Solaris</u>: Type **ikeyman** on the command line

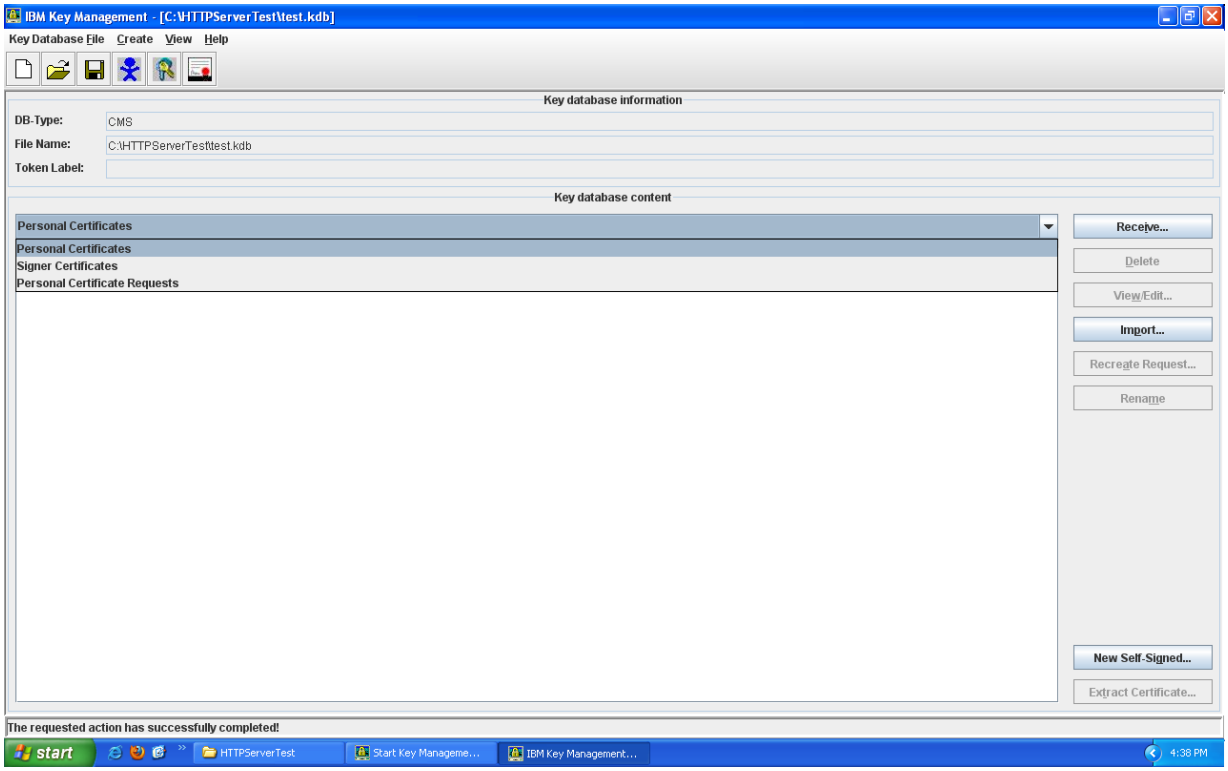
2. Choose **Open** from the **Key Database File** menu. Click **Key database type**, and select **CMS**.



