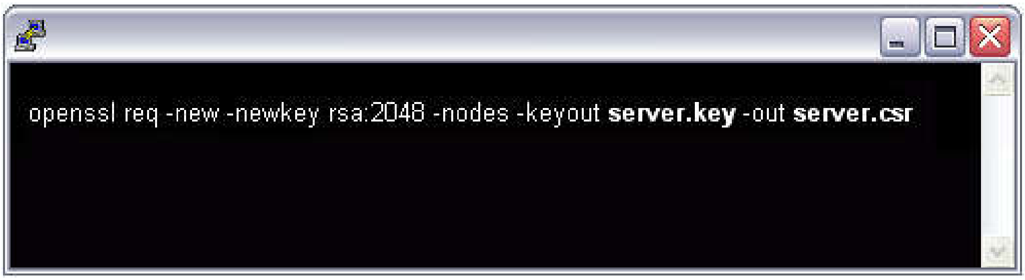
Courier IMAP CSR Creation and Installation

How to generate a CSR for Courier IMAP using OpenSSL

1. Login to your server via your terminal client (ssh). At the prompt, type:



```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
```

openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
where **server** is the name of your server.

2. This begins the process of generating two files: the **Private-Key** file for the decryption of your SSL Certificate, and a certificate signing request (**CSR**) file (used to apply for your SSL Certificate) with apache openssl.
When you are prompted for the **Common Name** (domain name), enter the fully qualified domain name for the site you are securing. If you are generating an Apache CSR for a Wildcard SSL Certificate your common name should start with an asterisk (such as *.yourdomain.com).
You will then be prompted for your organizational information, beginning with geographic information. There may be default information set already.

   This will then create your openssl .csr file.

3. Open the CSR file with a text editor and save it to text file and submit to us for process.

4. Save (backup) the generated .key file as it will be required later for Certificate installation.

Installing your Courier IMAP SSL Digital Certificate

1. **Create a combined .pem certificate file:**
Open a text editor and paste the contents of the primary certificate and the private key one after another in the following order:

   1. The Primary Certificate (**your_domain_name.crt**)
   2. The Private Key (**your_domain_name.key**)

   Include the 'BEGIN' and 'END' tags on each. The result should look like this:

   -----BEGIN CERTIFICATE-----
   (Your Primary SSL certificate: your_domain_name.crt)
   -----END CERTIFICATE-----
   -----BEGIN RSA PRIVATE KEY-----
   (Your Private Key: your_domain_name.key)
   -----END RSA PRIVATE KEY-----
   Save the combined file as **pack.pem**

2. **Save the Intermediate certificate:**
Copy the intermediate certificate into a text editor and save it as a new file named IntermediateCA.txt.

3. **Securing your Courier IMAP:**
Locate and open imapd-ssl file (typically found in /usr/lib/courier-imap/etc/). Add the following directives and file locations:

- TLS_CERTFILE=/some/path/pack.pem
- TLS_TRUSTCERTS=/some/path/IntermediateCA.txt

Please verify that line below line is allowing SSL3

- TLS_PROTOCOL=SSL3

4. **Securing your POP3:**
   Locate and open pop3d-ssl file (typically found in /usr/lib/courier-imap/etc/). Add the following directives and file locations:

   - TLS_CERTFILE=/some/path/pack.pem
   - TLS_TRUSTCERTS=/some/path/IntermediateCA.txt

5. **File permissions:**
   Make sure that the file permissions are set so that pack.pem is readable by root only.

6. **7) Restart the Courier IMAP server.**