使用openssl生成所需秘钥文件

生成环境是在mac系统下，使用openssl进行生成，首先打开终端，按下面这些步骤依次来做：

1. 生成模长为1024bit的私钥文件private\_key.pem

openssl genrsa -out private\_key.pem 2048

2. 生成证书请求文件rsaCertReq.csr

openssl req -new -key private\_key.pem -out rsa\_cer\_req.csr

注意：这一步会提示输入国家、省份、mail等信息，可以根据实际情况填写，或者全部不用填写，直接全部敲回车.

3. 生成证书rsaCert.crt，并设置有效时间为10年

openssl x509 -req -days 3650 -in rsa\_cer\_req.csr -signkey private\_key.pem -out rsa\_cert.crt

4. 生成供iOS使用的公钥文件public\_key.der

openssl x509 -outform der -in rsa\_cert.crt -out public\_key.der

5. 生成供iOS使用的私钥文件private\_key.p12

openssl pkcs12 -export -out private\_key.p12 -inkey private\_key.pem -in rsa\_cert.crt

注意：这一步会提示给私钥文件设置密码，直接输入想要设置密码即可，然后敲回车，然后再验证刚才设置的密码，再次输入密码，然后敲回车，完毕！

在解密时，private\_key.p12文件需要和这里设置的密码配合使用，因此需要牢记此密码.

6. 生成供Java使用的公钥public\_key.pem

openssl rsa -in private\_key.pem -out public\_key.pem -pubout

7. 生成供Java使用的私钥pkcs8\_private\_key.pem

openssl pkcs8 -topk8 -in rsa\_private\_key.pem -out pkcs8\_private\_key.pem -nocrypt

全部执行成功后，会生成如下文件，其中public\_key.der和private\_key.p12就是iOS需要用到的文件，如下：

Java使用

pkcs8\_private\_key.pem

public\_ley.pem

iOS使用

public\_key.der

private\_key.p12