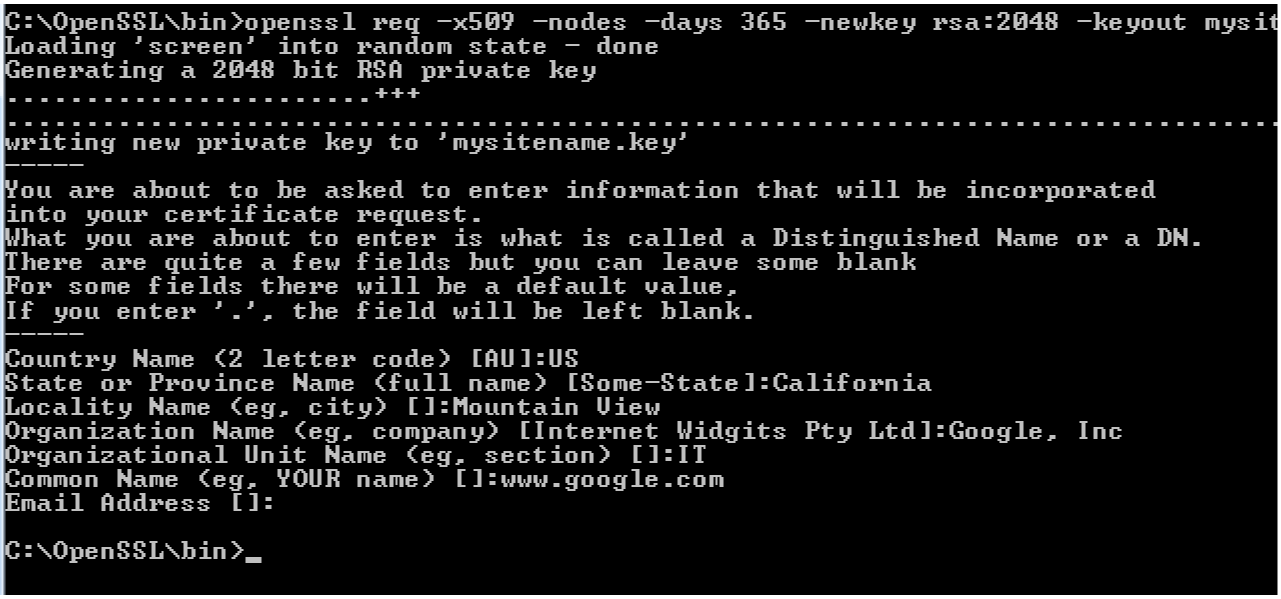
Generate Your Apache Self Signed Certificate

Great! So now you know when to use an **Apache self signed certificate** and when not to. Now, let's create one: First, we need to make sure OpenSSL is installed. If you are installing the self signed certificates on Windows, grab the Windows version of OpenSSL (If you get an error when you run the installer, you may need to download the Visual C++ 2008 Redistributables listed on that page first). If you are on another type of server, try running "openssl" on the command line to see if OpenSSL is already installed. If it is not, you will need to download a package or compile it from its source.

Once you have OpenSSL installed, just run this one command to create an Apache self signed certificate:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -
keyout mysitename.key -out mysitename.crt
```



```
C:\OpenSSL\bin>openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout mysit
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.......................+++
................................................................................
writing new private key to 'mysitename.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:Mountain View
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Google, Inc
Organizational Unit Name (eg, section) []:IT
Common Name (eg, YOUR name) []:www.google.com
Email Address []:

C:\OpenSSL\bin>_
```

You will be prompted to enter your organizational information and a common name. The common name should be the fully qualified domain name for the site you are securing (www.mydomain.com). You can leave the email address, challenge password, and optional company name blank. When the command is finished running, it will create two files: a mysitename.key file and a mysitename.crt self signed certificate file valid for 365 days.

Install Your Self Signed Certificate

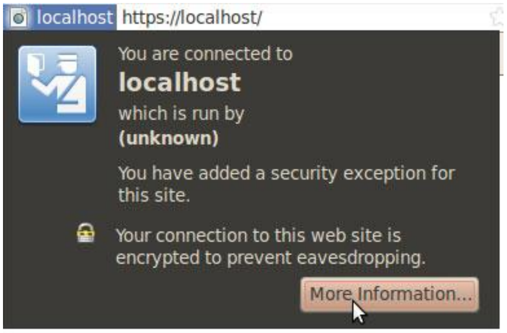
Now, you just need to configure your Apache virtual host to use the SSL certificate. If you only have one Apache virtual host to secure and you have an ssl.conf file being loaded, you can just edit that file. Otherwise, you will need to make a copy of the existing non-secure virtual host, paste it below, and change the port from port 80 to 443.

1. Open your Apache configuration file in a text editor. Depending on your operating system and Apache version, it will be located in different places but you will usually find it at /etc/httpd/httpd.conf. On a Windows machine, you will usually find it at C:\Program Files\Apache\Apache2\conf\httpd.conf
2. In most cases, you will find the <VirtualHost> blocks in a separate file in a directory like /etc/httpd/vhosts.d/ or /etc/httpd/sites/. Add the lines in bold below.
   ```
   <VirtualHost 192.168.0.1:443>
   DocumentRoot /var/www/website
   ServerName www.domain.com
   SSLEngine on
   SSLCertificateFile /etc/ssl/crt/primary.crt
   SSLCertificateKeyFile /etc/ssl/crt/private.key
   SSLCertificateChainFile /etc/ssl/crt/intermediate.crt
   </VirtualHost>
   ```
3. Change the names of the files and paths to match your certificate files. Save the changes and exit the text editor.
4. Restart your Apache web server using one of the following commands:
   ```
   /usr/local/apache/bin/apachectl startssl
   /usr/local/apache/bin/apachectl restart
   ```

Learn more about installing a certificate in Apache.

Check the Apache Self Signed Certificate Installation

If the Apache site is public, you can use our SSL Checker to verify that it is installed correctly (ignoring the warning that it is not trusted because it is self signed). Otherwise, just go to the website in your web browser using https in the address bar (https://www.mysitename.com) and verify that the certificate is being given out by the server by clicking the certificate icon (after clicking through the warnings).



You are connected to
localhost
which is run by
(unknown)

You have added a security exception for this site.

Your connection to this web site is encrypted to prevent eavesdropping.

http://www.sslshopper.com/ssl-checker.html