CSR 文件制作指南（Tomcat）

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)：

Common Name(CN)：申请 SSL 证书的具体网站域名

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

使用 keytool 工具生成 CSR 文件:

1. 先生成证书文件 keystore，证书文件中包含密钥

keytool -genkey -alias mycert -keyalg RSA -keysize 2048 -keystore ./mydomain.jks

keyalg 是密钥类型,必须是 RSA, keysize 是密钥长度为 2048, alias 是证书别名可自定义, keystore 是证书文件保存路径。

首先输入证书保护密码，然后依次输入：

问题	说明	示例
What is your first and last name?	申请证书的域名	www.example.com
What is the name of your organizational unit?	部门名称	IT Dept.
What is the name of your organization?	公司名称	Cernet, Inc.
What is the name of your City or Locality?	所在城市	Beijing
What is the name of your State or Province?	所在省份	Beijing
What is the two-letter country code for this unit?	ISO 国家代码（两位字符）	CN

输入完成后，确认输入内容是否正确：[no]: Y (输入 Y)

而后提示输入密钥密码,可以与证书密码一致,如果一致则直接按回车。

2. 通过证书文件生成证书请求:

keytool -certreq -sigalg SHA256withRSA -alias mycert -keystore ./mydomain.jks -file ./mydomain.csr

- -sigalg 是摘要算法，使用 SHA256withRSA
- -alias 是别名，必须与 2.1 步中的别名一致
- -keystore 是证书文件
- -file 是证书请求文件(CSR)

而后提示输入证书密码即可以生成 mydomain.csr。

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“What is your first and last 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”)。