Entrust.Net

Technical Information – CSR Generation

Client Confidential

TABLE OF CONTENTS

CSR GENERATION: VALID CSR FORMATS 3

1. APPACHE (MOD_SSL) 4

1.1 APPACHE(MOD_SSL): CSR GENERATION 4

2. APPACHE - SSL 7

2.1 APACHE - SSL: CSR GENERATION 7

3. O'REILLY WEBSITE PROFESSIONAL 2.X 10

3.1 O'REILLY WEBSITE PROFESSIONAL 2.X: CSR GENERATION 10

4. NETSCAPE ENTERPRISE SERVER 3.5X AND 3.6X 13

4.1 NETSCAPE ENTERPRISE SERVER 3.63 : CSR GENERATION 13

5. LOTUS DOMINO R5 16

5.1 LOTUS DOMINO R5 : CSR GENERATION 16

6. MICROSOFT INTERNET INFORMATION SERVER 5.0 18

6.1 MICROSOFT IIS 5.0: CSR GENERATION 18

7. MICROSOFT INTERNET INFORMATION SERVER 4.0 21

7.1 MICROSOFT INTERNET INFORMATION SERVER 4.0 : CSR GENERATION 21

8. MICROSOFT INTERNET INFORMATION SERVER 2.X AND 3.X 24

8.1 MICROSOFT INTERNET INFORMATION SERVER 2.X AND 3.X : CSR GENERATION 24

9. C2NET STRONGHOLD 27

9.1 C2NET STRONGHOLD : CSR GENERATION 27

10. BEA WEBLOGIC 4.5.X 30

10.1 BEA WEBLOGIC 4.5.X :CSR GENERATION 30

11. RAVEN SSL 1.4.1 MODULE FOR APACHE SUPPORT 32

11.1 RAVEN SSL 1.4.1 MODULE FOR APPACHE SUPPORT 32

CSR GENERATION: VALID CSR FORMATS

Valid Certificate Request (CSR) formats

You can send your CSR to Entrust in either PKCS #10 (Base-64 encoded) format or PEM format. By default, the servers supported by Entrust generate PCKS #10-formatted CSRs. These CSRs look similar to the following:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBujCCASMCAQAwejELMAkGA1UEBhMCQ0ExEzARBgNVBAgTC
lRFc3QgU3RhdGUxETAPBgNVBAcTCENvbG9yYWR0MRswGQYDVQ
QKExJDYW5hZGlhbiBUZXN0IE9yZy4xEjAQBgNVBAsTCU9VIE9
mZmljZTESMBAGA1UEAxMJd3d3LmV4LmNhMIGfMA0GCSqGSIb3
DQEBAQUAA4GNADCBiQKBgQD5PIij2FNa+Zfk1OHtptspcSBkf
kfZ3jFxYA6ypo3+YbQhO3PLTvNfQj9mhb0xWyvoNvL8Gnp1GU
Pgiw9GvRao603yHebgc2bioAKoTkWTmW+C8+Ka42wMrVrgcW3
2rNYmDnDWOSBWWR1L1j1YkQBK1nQnQzV3U/h0mr+ASE/nV7wI
DAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAAAhx1oQcw6P8cDED
G4UiwB0DOoQnFb3WYVl7d4+6lfOtKfuL/Ep0blLWXQoVpOICF
3gfAF6wcAbeg5MtiWwTwvXRtJ2jszsZbpOuIt0WU1+cCYivxu
Ti18CQNQrsrD4s2ZJytkzDTAcz1Nmiuh93eqYw+kydUyRYlOM
EIomNFIQ=
-----END CERTIFICATE REQUEST-----
```

CSRs in PEM format can also be generated by some of the servers supported by Entrust. These CSRs look similar to the following:

```
-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type:4,MIC-ONLY
Content-Domain:RFC822 Originator-Certificate:
MIIB6DCCAZICAQAwDQYJKoZIhvcNAQECBQAwfzELMAkGA1UEB
hMCRlIxETAPBgNVBAgTCE1vcmJpaGFuMQ8wDQYDVQQHEwZWYW
5uZXMxEzARBgNVBAoTCmN5YmVyb3Vlc3QxGDAWBgNVBAsTD3R
lY2huaWNhbCBzdGFmZjEdMBsGA1UEAxMUc2VjdXJlLmN5YmVy
b3Vlc3QuZnIwHhcNOTcwMTI4MTI1NzQ2WhcNOTgwMTI3MTI1O
TI2WjB/MQswCQYDVQQGEwJGUjERMA8GA1UECBMITW9yYmloYW
4xDzANBgNVBAcTBlZhbm5lczETMBEGA1UEChMKY3liZXJvdWV
zdDEYMBYGA1UECxMPdGVjaG5pY2FsIHN0YWZmMR0wGwYDVQQD
ExRzZWN1cmUuY3liZXJvdWVzdC5mcjBcMA0GCSqGSIb3DQEBA
QUAA0sAMEgCQQC2Coa23fXNjODNfe/R+CzBCgMi7N2W/8EHhg
nElZlHQxJXtPdzCgtYQFIPOKHn+7f8eBd+HX+MVi9pR+ITTyB
7AgMBAAEwDQYJKoZIhvcNAQECBQADQQATSHCcdzfF3jjfjDm8
aX4Uml2qkvnViLxk2FVnValupVh40kiIGwhhfKBY5xWQondV+
zVRXZyINY8sx8AFOcQh MIC-Info: RSA-MD5,RSA,
J1pln0dwsjb6RI0zx+Kaia7f3eJL2RF6+paIwq4ap0jr4lt+R
RILO2t5/jSRBPAIe1B7MJ+gJ7RiYqekU3My5g== V2ViU2l0Z
SBQcm8NCg==
-----END PRIVACY-ENHANCED MESSAGE-----
```

1. APPACHE (MOD_SSL)

1.1 APPACHE(MOD_SSL): CSR GENERATION

Generating a key pair and CSR with Appache (mod_ssl)

Entrust strongly recommends that you take the following precautions to ensure that you are able to install your Entrust.net Web server certificate:

- Do not use commas in any of the fields you fill in when creating the CSR. Commas are interpreted as the end of the field and will cause an invalid CSR to be generated.
- Do not use any of the following characters in the Web server Distinguished Name: ! @ # $ % ^ * ( ) ~ ? &gt; &lt; &amp; / \
- When you generate the CSR, make sure you are logged in as an Administrator to the computer that hosts your Web server.

Entrust strongly recommends that you upgrade to the latest versions of Apache, mod_ssl, and SSLeay before generating a key pair and CSR.

Note: These instructions assume that you are using SSLeay with mod_ssl. If you are using OpenSSL instead of SSLeay, you can find additional instructions at http://www.modssl.org/docs/2.3/ssl_faq.html.

To generate the key pair and CSR use the ssleay utility that comes with the SSLeay distribution. It is normally installed in SSL_BASE/bin directory, where SSL_BASE is the path you specified when building Apache with mod_ssl.

To generate a key pair and CSR with Apache (mod_ssl):

1. Select three large (approximately 200 KB) files from your hard drive for use as a seed for your random data. These files are referred to as “randfile1”, “randfile2”, and “randfile3” in the steps below.

2. Type ssleay genrsa -des3 -rand randfile1:randfile2:randfile3 1024 > servername.key. This will generate a 1024 bit RSA key pair and store it in the file servername.key.

3. Enter a passphrase when prompted. Please remember the passphrase you choose. If you forget this passphrase you will not be able to use your Entrust.net Web server certificate. If you write down this passphrase, please be sure to store it in a secure location.

4. Back up the file that contains your private key. Please be sure that the backup is stored in a secure location. Someone with access to your private key could decrypt the SSL-protected data sent and received by your Web server.

5. To generate the CSR type ssleay req -new -key servername.key –out servername.csr, where servername.key and servername.csr are, respectively, the key file you created and the file that will hold your CSR.

6. Enter the information you wish to include in your Web server Distinguished Name (DN) when prompted keeping the following example in mind:

   “O” Organization = Entrust Technologies

“OU”	Organizational Unit	= Entrust.net
“CN”	Common Name	= www.entrust.net (this is the URL of your website)
“C”	Country / Region	= CA
“St”	State / Province	= Ontario
“L”	Locality	= Ottawa

For more detailed information on the DN please see Creating Your Distinguished Name.

7. Once you have entered the required information the CSR is created and stored in a file with a .csr extension (for example, &quot;servername.csr&quot;). The file contains a section that looks like the example below.

