Installing SSL Certificate on IBM HTTP Server

Digi-Sign will send you more than one certificate. In addition to the SSL certificate for your server, Digi-Sign sends an Intermediate CA Certificate and a Root CA Certificate. Before installing the SSL certificate, install both of these CA certificates into your key database. Follow the instructions in 'Storing a CA certificate' below.

If the authority who issues the SSL certificate is not a trusted CA in the key database, you must first store the CA certificate and designate the CA as a trusted CA. Then you can import the CA-signed SSL certificate into the key database. You cannot import a CA-signed SSL certificate from a CA who is not a trusted CA in the key database. For instructions see 'Storing a CA certificate' below.

Storing a CA certificate:

1. Enter IKEYMAN on a command line on UNIX, or start the Key Management utility in the IBM HTTP Server folder on Windows.
2. Select Key Database File from the main User Interface, select Open.
3. In the Open dialog box, select your key database name. Click OK.
4. In the Password Prompt dialog box, enter your password and click OK.
5. Select Signer Certificates in the Key Database content frame, click the Add button.
6. In the Add CA Certificate from a File dialog box, select the certificate to add or use the Browse option to locate the certificate. Click OK.
7. In the Label dialog box, enter a label name and click OK.

Import the CA-signed SSL certificate into a key database:

1. Enter IKEYMAN on a command line on UNIX, or start the Key Management utility in the IBM HTTP Server folder on Windows.
2. Select Key Database File from the main User Interface, select Open.
3. In the Open dialog box, select your key database name. Click OK.
4. In the Password Prompt dialog box, enter your password, click OK.
5. Select Personal Certificates in the Key Database content frame and then click the Receive button.
6. In the Receive Certificate from a File dialog box, select the certificate file. Click OK.