



## Entrust Managed Services PKI™ Creating an SSL certificate and adding it to IBM® WebSphere® MQ 7.0

Document issue: 1.0  
Date of issue: March 2009

### Preparing the key database

1. On the WebSphere MQ computer, start the Key Management GUI:
  - On Windows, use the `strmqikm` command.
  - On UNIX, use the `gsk7ikm` command.
2. Click **Key Database File > New**.
3. Fill out the **New** dialog box:
  - From **Key database type** list, select **CMS**.
  - In the **File Name** field, specify `key.kdb`.
  - In the **Location** field, leave the default.
  - Click **OK**.
4. Fill out the **Password Prompt** dialog box:
  - In **Password**, specify a password.
  - In **Confirm Password**, retype the password.
  - Disable **Set expiration time?**
  - Enable **Stash the password to a file?**
  - Click **OK**.

**Attention:** Stashing the password is mandatory. If you do not stash the password, SSL fails.

A list of signer (CA) certificates appears. You have now set up your key database. Leave the Key Management interface open and proceed to the next section.

### Exporting CA certificates

1. On the WebSphere MQ computer, switch to the Internet Explorer browser.
2. Download the CA certificate from this URL:  
`https://<adminservices.managed.entrust.com>/cda-cgi/clientcgi.exe?action=start`  
where `<adminservices.managed.entrust.com>` is replaced with the URL of your managed PKI.
3. Save as `cacert.crt`. Save to the desktop.

4. Double-click `cacert.crt` and then click **Certification Path**. You see the chain of CA certificates.
5. Extract the root CA certificate and any intermediate CA certificates from `cacert.crt`:
  - Select the certificate from the chain.
  - Click **View Certificate > Details > Copy to file**.
  - Save to the desktop with a `.cer` extension.
  - Repeat for each certificate.

You now have a number of files on your desktop:

- `rootCAcert.cer` (the root CA certificate)
- `IntermdtCA<n_1>.cer` (these may not exist)
- `cacert.crt` (the issuing CA's certificate)

### Importing CA certificates into WebSphere MQ

1. In the IBM Key Management interface, select **Signer Certificates** from the drop-down list, if it is not already selected.
2. Click **Add**.
3. Fill out the **Add CA's Certificate from a File** dialog box:
  - For the **Data type**, select **Binary DER data**.
  - Click **Browse** and select `rootCAcert.cer`.
  - Click **OK**.
4. On the **Enter a Label** dialog box, enter `Root CA Certificate for WebSphere MQ` and click **OK**.  
The root CA certificate is added to the key database.
5. Add all remaining CA certificates to WebSphere MQ, including any intermediate CA certificates as well as `cacert.crt`. Ensure that you add your certificates in the order that they appear in the chain, starting with the closest to the root.  
Your CA certificates are now loaded.

## Creating an SSL certificate

Create a WebSphere MQ account in your PKI:

1. Go to the computer where your Entrust administrative digital ID is located.
2. Log in to Administration Services at  
`https://<admins.services.managed.entrust.com>/AdminServices`  
where <admins.services.managed.entrust.com> is replaced with the URL of your managed PKI.
3. Click **Create Account**.
4. On the **Create Account** page:
  - Select **Web Server**.
  - Select **Enterprise - Default**.
  - Click **Submit**.Another account page appears.
5. Fill out the page and click **Submit**.
6. Record the **Reference Number** and **Authorization Code**. You will use this information in later steps to create the CSR and generate the SSL certificate.  
  
You have now created a WebSphere MQ account.  
  
Generate a Certificate Signing Request (CSR) as follows:
7. In the IBM Key Management interface, click **Create > New Certificate Request**.
8. Fill out the **Create New Key [...]** dialog box as follows:
  - o **Key Label:** For a queue manager, enter `ibmwebsphermq` followed by the name of your queue manager changed to lower case. For example, `ibmwebsphermqmql`. For a WebSphere MQ client, use `ibmwebsphermq` followed by your logon user ID changed to lower case, for example `ibmwebsphermqmyuserid`.
  - o **Key size:** Pick any key size.
  - o **Common Name:** Enter the reference number that was supplied when you created the WebSphere MQ account.
  - o **Organization:** Enter your organization's name.
  - o **Country:** Specify your country's two letter country code
  - o Remaining optional fields: Either accept the default values, or type or select new values. Note that you can supply only one name in the **Organizational Unit** field.
  - o **Enter the name of a file [...]:** Accept the default `certreq.arm`.
  - o Click **OK**.

9. On the confirmation dialog box, click **OK**.

The **Personal Certificate Requests** list shows the label of the CSR you created.

Leave the IBM Key Management interface open. You will come back to it in a later step.

Generate the SSL certificate as follows:

10. Open the CSR in a text editor. By default, it is located in `<WebSph_MQ_install_root>\certreq.arm`.
11. Copy the contents to the clipboard, including the `--BEGIN NEW CERTIFICATE REQUEST--` and `--END NEW CERTIFICATE REQUEST--` lines.
12. On the WebSphere MQ computer, browse to this URL:  
`https://<admins.services.managed.entrust.com>/cda-cgi/clientcgi.exe?action=start`  
where <admins.services.managed.entrust.com> is replaced with the URL of your managed PKI.
13. Click **Create Web Server Certificate from PKCS# 10 Request**.
14. Fill out the page as follows:
  - Paste the CSR from the clipboard.
  - Enter the reference number.
  - Enter the authorization code.
  - From **Options**, select **displayed as [...] raw DER**.
  - Click **Submit Request**.
15. Click **Download** and save as `servercert.bin` to the desktop

The SSL certificate is generated and displayed in raw DER format.

You now have an SSL certificate.

## Importing the SSL certificate into WebSphere MQ

1. In the IBM Key Management interface, select **Personal Certificates** from the drop-down list.
2. Click **Receive**.
3. Fill out the **Receive Certificate from a File** dialog box as follows:
  - For the **Data type**, select **Binary DER data**.
  - Click **Browse** and choose `servercert.bin`.
  - Click **OK**.

**Note:** If you already have a personal certificate in your key database, a window appears, asking if you want to set the key you are adding as the default key in the database. Click **Yes** or **No**. The **Enter a Label** window appears. Choose a label and click **OK**.

Your SSL certificate is now loaded into WebSphere MQ.