```
-----BEGIN CERTIFICATE REQUEST-----
MIISDOIUlkmlsRRlkSllskjauASKJlalOSISLKjwBgNV
BAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwtPcHBvcnR1bml0aTEYMBYGA1UE
CxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cu
Zm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEBAQUAAAkl
mLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6pDvAjuy
C+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diuu
PlHDAgEDoAAwDQYJKoZIhvcNAQEEBQADQQBf8LSLKknl
sklSSLlworrr334ZmXD1AvUjuDPCWzFupReiq7UR8Z0w
JUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END CERTIFICATE REQUEST-----
```

8. Open the file that contains the CSR (for example, “servername.”) in a text editor and select the entire contents of this file (including the “-----BEGIN CERTIFICATE REQUEST-----“ and “-----END CERTIFICATE REQUEST-----“ lines)

9. Copy the selected information to the clipboard. You will use this information in the Entrust.net online registration process.

10. Close your text editor.

    To use the CSR to obtain your Entrust.net certificate(s), go to http://www.entrust.net.

If you are having difficulty finding what you're looking for, please e-mail us.

Creating Your Distinguished Name

Country code: The two-letter ISO abbreviation for your country (for example, US for the United States).

State or Province: The name of the state or province in which your organization has its head office. Please enter the full name of the state or province. Do not abbreviate.

Locality: Usually the name of the city in which your organization has its head office.

Organization: The name under which your organziation is registered. This organization must own the domain name that appears in common name of your Web server. Do not abbreviate your organization's name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?. This is the name you recorded in the enrollment guide.

Organizational unit: Normally the name of the department or group that will be using the secure Web server.

Common name: The name of your Web server as it will appear in the server's URL (for example, www.entrust.com). This name must be identical to the fully qualified domain name of the Web server for which you are requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse to establish a secure connection with your site. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Do not use use wildcards such as * or ?, and do not use an IP address.

2. APPACHE - SSL

2.1 APACHE - SSL: CSR GENERATION

Generating a key pair and CSR with Apache – SSL

Entrust strongly recommends that you take the following precautions to ensure that you are able to install your Entrust.net Web server certificate:

- Do not use commas in any of the fields you fill in when creating the CSR. Commas are interpreted as the end of the field and will cause an invalid CSR to be generated.
- Do not use any of the following characters in the Web server Distinguished Name: ! @ # $ % ^ * ( ) ~ ? > < & / \
- When you generate the CSR, make sure you are logged in as an Administrator to the computer.THAT HOSTS YOUR WEB SERVER.

Entrust strongly recommends that you upgrade to the latest versions of Apache-SSL and SSLeay (or OpenSSL) before generating a key pair and CSR.

Note: These instructions assume that you are using SSLeay with Apache-SSL. If you are using OpenSSL instead of SSLeay, you can find additional instructions at http://www.modssl.org/docs/2.3/ssl_faq.html.

To generate the key pair and CSR you use a utility named ssleay. It is normally installed in SSLTOP/bin where SSLTOP is the path you specified when building Apache-SSL.

To generate a key pair and CSR, follow these steps:

1. Select three large (approximately 200 KB) files from your hard drive for use as a seed for your random data. These files are referred to as “randfile1”, “randfile2”, and “randfile3” in the steps below.

2. Enter ssleay genrsa -des3 -rand randfile1:randfile2:randfile3 1024 > servername.key. This will generate a 1024 bit RSA key pair and store it in the file servername.key.

3. Enter a passphrase when prompted. Please remember the passphrase you choose. If you forget this passphrase you will not be able to use your Entrust.net Web server certificate. If you write down this passphrase, please be sure to store it in a secure location.

4. Back up the file that contains your private key. Please be sure that the backup is stored in a secure location. Someone with access to your private key could decrypt the SSL-protected data sent and received by your Web server.

5. Type ssleay req -new -key servername.key –out servername.csr to generate the CSR, where servername.key and servername.csr are, respectively, the key file you created and the file that will hold your CSR.

6. When prompted, enter the information you wish to include in your Web server Distinguished Name (DN), keeping the following example in mind:

“O”	Organization	= Entrust Technologies
“OU”	Organizational Unit	= Entrust.net
“CN”	Common Name	= www.entrust.net (this is the URL of your website)
“C”	Country / Region	= CA
“St”	State / Province	= Ontario
“L”	Locality	= Ottawa

For more detailed information on this please see Creating Your Distinguished Name.

7. Once you have entered the required information the CSR will be created and stored in a file with a .csr extension (for example, “servername.csr”). The file will contain a section that looks like the example below. This section is the CSR itself.

