Installing SSL Certificate on BEA WebLogic

When you receive your certificates you need to store them in the mydomain directory.

Note: If you obtain a private key file from a source other than the Certificate Request Generator servlet, verify that the private key file is in PKCS#5/PKCS#8 PEM format.

To use a certificate chain, append the additional PEM-encoded digital certificates to the digital certificate that issued for the WebLogic Server (the Intermediate CA and Root CA certificate). The last digital certificate in the file chain will be the Root CA certificate that is self-signed. (example below:)

-----BEGIN CERTIFICATE-----
MIIB+jCCAWMCAgGjMA0GCSqGSIb3DQEBBAUAMEUxCzAJBgNVBAYTAlV
…..(your Intermediate CA certificate)…..
bW1EDp3zdHSo1TRJ6V6e6bR64eVaH4QwnNOfpSXY
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIE0DCCA7igAwIBAgIQMKeebbHpGVqxyFDTln1j1TANBgkqhkiG9w0BAQUF
.....(your Root CA certificate).....
WjEZgqr9NaoNZCZpyfZxPsOFYzoxLYEmJs3AJHxkhIHg6YQU
-----END CERTIFICATE-----

Configure WebLogic Server to use the SSL protocol, you need to enter the following information on the SSL tab in the Server Configuration window:

In the Server Certificate File Name field, enter the full directory location and name of the digital certificate for WebLogic Server.

In the Trusted CA File Name field, enter the full directory location and name of the digital certificate for the CA who signed the digital certificate of WebLogic Server. In the Server Key File Name field, enter the full directory location and name of the private key file for WebLogic Server.

Use the following command-line option to start WebLogic Server. -D weblogic.management.pkpassword=password where password is the password defined when requesting the digital certificate.

Storing Private Keys and Digital Certificates

Once you have a private key and digital certificate, copy the private key file generated by the Certificate Request Generator servlet and the digital certificate you received into the mydomain directory. Private Key files and digital certificates are generated in either PEM or Definite Encoding Rules (DER) format. The filename extension identifies the format of the digital certificate file. A PEM (.pem) format private key file begins and ends with the following lines, respectively:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
-----END ENCRYPTED PRIVATE KEY-----
```

A PEM (.pem) format digital certificate begins and ends with the following lines, respectively:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

Note: Typically, the digital certificate file for a WebLogic Server is in one file, with either a .pem or .der extension, and the WebLogic Server certificate chain is in another file. Two files are used because different WebLogic Servers may share the same certificate chain.

The first digital certificate in the certificate authority file is the first digital certificate in the WebLogic Server's certificate chain. The next certificates in the file are the next digital certificates in the certificate chain. The last certificate in the file is a self-signed digital certificate that ends the certificate chain. A DER (.der) format file contains binary data. WebLogic Server requires that the file extension match the contents of the certificate file.

Note: If you are creating a file with the digital certificates of multiple certificate authorities or a file that contains a certificate chain, you must use PEM format. WebLogic Server provides a tool for converting DER format files to PEM format, and visa versa.