CSR 文件制作指南（Apache）

在申请数字证书之前，必须先生成证书私钥和证书请求文件(CSR,Cerificate Signing Request)，CSR 是您的公钥证书原始文件，包含了您的服务器信息和您的单位信息，需要提交给 CA 认证中心。在生成 CSR 文件时会同时生成私钥文件，请妥善保管和备份您的私钥。

生成 CSR 文件时，一般需要输入以下信息(中文需要 UTF8 编码)：

Organization Name(O)：申请单位名称法定名称，可以是中文或英文

Organization Unit(OU)：申请单位的所在部门，可以是中文或英文

Country Code(C)：申请单位所属国家，只能是两个字母的国家码，如中国只能是：CN

State or Province(S)：申请单位所在省名或州名，可以是中文或英文

Locality(L)：申请单位所在城市名，可以是中文或英文

Common Name(CN)：申请 SSL 证书的具体网站域名

使用 OpenSSL 工具生成 CSR 文件:

openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout myprivate.key -out mydomain.csr

- -new 指定生成一个新的 CSR
- -nodes 指定私钥文件不被加密
- -sha256 指定摘要算法
- -keyout 生成私钥
- -newkey rsa:2048 指定私钥类型和长度
- -out 最终生成 CSR 文件 mydomain.csr

需要输入的信息说明如下：

字段	说明	示例
Country Name	ISO 国家代码（两位字符）	CN
State or Province Name	所在省份	Beijing
Locality Name	所在城市	Beijing
Organization Name	公司名称	Cernet, Inc.
Organizational Unit Name	部门名称	IT Dept.
Common Name	申请证书的域名	www.example.com

Email Address	不需要输入	
A challenge password	不需要输入	

完成命令提示的输入后，会在当前目录下生成 myprivate.key（私钥文件）和 mydomain.csr（CSR，证书请求文件）两个文件。

在使用 openssl 工具生成中文证书时需要注意中文编码格式，使用 utf8 编码，同时需要编译 openssl 工具时指定支持 utf8 格式。

如果对中文有需求，推荐您使用 keytool 工具。

注意事项：

1. CSR 的密钥长度有严格要求，要求是 2048 位，密钥类型必须为 RSA。
2. 如果申请证书是多域名或者通配子域名，在“Common Name”字段只需要输入一个域名即可(通配子域名可以输入“*.example.com”)。