```
-----BEGIN CERTIFICATE REQUEST-----
MIISDOIUlkmlsRRlkSllskjauASKJlalOSISLKjwBgNV
BAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwtPcHBvcnR1bml0aTEYMBYGA1UE
CxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cu
Zm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEBAQUAAAkl
mLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6pDvAjuy
C+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diuu
PlHDAgEDoAAwDQYJKoZIhvcNAQEEBQADQQBf8LSLKknl
sklSSLlworrr334ZmXD1AvUjuDPCWzFupReiq7UR8Z0w
JUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END CERTIFICATE REQUEST-----
```

8. Open the file that contains the CSR (for example, "servername.csr") in a text editor and copy the CSR section (including the “-----BEGIN CERTIFICATE REQUEST-----“ and “-----END CERTIFICATE REQUEST-----“ lines) to the clipboard. You will use this information in the Entrust.net online registration process.

9. Paste the CSR into the space provided in the online request form.

10. Close your text editor.

    To use the CSR to obtain your Entrust.net certificate(s), go to http://www.entrust.net.

If you are having difficulty finding what you're looking for, please e-mail us.

Creating Your Distinguished Name

Country code: The two-letter ISO abbreviation for your country (for example, US for the United States).

State or Province: The name of the state or province in which your organization has its head office. Please enter the full name of the state or province. Do not abbreviate.

Locality: Usually the name of the city in which your organization has its head office.

Organization: The name under which your organization is registered. This organization must own the domain name that appears in common name of your Web server. Do not abbreviate your organization's name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?. This is the name you recorded in the enrollment guide.

Organizational unit: Normally the name of the department or group that will be using the secure Web server.

Common name: The name of your Web server as it will appear in the server's URL (for example, www.entrust.com). This name must be identical to the fully qualified domain name of the Web server for which you are requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse to establish a secure connection with your site. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Do not use wildcards such as * or ?, and do not use an IP address.

3. O’REILLY WEBSITE PROFESSIONAL 2.X

3.1 O’REILLY WEBSITE PROFESSIONAL 2.X: CSR GENERATION

Generating a key pair and CSR with O’Reilly WebSite Professional 2.x:

Entrust strongly recommends that you take the following precautions to ensure that you are able to install your Entrust.net Web server certificate:

- Do not use commas in any of the fields you fill in when creating the CSR. Commas are interpreted as the end of the field and will cause an invalid CSR to be generated.
- Do not use any of the following characters in the Web server Distinguished Name: ! @ # $ % ^ * ( ) ~ ? > < & / \
- When you generate the CSR, make sure you are logged in as an Administrator to the computer that hosts your Web server.

To generate a key pair and CSR in O'Reilly WebSite Professional 2.x:

1. Ensure that your Web server contains the root certificate used by Entrust if you have not already done so. See Checking the root certificate for instructions.

2. Open the WebSite Server Properties window (in Microsoft Windows NT, right-click the WebSite Pro icon in the Windows system tray and select ”WebSite server properties” from the pop-up menu).

3. Click the Key Ring tab.

4. Click New Key Pair. The New Key Pair wizard appears.

5. Step through the wizard to create a new key pair, keeping the following example in mind:

“O”	Organization	= Entrust Technologies
“OU”	Organizational Unit	= Entrust.net
“CN”	Common Name	= www.entrust.net (this is the URL of your website)
“C”	Country / Region	= CA
“St”	State / Province	= Ontario
“L”	Locality	= Ottawa

For more detailed information on the DN please see Creating Your Distinguished Name.

6. Once you have finished with the wizard, your request is saved to the file you specified.

7. Please be sure to back up the new key pair you generated. The key file is called “website.key” and it is located in the “\WebSite\admin” directory. The private key is a very sensitive piece of information. Be sure to store it in a secure location. Someone with access to your private key could decrypt the SSL-protected data sent and received by your Web server.

8. Open the certificate request file in a text editor. The certificate request file is named “cert-request.pem” by default although you may have given it a different name in the New Key Pair wizard. The CSR is the section of the file that looks like this example:

