Below is the step-by-step process of how to request, obtain, install and configure a 2048-bit SSL certificate from InCommon via UCSF ITS on an Apache webserver running Red Hat Enterprise Linux 5.7. This tutorial should also work for equivalent CentOS and Fedora releases. This information can be found in the Red Hat Enterprise Linux 5 Deployment Guide: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Deployment_Guide/s2-secureserver-generatingkey.html. The crypto-utils package must be installed to create server keys and CSR requests.

I ran the following commands as root on a RHEL 5.7 server named *server.ucsf.edu*; please substitute your server and organization information where applicable.

1. Shell> genkey *server.ucsf.edu*
    a. In the Key Pair Generation window press the Tab key until Next is selected and then press the Enter key.
    b. In the Choose Key Size window, arrow down until 2048-bit is selected, press the Tab key until Next is selected and then press the Enter key. I opted for a 2048-bit key, not the default 1024-bit setting, note the performance comments in the genkey window. The location of the server key is /etc/pki/tls/private/*server.ucsf.edu.key*.
    c. In the Generate CSR window press the Enter key.
    d. In the Choose Certificate Authority window use the arrow key to select Other. Press the Tab key until Next is selected and then press the Enter key.
    e. In the Enter Details For Your Certificate window use the Tab key to navigate the fields and populate them with the appropriate information. Press the Tab key until Next is selected and then press the Enter key.
    f. Your shell output will display "A copy of this CSR has been saved in the file /etc/pki/tls/certs/*server.ucsf.edu.0.csr*". Press the Enter key to continue.
    g. In the Protecting Your Private Key window I chose not to encrypt this key because an encrypted key can prevent Apache from starting correctly. Please make sure to take all appropriate measures to protect your SSL key regardless if it is encrypted or not. Press the Tab key until Next is selected and then press the Enter key.
2. Using a web browser, make you way to http://help.ucsf.edu and click on the Submit a ticket for ITS or School of Nursing IT link. Login and click on the new Request button. Submit your request per https://wiki.library.ucsf.edu/display/ITSSecurityPolicy/InCommon+-+How+to+Request+a+Certificate
    a. In the Summary field type in InCommon SSL
    b. In the Notes field type in the following information that matches your server:
        i. Type of certificate: SSL, (choose of the following type: Single domain certificate, Multi-Domain, Unified Communications Certificate or Wildcard) see https://wiki.library.ucsf.edu/display/ITSSecurityPolicy/Overview+of+UCSF%27s+SSL+Certificate+Service for more information.
        ii. Email: *your_email@ucsf.edu*
        iii. Web Server Software: Red Hat Enterprise Linux 5.7, Apache 2.2.3
        iv. Note: The requested SSL certificate will be used to secure logins/passwords
        v. Name(s): *server.ucsf.edu*
        vi. Server IP: 128.218.xxx.xxx
        vii. Certificate Signing Request (CSR):
3. Shell> more /etc/pki/tls/certs/*server.ucsf.edu.0.csr*
4. Copy/paste the output of step 3 below the Certificate Signing Request (CSR) line in step 2vii.
5. Click on the Save button.
6. An email will be sent confirming that ITS has received your SSL request.
7. Another email titled "Enrollment Successful - Your SSL certificate for *server.ucsf.edu* is ready" will be sent. Download the files from the following links:
    a. as X509, Base64 encoded.
    b. as X509 Certificate only, Base64 encoded
    c. as X509 Intermediates/root only, Base64 encoded
8. Move the downloaded files to /etc/pki/tls/certs
9. Edit /etc/httpd/conf.d/ssl.conf

a. Shell> vi /etc/httpd/conf.d/ssl.conf
b. Edit the following three lines to read:
    i. SSLCertificateFile /etc/pki/tls/certs/*server_ucsf_edu_cert.cer*
    ii. SSLCertificateKeyFile /etc/pki/tls/private/*server.ucsf.edu.key*
    iii. SSLCertificateChainFile /etc/pki/tls/certs/*server_ucsf_edu.cer*

10. Re-start Apache
    Shell> /etc/init.d/httpd restart
11. Test the installed SSL certificate
    Point a browser such Apple Safari, Google Chrome, Microsoft Internet Explorer or Mozilla Firefox at *https://server.ucsf.edu/*. Are any certificate errors reported?
12. If the SSL certificate is accepted without error then you correctly installed and configured the web server SSL certificate correctly.

Andrew Philipoff
aphilipoff@medicine.ucsf.edu
Information Systems
Department of Medicine, UCSF
Phone 415-476-1344