How do I create a SSL Certificate using Apache?

(Portions of this document have been taken from http://httpd.apache.org/docs/2.2/ssl/)

Here is a step-by-step description:

1. Make sure OpenSSL is installed and in your PATH.
2. Create a RSA private key for your Apache server (will be PEM formatted).
   ```
   $ openssl genrsa -out server.key 2048
   ```
3. Make sure the server.key is only readable by root.
   ```
   $ chmod 400 server.key
   ```
4. Create a Certificate Signing Request (CSR) with the server RSA private key (output will be PEM formatted). Make sure you enter the FQDN ("Fully Qualified Domain Name") of the server when OpenSSL prompts you for the "CommonName", i.e. when you generate a CSR for a website which will be later accessed via https://www.myserver.lsu.edu/, enter "www.myserver.lsu.edu" here.
   ```
   $ openssl req -new -key server.key -out server.csr
   ```
5. Verify the details of this CSR by using before submitting it to be signed.
   ```
   $ openssl req -noout -text -in server.csr
   ```
6. You now have to send this Certificate Signing Request (CSR) to LSU's Certifying Authority (CA) to be signed. Once the CSR has been signed, you will have a real Certificate, which can be used by Apache.
   a. Go to www.lsu.edu/pki and click the “Request a new certificate by uploading a CMC or PKCS #10 request file” link to submit your certificate request.
   b. Open the CSR file with a text editor and paste the contents text of it there. Choose the correct template (LSU Public or Internal) and submit.
   c. Wait for a confirmation email from pki@lsu.edu. Reply with YES if correct. Once your CSR has been signed, you will receive a certificate issued email.
   d. Return to www.lsu.edu/pki and click on the “Check on the status of a request you've already made” link.
   e. Download the certificate in Base 64 and copy the contents to a file named server.crt on the server.
7. Download LSU Issuing CA 1's certificate in Base 64 format from www.lsu.edu/pki. Rename the file to ca.crt and place it in the same location as your server.crt.
8. You should now have three files: server.key, ca.crt, and server.crt. These can be used as follows in your httpd.conf file:
   ```
   SSLCertificateFile    /path/to/this/server.crt
   SSLCertificateKeyFile /path/to/this/server.key
   SSLCertificateChainFile /path/to/this/ca.crt
   ```
9. Save the server.csr file because it can be used again when this one expires.

Please go to http://httpd.apache.org/docs/2.2/ssl/ for further details.