```
-----BEGIN CERTIFICATE REQUEST-----
MIISDOIUlkmlsRRlkSllskjauASKJlalOSISLKjwBgNV
BAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwtPcHBvcnR1bml0aTEYMBYGA1UE
CxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cu
Zm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEBAQUAAAkl
mLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6pDvAjuy
C+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diuu
PlHDAgEDoAAwDQYJKoZIhvcNAQEEBQADQQBf8LSLKknl
sklSSLlworrr334ZmXD1AvUjuDPCWzFupReiq7UR8Z0w
JUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END CERTIFICATE REQUEST-----
```

9. Select the entire contents of the file (including the “-----BEGIN NEW CERTIFICATE REQUEST-----“ and “-----END NEW CERTIFICATE REQUEST-----“ lines) and copy it to the clipboard. You will use this information in the Entrust.net online registration process.

10. Close your text editor.

    To use the CSR to obtain your Entrust.net certificate(s), go to http://www.entrust.net

If you are having difficulty finding what you are looking for, please e-mail us.

Checking the root certificate

To find out if your Web server contains the updated root certificate for Entrust, follow these steps:

1. Open the WebSite Server Properties window (in Microsoft Windows NT, right-click the WebSite Pro icon in the Windows system tray and select WebSite server properties from the pop-up menu).

2. Click the Key Ring tab.

3. Select Trusted roots.

4. Double-click Thawte Server CA.

5. Click the Certificate tab.

6. If the expiry date is December 31, 2020, click the OK button and skip the remainder of these steps; you have the updated root certificate. If the expiry date is not December 31, 2020, continue through the steps below to delete the current certificate and import a new one.

7. Click the OK button.

8. Right-click the Thawte Server CA entry, select Delete, and click Yes in the confirmation dialog.

9. Close and reopen the WebSite Server Properties window. You must do this before you can import the new root certificate. In a Web browser, open the URL http://www.entrust.net/support/serverbasic.txt. The new root certificate appears in your browser window.

10. Copy the root certificate including the header and trailer from your browser window into your clipboard.

11. Open a text editor, copy the root certificate into the editor and save the file.

12. In the WebSite Server Properties window, click the Key Ring tab.

13. Select Trusted roots and click Add Trusted Root....

14. Select the file that contains the new root certificate and click the OK button.

15. Restart your server.

You have just imported a root certificate that will be valid until 2020.

Creating Your Distinguished Name

Country code: The two-letter ISO abbreviation for your country (for example, US for the United States).

State or Province: The name of the state or province in which your organization has its head office. Please enter the full name of the state or province. Do not abbreviate.

Locality: Usually the name of the city in which your organization has its head office.

Organization: The name under which your organization is registered. This organization must own the domain name that appears in common name of your Web server. Do not abbreviate your organization's name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?. This is the name you recorded in the enrollment guide.

Organizational unit: Normally the name of the department or group that will be using the secure Web server.

Common name: The name of your Web server as it will appear in the server's URL (for example, www.entrust.com). This name must be identical to the fully qualified domain name of the Web server for which you are requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse to establish a secure connection with your site. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Do not use wildcards such as * or ?, and do not use an IP address.

4. NETSCAPE ENTERPRISE SERVER 3.5X AND 3.6X

4.1 NETSCAPE ENTERPRISE SERVER 3.5X AND 3.6X : CSR GENERATION

Generating a key pair and CSR with Netscape Enterprise Server 3.5x and 3.6x

Entrust strongly recommends that you take the following precautions to ensure that you are able to install your Entrust.net Web server certificate:

- Do not use commas in any of the fields you fill in when creating the CSR. Commas are interpreted as the end of the field and will cause an invalid CSR to be generated.
- Do not use any of the following characters in the Web server Distinguished Name: ! @ # $ % ^ * ( ) ~ ? > < & / \
- When you generate the CSR, make sure you are logged in as an Administrator to the computer that hosts your Web server.

To generate a key pair and CSR with Netscape Enterprise server 3.51, use a utility named "sec-key". Follow these steps:

1. On the computer that hosts Netscape Enterprise server, run the program <server_root>bin\admin\admin\bin\sec-key.

2. At the prompt, enter a name (alias) for the new key file. Entrust recommends that you choose a name similar to that of your server. The name cannot contain spaces, but it can use the symbols that your operating system allows in filenames (such as underscores). By default, the key file is stored in <server_root>/alias/<key_pair_name>-key.db. For instance, if you named the key file "my_server", the file would be stored in the directory <server_root>/alias/my_server-key.db.

3. Click the OK button. An information dialog appears.

4. Click the OK button. A dialog containing a progress meter appears. Enter random data as requested. For example, if you are using Microsoft Windows NT^{TM} move the mouse pointer around your desktop until the progress meter is full. Your random data is used in creating the key pair. A password dialog automatically appears.

5. Enter a password of eight characters or more for your key file. The password must contain at least one character that is not a letter (for instance, a number or punctuation mark). Make sure you memorize this password. The security of your server is only as good as the security of the key file and its password. Once you have enabled SSL for your server, you will be asked to enter the key file password every time you start the server.

6. Click the OK button. A confirmation dialog appears.

7. Enter your password again and click the OK button. A confirmation dialog appears explaining where the key file has been stored.

8. Click the OK button.

9. Back up your key file. If you lose your key file or it becomes corrupted you will not be able to use your Entrust.net Web server certificate. Please store the backup files in a secure location. Someone with access to your private key could decrypt the SSL-protected data sent and received by your Web server.

Once you have generated a key pair you are ready to generate a CSR that you can submit to Entrust. Follow these steps:

1. Log on to the Netscape administration server.

2. Click Keys > Certificates in the General Administration section.

3. Click Request Certificate. The Request a Server Certificate page appears. Select New certificate.

4. Select CA Email address and type your own email address in the space provided.

5. From the Alias drop-down list, select the key file that contains the public key you wish to include in the certificate.

6. Enter a password for your key file in the space provided.

7. Enter your name, telephone number, and email address in the spaces provided.

8. Enter the distinguished name (DN) of your server, keeping the following example in mind:

“O”	Organization	= Entrust Technologies
“OU”	Organizational Unit	= Entrust.net
“CN”	Common Name	= www.entrust.net (this is the URL of your website)
“C”	Country / Region	= CA
“St”	State / Province	= Ontario
“L”	Locality	= Ottawa

For more detailed information on the DN please see Creating Your Distinguished Name.

9. Click the OK button once you have entered the necessary information. Your certificate request is displayed. The CSR is the section of the request that looks like the example below.
Note: The request is also saved in a file; please be sure to back up the request file.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIISDOIUlkmlsRRlkSllskjauASKJlalOSISLKjwBgNV
BAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwtPcHBvcnR1bml0aTEYMBYGA1UE
CxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cu
Zm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEBAQUAAAkl
mLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6pDvAjuy
C+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diuu
PlHDAgEDoAAwDQYJKoZIhvcNAQEEBQADQQBf8LSLKknl
sklSSLlworrr334ZmXD1AvUjuDPCWzFupReiq7UR8Z0w
iJUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END NEW CERTIFICATE REQUEST-----
```

10. Copy the CSR (including the “-----BEGIN NEW CERTIFICATE REQUEST-----“ and “-----END NEW CERTIFICATE REQUEST-----“ lines) to the clipboard. You will use this information in the Entrust.net online registration process.

To use the CSR to obtain your Entrust.net certificate(s), go to http://www.entrust.net.

If you are having difficulty finding what you're looking for, please e-mail us.

Creating Your Distinguished Name

Country code: The two-letter ISO abbreviation for your country (for example, US for the United States).

State or Province: The name of the state or province in which your organization has its head office. Please enter the full name of the state or province. Do not abbreviate.

Locality: Usually the name of the city in which your organization has its head office.

Organization: The name under which your organization is registered. This organization must own the domain name that appears in common name of your Web server. Do not abbreviate your organization's name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?. This is the name you recorded in the enrollment guide.

Organizational unit: Normally the name of the department or group that will be using the secure Web server.

Common name: The name of your Web server as it will appear in the server's URL (for example, www.entrust.com). This name must be identical to the fully qualified domain name of the Web server for which you are requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse to establish a secure connection with your site. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Do not use wildcards such as * or ?, and do not use an IP address.

5. LOTUS DOMINO R5

5.1 LOTUS DOMINO R5 : CSR GENERATION

Generating a key pair and CSR with Lotus Domino R5

Entrust strongly recommends that you take the following precautions to ensure that you are able to install your Entrust.net Web server certificate:

- Do not use commas in any of the fields you fill in when creating the CSR. Commas are interpreted as the end of the field and will cause an invalid CSR to be generated.
- Do not use any of the following characters in the Web server Distinguished Name: ! @ # $ % ^ *( ) ~ ? > < & / \
- When you generate the CSR, make sure you are logged in as an Administrator to the computer that hosts your Web server.

To generate a key pair and CSR in Domino R5:
From the Server Certificate Administration database interface, perform the following procedure to generate the key ring and the CSR:

1. Click the 1. Create Key Ring option.

2. Enter the appropriate information in each field keeping the following example in mind:

"O"	Organization	= Entrust Technologies
"OU"	Organizational Unit	= Entrust.net
"CN"	Common Name	= www.entrust.net (this is the URL of your website)
"C"	Country / Region	= CA
"St"	State / Province	= Ontario
"L"	Locality	= Ottawa

   For more detailed information on this please see Creating Your Distinguished Name.