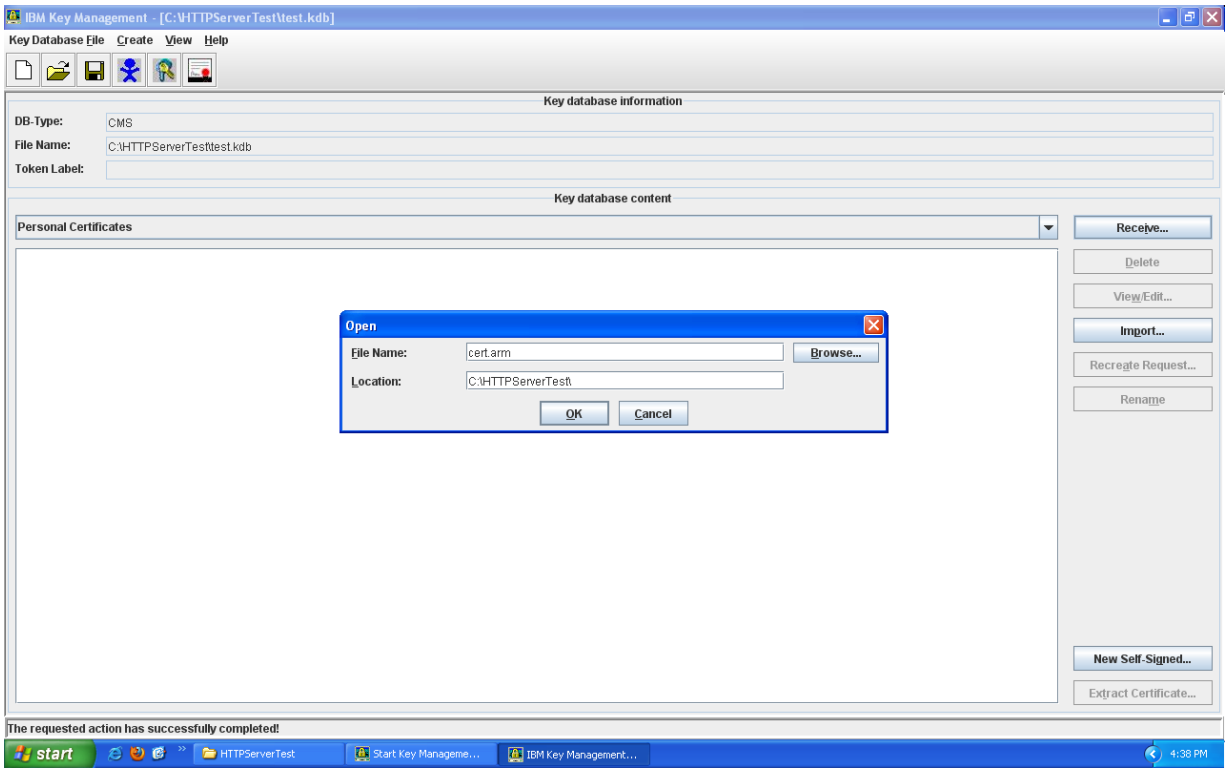
3. Click **Browse** to navigate to the directory containing the key database files.
4. Select the key database file to which you want to add the certificate. For example, key.kdb.
5. Click **Open**
6. In the Password Prompt window, type the password you set when you created the key database and then click **OK**.



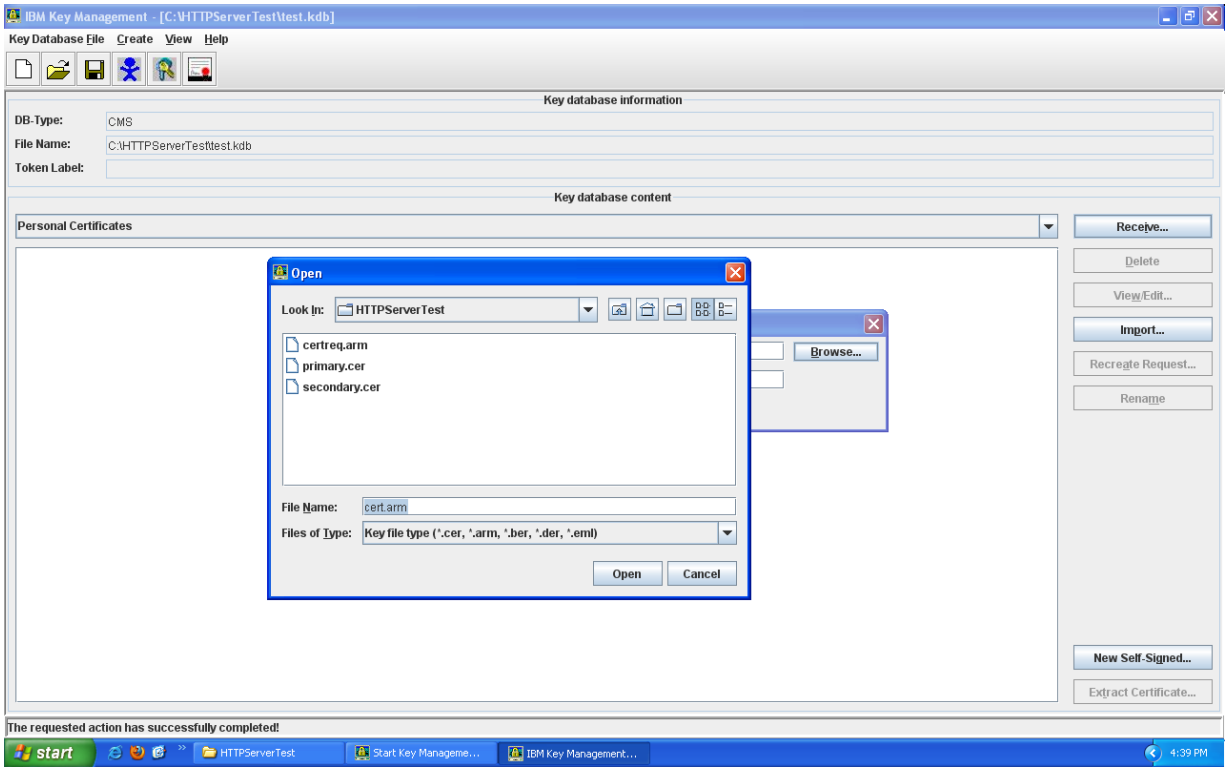
7. Select the **Personal Certificates** view.



