How To Generate a Certificate Signing Request (CSR) and Key in Apache® + MOD SSL

To generate a certificate signing request (CSR) and key in Apache + MOD SSL, please follow these step-by-step instructions:

1. Install “OpenSSL”, if not found on server, and put in “PATH”.

2. Create a RSA key for your Apache server by: cd to /apacheserverroot/conf/ssl.key directory. (ssl key is the default key directory. If you have a different setting, cd to your server’s private key directory.)

3. Type the following commands to generate a key pair:
   $openssl genrsa -des3 -out server.key 1024

4. Enter and verify the “PEM passphrase”. The passphrase will be used to install the server certificate.  
   *Warning: If you lose the passphrase, you must purchase another certificate.*

5. Type the following commands to create a CSR with the server RSA private key:
   $openssl req -new -key server.key -out server.csr
   (The output will be PEM formatted.)

6. When creating a CSR, you must follow these conventions.
   • Enter the “Distinguished Name Field” information.
   • **Note:** The following characters cannot be accepted: < > - ! @ # % ^ * / \ ( ) ?

<table>
<thead>
<tr>
<th>Distinguished Name Field</th>
<th>Explanation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Country Name</strong></td>
<td>The two-letter ISO abbreviation for your country.</td>
<td>US = United States</td>
</tr>
<tr>
<td><strong>State or Province Name</strong></td>
<td>The state or province where your organization is legally located. Do not abbreviate the state or province name.</td>
<td>Utah</td>
</tr>
<tr>
<td><strong>City or Locality</strong></td>
<td>The city where your organization is legally located.</td>
<td>Salt Lake City</td>
</tr>
<tr>
<td><strong>Company (Organization) Name</strong></td>
<td>The exact legal name of your organization. Do not abbreviate your organization name.</td>
<td>IdenTrust Inc.</td>
</tr>
<tr>
<td><strong>Department Name</strong></td>
<td>Section of the organization.</td>
<td>Marketing</td>
</tr>
<tr>
<td><strong>Server Hostname</strong></td>
<td>The fully qualified domain name for your web server. This must be an exact match.</td>
<td>If you intend to secure the URL <a href="https://www.identrust.com/">https://www.identrust.com/</a>, then your CSR's Server Hostname must be <a href="http://www.identrust.com">www.identrust.com</a></td>
</tr>
<tr>
<td><strong>Server Administrator’s Email Address</strong></td>
<td>Your email address</td>
<td><a href="mailto:abc@identrust.com">abc@identrust.com</a></td>
</tr>
</tbody>
</table>
7. Do not enter extra attributes at the prompt. 
   *Warning*: Leave the challenge password blank.

8. View the details of the CSR via the command:
   ```
   $ openssl req -noout -text -in server.csr
   ```

9. Send the **entire certificate request** to IdenTrust, including ----BEGIN CERTIFICATE REQUEST---- and ----END CERTIFICATE REQUEST----

**Key Pair Backup**

1. Backup this “server.key” file and remember the passphrase you had to enter at a secure location.

2. View the details of the RSA private key via the command:
   ```
   $ openssl rsa -noout -text -in server.key
   ```