3. Click the Create Key Ring button. This generates the key ring file and stores it in the location displayed below the Key Ring Information area of the screen. The Server Certificate Administration interface screen appears.
   Note: It is very important to protect the generated key ring file. Anyone with access to this file and its password could set up a server of their own that appears in every way to be your authentic server.

4. Click the 2. Create Certificate Request option.

5. Follow the instructions that are displayed onscreen.

6. Click the Create Certificate Request button. The Certificate Request Created dialog box appears.

7. Select the entire contents of the window at the bottom of the dialog box (including the "-----BEGIN NEW CERTIFICATE REQUEST-----" and "-----END NEW CERTIFICATE REQUEST-----" lines).

8. Copy the selected text. You will paste this text into the appropriate form on the Entrust.net Web site when asked to supply a CSR.
   To use the CSR to obtain your Entrust.net certificate(s), go to http://www.entrust.net.

If you are having difficulty finding what you are looking for, please e-mail us.

Creating Your Distinguished Name

Country code: The two-letter ISO abbreviation for your country (for example, US for the United States).

State or Province: The name of the state or province in which your organization has its head office. Please enter the full name of the state or province. Do not abbreviate.

Locality: Usually the name of the city in which your organization has its head office.

Organization: The name under which your organization is registered. This organization must own the domain name that appears in common name of your Web server. Do not abbreviate your organization's name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?. This is the name you recorded in the enrollment guide.

Organizational unit: Normally the name of the department or group that will be using the secure Web server.

Common name: The name of your Web server as it will appear in the server's URL (for example, www.entrust.com). This name must be identical to the fully qualified domain name of the Web server for which you are requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse to establish a secure connection with your site. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Do not use wildcards such as * or ?, and do not use an IP address.

6. MICROSOFT INTERNET INFORMATION SERVER 5.0

6.1 MICROSOFT IIS 5.0: CSR GENERATION

Generating a key pair and CSR with Microsoft Windows 2000 / Internet Information Server 5.0

Entrust strongly recommends that you take the following precautions to ensure that you are able to install your Entrust.net Web server certificate:

- Do not use commas in any of the fields you fill in when creating the CSR. Commas are interpreted as the end of the field and will cause an invalid CSR to be generated.
- Do not use any of the following characters in the Web server Distinguished Name: ! @ # $ % ^ * ( ) ~ ? &gt; &lt; &amp; / \
- When you generate the CSR, make sure you are logged in as an Administrator to the computer that hosts your Web server.

To generate a key pair and CSR in Internet Information Server 5.0:

1. Open the Internet Information Services window by selecting Start Menu > Programs > Administrative Tools > Internet Services Manager.

2. Highlight the Web server you wish to secure, right-click on it and select Properties.

3. Select the Directory Security tab.

4. Select Server Certificate under the Secure Communications section. The Web Server Certificate Wizard appears.

5. Click the Next button.

6. Select the Create a new certificate option and click the Next button.

7. Select the Prepare the request now, but send it later option and click the Next button.

8. Enter a name for the CSR you are generating. For example, EntrustCSR.

9. Select an appropriate Bit length for the key-pair you are creating. The two most common options are Bit Lengths of either 512 or 1024. Once you have selected the desired Bit length click the Next button.

   Note: Selecting a bit length of 512 does not mean that your web server will be able to establish 40-bit SSL/TLS sessions only. The level of security for an SSL/TLS session depends on the capabilities of the Web browser accessing your site. A 128-bit SSL/TLS session can be established only if the Web browser accessing your site supports 128-bit security.

   You are prompted to enter values for your CSR (Certificate Signing Request).

   Step through the wizard to create a new key pair keeping the following example in mind:

“O” Organization = Entrust Technologies

“OU”	Organizational Unit	= Entrust.net
“CN”	Common Name	= www.entrust.net (this is the URL of your website)
“C”	Country / Region	= CA
“St”	State / Province	= Ontario
“L”	Locality	= Ottawa

For more detailed information on this please see Creating Your Distinguished Name.

10. Type an easily remembered filename when you are prompted to enter a name for the Certificate Request. For example, EntrustReq.txt