8. Click **Receive**



9. Click **Browse** to select the name and location of the certificate file name.



10. Click **OK**

11. Verify certificate installation using the Symantec Installation Checker.

Installation Instructions for IBM Websphere using the command line

Step 1: Download the Symantec Intermediate CA Certificate

1. Download the Intermediate CA certificate.
2. Select the appropriate Intermediate CA certificate for your SSL Certificate type.
3. Copy the Intermediate CA certificate and paste it on a Notepad.
4. Save the file as **intermediate.cer**

Step 2: Install Symantec Intermediate CA Certificate

1. Run following command to add the **intermediate.cer** into the key database:

   For UNIX:

   gsk7cmd -cert -add -db filename -pw password -label label -file filename -format ascii

   For Windows**:**

   runmqckm -cert -add -db filename -pw password -extensionel -file filename -format ascii

   - **-db** filename is the fully qualified file name of a CMS key database, for example: dbkey.kdb
   - **-pw** password is the password for the CMS key database with an extansion .cms
   - **-label** is the key label attached to the certificate, for example: "ibmwebspheremqqmname"
   - **-file** filename is the fully qualified file name of the file containing the Intermediate CA certificate, for example intermediate.cer
   - **-format** ascii is the format of the certificate. The value can be ascii for Base64-encoded ASCII. The default is ascii.

Step 3: Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad
   The text file should look like:
   -----BEGIN CERTIFICATE-----

   [encoded data]

   -----END CERTIFICATE-----

3. Save the file with extension **.cer**

Step 4: Install the SSL Certificate

1. To install a certificate in iKeycmd (using UNIX command line), run following command:

   For UNIX:

   gsk7cmd -cert -receive -file filename -db filename -pw password -format ascii

   For Windows:

   runmqckm -cert -receive -file filename -db filename -pw password -format ascii

   - **-file** filename is the fully qualified file name of the file containing the personal certificate.
   - **-db** filename is the fully qualified file name of a CMS key database, for example: dbkey.kdb
   - **-pw** password is the password for the CMS key database with an extansion .cms
   - **-label** is the key label attached to the certificate, for example: "ibmwebspheremqqmname"

- **-format** ascii is the format of the certificate. The value can be ascii for Base64-encoded ASCII. The default is ascii.

Steps 5: Extract SSL Certificate

1. To extract a certificate in iKeycmd, run following command:

   For UNIX:

   gsk7cmd -cert -extract -db filename -pw password -label label -target filename -format ascii

   For Windows

   runmqckm -cert -extract -db filename -pw password -label label -target filename -format ascii

   - **-db** filename is the fully qualified pathname of a CMS key database.
   - **-pw** password is the password for the CMS key database with an extansion .cms
   - **-label** label is the label attached to the certificate.
   - **-target** filename is the name of the destination file
   - **-format** ascii is the format of the certificate. The value can be ascii for Base64-encoded ASCII. The default is asci.

2. Verify certificate installation using the Symantec Installation Checker.