**https://blog.csdn.net/liitdar/article/details/80755073**

**2.1 生成server的秘钥对**

openssl genrsa -out server-key.pem 2048

**2.2 生成server的身份证申请（CSR）**

openssl req -nodes -new -key server-key.pem -subj "//CN=localhost" -out server-csr.pem

在Windows平台使用Git执行bash脚本生成SSL证书时，以下命令会产生错误Subject does not start with '/'：

openssl req -new -x509 -days 365 -key ca\_private.key -out ca\_cert.crt -subj "/C=CN/ST=BJ/L=BJ/O=abc/OU=abc/CN=abc/emailAddress=abc@abc.com"

该错误是由Git for Windows中MinGW/MSYS模块的路径转换机制引起的。

解决方案：将-subj参数中第一个“/”改为“//”，其余“/”改为“\”，如下：

-subj "//C=CN\ST=BJ\L=BJ\O=abc\OU=abc\CN=abc\emailAddress=abc@abc.com"

---------------------

**2.3 生成CA的身份证（CRT）**

**2.3.1 生成CA的秘钥对**

使用 OpenSSL 的 genrsa 命令，生成 CA 的秘钥对：

openssl genrsa -out ca-key.pem 2048

2.3.2 生成CA的身份证使用 OpenSSL 的 x509 命令，生成 CA 的自签名身份证：

openssl req -x509 -new -nodes -key ca-key.pem -days 10000 -out ca-crt.pem -subj "//CN=test-ca"

上面的命令生成了 CA 的自签署的身份证文件 ca-crt.pem。其中，ca-key.pem 是前面创建的 CA 的私钥（其实是秘钥对）。需要注意的是：因为是自签名的 CA 身份证，所以上面步骤中没有生成身份证申请文件（CSR）的过程，直接输出了 CA 的身份证。另外，在本例中 CA 的域名是“test-ca”。