11. Note the location of the file and click the Next button. A confirmation screen appears.

12. Click the Next button to proceed. The completion screen appears.

13. Click the Finish button to complete the key pair generation process.

14. Browse to the location of the CSR file and open it. The CSR looks like this example:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIISDOIUlkmlsRRlkSllskjauASKJlalOSISLKjwBgN
VBAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZS
BUb3duMRQwEgYDVQQKEwtPcHBvcnR1bml0aTEYMBYGA
1UECxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3
d3cuZm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEBAQU
AAAklmLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6p
DvAjuyC+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh
2V7diuuPlHDAgEDoAAwDQYJKoZIhvcNAQEEBQADQQBf
8LSLKknlsklSSLlworrr334ZmXD1AvUjuDPCWzFupRe
iq7UR8Z0wiJUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END NEW CERTIFICATE REQUEST-----
```

15. Select the entire contents of this file (including the “-----BEGIN NEW CERTIFICATE REQUEST-----“ and “-----END NEW CERTIFICATE REQUEST-----“ lines).

16. Copy the selected information to the clipboard. You will use this information in the Entrust.net online registration process.
    To use the CSR to obtain your Entrust.net certificate(s), go to http://www.entrust.net

If you are having difficulty finding what you are looking for, please e-mail us.

Creating Your Distinguished Name

Country code: The two-letter ISO abbreviation for your country (for example, US for the United States).

State or Province: The name of the state or province in which your organization has its head office. Please enter the full name of the state or province. Do not abbreviate.

Locality: Usually the name of the city in which your organization has its head office.

Organization: The name under which your organization is registered. This organization must own the domain name that appears in common name of your Web server. Do not abbreviate your organization's name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?. This is the name you recorded in the enrollment guide.

Organizational unit: Normally the name of the department or group that will be using the secure Web server.

Common name: The name of your Web server as it will appear in the server's URL (for example, www.entrust.com). This name must be identical to the fully qualified domain name of the Web server for which you are requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse to establish a secure connection with your site. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Do not use wildcards such as * or ?, and do not use an IP address.

7. MICROSOFT INTERNET INFORMATION SERVER 4.0

7.1 MICROSOFT INTERNET INFORMATION SERVER 4.0 : CSR GENERATION

Generating a key pair and CSR with Microsoft Internet Information Server 4.0

It is strongly recommended that you take the following precautions to ensure that you will be able to install your Entrust.net Web server certificate:

- If you reside in Canada or the United States, install the 128-bit version of Internet Explorer on the computer that hosts your Web server. This software updates some important cryptographic files (in particular “schannel.dll”). It is available from Microsoft at http://microsoft.com/windows/ie/download/128bit/intro.htm.
- Do not use commas in any of the fields you fill in when creating the CSR. Commas are interpreted as the end of the field and will cause an invalid CSR to be generated.
- Do not use any of the following characters in the Web server Distinguished Name: ! @ # $ % ^ * ( ) ~ ? &gt; &lt; &amp; / \
- When you generate the CSR, make sure you are logged in as an Administrator to the computer that hosts your Web server.

To generate a key pair and CSR in Internet Information Server 4.0, follow these steps:

1. Run the Internet Service Manager.

2. Select your Web site and click the Key Manager icon. The Key Manager appears.

3. Click Key > Create New Key.... The Create New Key Wizard appears.

4. In the first step of the wizard, select Put the request in a file that you will send to an authority and enter a name for your CSR file.

5. Proceed through the Create New Key Wizard keeping the following example in mind:

“O”	Organization	= Entrust Technologies
“OU”	Organizational Unit	= Entrust.net
“CN”	Common Name	= www.entrust.net (this is the URL of your website)
“C”	Country / Region	= CA
“St”	State / Province	= Ontario
“L”	Locality	= Ottawa

Note:

- Do not use the following characters in any of the fields in the Create New Key wizard: > < & ! @ # $ % ^ * ( ) ~ ? / \.
- Make sure that the password you enter contains fewer than 8 characters. It is very important that you remember this password. If you forget it you will not be able to use your Entrust.net Web server certificate. If you write the password down, please be sure to store it in a secure location.

- It is recommended that you choose a 1024-bit key if that option is available.

For more detailed information on this please see Creating Your Distinguished Name.

6. When you have completed the wizard a CSR will be generated and stored in the file you specified.

7. Click Computers > Commit Changes Now to save the new key. Then click the OK button in the confirmation dialog box.

8. Please be sure to back up your private key. To do this, select the key in Key Manager, click Key > Export Key > Backup File, click the OK button in the confirmation dialog box and choose a name for the key file. The private key and password are very sensitive. Be sure to store the key file in a secure location. If you write down the password please store it in a secure location as well. Someone with access to your private key and password could decrypt the SSL-protected data sent and received by your Web server.

9. Open the file that contains your CSR in a text editor. You specified the name of this file in the Create New Key Wizard. The CSR is the section of the file that looks like the example below. Please be sure to back up this file.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIISDOIUlkmlsRRlkSllskjauASKJlalOSISLKjwBgN
VBAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZS
BUb3duMRQwEgYDVQQKEwtPcHBvcnR1bml0aTEYMBYGA
1UECxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3
d3cuZm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEBAQU
AAAklmLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6p
DvAjuyC+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh
2V7diuuPlHDAgEDoAAwDQYJKoZIhvcNAQEEBQADQQBf
8LSLKknlsklSSLlworrr334ZmXD1AvUjuDPCWzFupRe
iq7UR8Z0wiJUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END NEW CERTIFICATE REQUEST-----
```

10. Select the entire contents of this file (including the "-----BEGIN NEW CERTIFICATE REQUEST-----" and "-----END NEW CERTIFICATE REQUEST-----" lines).

11. Copy this to the clipboard. You will use this information in the Entrust.net online registration process.

12. Close your text editor.

    To use the CSR to obtain your Enrust.net certificate(s), go to http://www.entrust.net

If you are having difficulty finding what you are looking for, please e-mail us.

Creating Your Distinguished Name

Country code: The two-letter ISO abbreviation for your country (for example, US for the United States).

State or Province: The name of the state or province in which your organization has its head office. Please enter the full name of the state or province. Do not abbreviate.

Locality: Usually the name of the city in which your organization has its head office.

Organization: The name under which your organization is registered. This organization must own the domain name that appears in common name of your Web server. Do not abbreviate your organization's name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?. This is the name you recorded in the enrollment guide.

Organizational unit: Normally the name of the department or group that will
be using the secure Web server.

Common name: The name of your Web server as it will appear in the server's URL (for example, www.entrust.com). This name must be identical to the fully qualified domain name of the Web server for which you are requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse to establish a secure connection with your site. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Do not use wildcards such as * or ?, and do not use an IP address.

8. MICROSOFT INTERNET INFORMATION SERVER 2.X AND 3.X

8.1 MICROSOFT INTERNET INFORMATION SERVER 2.X AND 3.X : CSR GENERATION

Generating a key pair and CSR with Microsoft Internet Information Server 2.x and 3.x

Entrust strongly recommends that you take the following precautions to ensure that you will be able to install your Entrust.net Web server certificate:

- If you reside in Canada or the United States, install the 128-bit version of Internet Explorer on the computer that hosts your Web server. This software updates some important cryptographic files (in particular &quot;schannel.dll&quot;). It is available from Microsoft at http://microsoft.com/windows/ie/download/128bit/intro.htm.
- Do not use commas in any of the fields you fill in when creating the CSR. Commas are interpreted as the end of the field and will cause an invalid CSR to be generated.
- Do not use any of the following characters in the Web server Distinguished Name: ! @ # $ % ^ * ( ) ~ ? > < & / \
- When you generate the CSR, make sure you are logged in as an Administrator to the computer that hosts your Web server.

To generate a key pair and CSR in Internet Information Server 2.x and 3.x, follow these steps:

1. Run the Internet Service Manager (click Start > Programs > Microsoft Internet Server > Internet Service Manager).

2. Click the Key Manager icon in the Internet Service Manager toolbar.

3. Click on WWW to create a key pair for the World Wide Web server.

4. Click Key > Create New Key.

5. In the Create New Key and Certificate Request dialog box fill in the requested information, keeping the following example in mind:

“O”	Organization	= Entrust Technologies
“OU”	Organizational Unit	= Entrust.net
“CN”	Common Name	= www.entrust.net (this is the URL of your website)
“C”	Country / Region	= CA
“St”	State / Province	= Ontario
“L”	Locality	= Ottawa

Note:

- Do not use the following characters in any of the fields in the Create New Key wizard: > < ! @ # $ % ^ * ( ) ~ ? / \.
- Make sure that the password you enter contains fewer than 8 characters. It is very important that you remember this password. If you forget it you will not be able to use your Entrust.net Web server certificate. If you write the password down, please be sure to store it in a secure location.
- It is recommended that you choose a 1024-bit key if that option is available.

For more detailed information on this please see Creating Your Distinguished Name.

6. Click the OK button when you have finished entering the required information.

7. When prompted, retype the password you typed in the form, and click the OK button. An icon appears as the key is being created. When the key has been created, the New Key Information dialog box appears.

8. Click the OK button.

9. To save the new key, click Servers > Commit Changes Now.

10. When asked if you want to commit all changes now, click Yes. Your key will appear in the Key Manager window. The key is generated on your local computer by default.

11. Please be sure to back up your private key. The private key and password are very sensitive. Be sure to store the key file in a secure location. If you write down the password please store it in a secure location as well. Someone with access to your private key and password could decrypt the SSL-protected data sent and received by your Web server.

12. Open the file that contains your CSR in a text editor. You specified the name of this file in the Create New Key Wizard. (If you chose the default it is called “New Key.req”) The CSR is the section of the file that looks like the example below. Please be sure to back up this file.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIISDOIUlkmlsRRlkSllskjauASKJlalOSISLKjwBgNV
BAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwtPcHBvcnR1bml0aTEYMBYGA1UE
CxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cu
Zm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEBAQUAAAkl
mLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6pDvAjuy
C+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diuu
PlHDAgEDoAAwDQYJKoZIhvcNAQEEBQADQQBf8LSLKknl
sklSSLlworrr334ZmXD1AvUjuDPCWzFupReiq7UR8Z0w
iJUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END NEW CERTIFICATE REQUEST-----
```

13. Select the entire contents of this file (including the “-----BEGIN NEW CERTIFICATE REQUEST-----“ and “-----END NEW CERTIFICATE REQUEST-----“ lines).

14. Copy this information to the clipboard. You will use this information in the Entrust.net online registration process.

15. Close your text editor.

    To use the CSR to obtain your Enrust.net certificate(s), go to http://www.entrust.net

If you are having difficulty finding what you are looking for, please e-mail us.

Creating Your Distinguished Name

Country code: The two-letter ISO abbreviation for your country (for example, US for the United States).

State or Province: The name of the state or province in which your organization has its head office. Please enter the full name of the state or province. Do not abbreviate.

Locality: Usually the name of the city in which your organization has its head office.

Organization: The name under which your organization is registered. This organization must own the domain name that appears in common name of your Web server. Do not abbreviate your organization's name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?. This is the name you recorded in the enrollment guide.

Organizational unit: Normally the name of the department or group that will be using the secure Web server.

Common name: The name of your Web server as it will appear in the server's URL (for example, www.entrust.com). This name must be identical to the fully qualified domain name of the Web server for which you are requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse to establish a secure connection with your site. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Do not use wildcards such as * or ?, and do not use an IP address.

9. C2NET STRONGHOLD

9.1 C2NET STRONGHOLD : CSR GENERATION

Generating a key pair and CSR with C2Net Stronghold

Entrust strongly recommends that you take the following precautions to ensure that you are able to install your Entrust.net Web server certificate:

- Do not use commas in any of the fields you fill in when creating the CSR. Commas are interpreted as the end of the field and will cause an invalid CSR to be generated.
- Do not use any of the following characters in the Web server Distinguished Name: ! @ # $ % ^ * ( ) ~ ? > < & / \
- When you generate the CSR, make sure you are logged in as an Administrator to the computer that hosts your Web server.

To generate a key and CSR with your Stronghold Web server, follow these steps:

1. On the command line enter genkey <server_name>, where <server_name> is the name of your Web server. The name of the files (including the full path) in which the key and certificate will be stored is displayed. If you are requesting a new certificate using an existing private key, enter genreq <server_name>.

2. When prompted, enter the size of key (in bits) you would like to generate. It is recommended that you use a 1024-bit key if that option is available. Once you make your selection Stronghold will generate random data.

3. When prompted, enter random key strokes as instructed. The random data you generate is used in creating your key pair.

4. Once you have generated the random data, enter “y” to have the key pair generated.

5. Enter O when asked "Would you like to send a certificate request to a CA?". You will be prompted to enter the information that will be used in the distinguished name (DN) for your server. Enter the necessary information keeping the following example in mind:

“O”	Organization	= Entrust Technologies
“OU”	Organizational Unit	= Entrust.net
“CN”	Common Name	= www.entrust.net (this is the URL of your website)
“C”	Country / Region	= CA
“St”	State / Province	= Ontario
“L”	Locality	= Ottawa

For more detailed information on this please see Creating Your Distinguished Name.

6. When you have finished entering the appropriate data, your CSR will be saved to the file displayed when you ran genkey. Please be sure to back up this file. The CSR is the section of the file that looks like this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIISDOIUlkmlsRRlkSllskjauASKJlalOSISLKjwBgNVBAg
TDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR
QwEgYDVQQKEwtPcHBvcnR1bml0aTEYMBYGA1UECxMPT25sa
W5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cuZm9yd2FyZC5j
by56YTBaMA0GCSqGSIb3DQEBAQUAAAklmLKSuljSOIjsfBW
u5WLHD/G4BJ+PobiC9d7S6pDvAjuyC+dPAnL0d91tXdm2j1
90D1kgDoSp5ZyGSgwJh2V7diuuPlHDAgEDoAAwDQYJKoZIh
vcNAQEEBQADQQBf8LSLKknlsklSSLlworrr334ZmXD1AvUj
uDPCWzFupReiq7UR8Z0wiJUUsllkfq/IuuIlz6oCq6htdH7
/tvKhh
-----END NEW CERTIFICATE REQUEST-----
```

7. Please be sure to back up your key file. If you lose your key file or it becomes corrupted you will not be able to use your Entrust.net Web server certificate. Please store the backup file in a secure location. Someone with access to your private key could decrypt the SSL-protected data sent and received by your Web server.

8. Open the request file in a text editor and copy the CSR to the clipboard (including the "-----BEGIN NEW CERTIFICATE REQUEST----" and "-----END NEW CERTIFICATE REQUEST-----" lines). You will paste this text into the appropriate form on the Entrust.net Web site when asked to supply a CSR.

9. Close your text editor.

   To use the CSR to obtain your Entrust.net certificate(s), go to http://www.entrust.net.

If you are having difficulty finding what you are looking for, please e-mail us.

Creating Your Distinguished Name

Country code: The two-letter ISO abbreviation for your country (for example, US for the United States).

State or Province: The name of the state or province in which your organization has its head office. Please enter the full name of the state or province. Do not abbreviate.

Locality: Usually the name of the city in which your organization has its head office.

Organization: The name under which your organization is registered. This organization must own the domain name that appears in common name of your Web server. Do not abbreviate your organization's name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?. This is the name you recorded in the enrollment guide.

Organizational unit: Normally the name of the department or group that will be using the secure Web server.

Common name: The name of your Web server as it will appear in the server's URL (for example, www.entrust.com). This name must be identical to the fully qualified domain name of the Web server for which you are requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse to establish a secure connection with your site. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Do not use wildcards such as * or ?, and do not use an IP address.

10. BEA WEBLOGIC 4.5.X

10.1 BEA WEBLOGIC 4.5.X :CSR GENERATION

Generating a key pair and CSR with BEA Weblogic 4.5.x

Entrust strongly recommends that you take the following precautions to ensure that you are able to install your Entrust.net Web server certificate:

- Install and set up the Web server as an HTTP server.
- Do not use commas in any of the fields you fill in when creating the CSR. Commas are interpreted as the end of the field and will cause an invalid CSR to be generated.
- Do not use any of the following characters in the Web server Distinguished Name: ! @ # $ % ^ * ( ) ~ ? > < & / \
- When you generate the CSR, make sure you are logged in as an Administrator to the computer that hosts your Web server.

To generate a key pair and CSR in WebLogic 4.5.x:

1. Load the Certificate servlet from your WebLogic Server into a browser. Use an URL that follows the format: http://localhost:port/Certificate

   where:
   - localhost is the name of the computer that hosts your Web server.
   - port is the appropriate port number on your server.
   - Certificate is the name of the servlet you are using to generate your key and CSR.

   Note: The certificate servlet is registered in the weblogic.properties file, and it is protected so that only the system administrator can use it. If you cannot run the servlet, check your weblogic.properties file for the following properties:

```
weblogic.httpd.register.Certificate=utils.certificate
weblogic.allow.execute.weblogic.servlet.Certificate=system
```

2. Log in as the system administrator

3. Follow the online help to generate your public/private key pair and the Certificate Signing Request (CSR). The FULL HOST NAME field is used as the common name (CN) in the CSR. Three files are added to the WebLogic Server's startup directory:
   www_mydomain_com-key.der - This is your private key file.
   www_mydomain_com-request.dem - This is the encrypted CSR file, in a binary format.
   www_mydomain_com-request.pem - This is the CSR file, which you submit to Entrust.net. It is ASCII-encoded so that you can copy it and paste it into the appropriate Web form.

4. Copy the contents of the ASCII-encoded CSR file. For example, copy the contents of www_mydomain_com-request.pem, and paste it into the appropriate form on the Entrust.net Web site. The contents of this file are displayed by your browser after the generation of the CSR.

   To use the CSR to obtain your Entrust.net certificate(s), go to http://www.entrust.net.

Note: If you need more help you can also consult the WebLogic online documentation at: http://www.weblogic.com/docs45/classdocs/API_secure.html.

If you are having difficulty finding what you are looking for, please e-mail us.

11. RAVEN SSL 1.4.1 MODULE FOR APACHE SUPPORT

Enabling Server Auth SSL with Entrust.net

11.1 RAVEN SSL 1.4.1 MODULE FOR APPACHE SUPPORT

This document assumes that the Raven SSL Module has been installed and configured to work with an Apache http server that was compiled to work with the Raven SSL Module. It is assumed that the Apache is configured to listen for SSL requests on port 443 (or another specified port).

Entrust strongly recommends that you take the following precautions to ensure that you are able to install your Entrust.net Web server certificate:

- Do not use commas in any of the fields you fill in when creating the CSR. Commas are interpreted as the end of the field and will cause an invalid CSR to be generated.
- Do not use any of the following characters in the Web server Distinguished Name: ! @ # $ % ^ * ( ) ~ ? > < & / \
- When you generate the CSR, make sure you are logged in as an Administrator to the computer that hosts your Web server.

Generating a Certificate and Key (NOTE: This step is unnecessary if you have previously created a certificate and key):

1. Type ravenctl at the shell prompt to start the RavenCTL Management Interface. If your PATH is set correctly, this will start the interface immediately, otherwise you need to include the full path to Raven's "bin" directory. (e.g. if the ravenctl script is located at /usr/local/raven/bin, type: /usr/local/raven/bin/ravenctl).
2. Select [2] Raven PKI Certificate Manager.
3. Select [1] Generate Certificate and Key from the RavenCTL PKI Management Interface.
4. Follow the on-screen directions to generate a key pair and certificate. Take note of the filenames you choose to hold these items as they will be required later. Keep the following example in mind as you are filling in the information for the distinguished name:

“O”	Organization	= Entrust Technologies
“OU”	Organizational Unit	= Entrust.net
“CN”	Common Name	= www.entrust.net (this is the URL of your website)
“C”	Country / Region	= CA
“St”	State / Province	= Ontario
“L”	Locality	= Ottawa

For more detailed information on the DN please see Creating Your Distinguished Name.

5. A file directory with the specified filename will be generated in the [install-prefix]/raven/module/pki/keys with a .key extension, and in the [install-prefix]/raven/module/pki/certs directory with a .cert extension. The [install-prefix] specifies the path to the raven directory. This is /usr/local using the default Raven installation.

Generating and Submitting the Certificate Signing Request (CSR):

1. From the RavenCTL PKI Management Interface, select [4] Generate Certificate Signing Request.

2. Select the name of the certificate for which you wish to generate a CSR (choose the file created in the above process if appropriate).

3. Follow the on-screen directions to generate the CSR. Take note of the following:

   - Answer “N” to the question: “Is this CSR being sent to Verisign?”.
   - Remember the pass phrase you enter, as it is required to start the SSL enabled WebServer.
   - Entrust.net only accepts CSRs via an online web form. To answer “Send CSR via Email to?”, enter the email address of whomever will make the online request to Entrust.net.

4. Instruct the recipient of the email generated above to paste the enclosed CSR into the appropriate Entrust.net web form. The CSR includes the “-----BEGIN CERTIFICATE REQUEST-----“ and “-----END CERTIFICATE REQUEST-----“ lines, and everything in between.

If you are having difficulty finding what you are looking for, please e-mail us.

Creating Your Distinguished Name

Country code: The two-letter ISO abbreviation for your country (for example, US for the United States).

State or Province: The name of the state or province in which your organization has its head office. Please enter the full name of the state or province. Do not abbreviate.

Locality: Usually the name of the city in which your organization has its head office.

Organization: The name under which your organization is registered. This organization must own the domain name that appears in common name of your Web server. Do not abbreviate your organization's name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?. This is the name you recorded in the enrollment guide.

Organizational unit: Normally the name of the department or group that will be using the secure Web server.

Common name: The name of your Web server as it will appear in the server's URL (for example, www.entrust.com). This name must be identical to the fully qualified domain name of the Web server for which you are requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse to establish a secure connection with your site. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Do not use wildcards such as * or ?, and do not use an IP address.