如何生成 RSA 密钥

通过 openssl 工具生成 RSA 的公钥和私钥 (openssl 工具可在互联网中下载到,

也可以 点此 下载无线接口包，里面包含此工具)

打开 openssl 文件夹下的 bin 文件夹，执行 openssl.exe 文件。

1）生成 RSA 私钥

输入“ 生成命令 .txt ”文件中：“ genrsa -out rsa_private_key.pem 1024 ”,

并回车得到生成成功的结果，如下图：

此时，我们可以在 bin 文件夹中看到一个文件名为 rsa_private_key.pem 的文

件，用记事本方式打开它，可以看到 -----BEGIN RSA PRIVATE KEY----- 开头,

-----END RSA PRIVATE KEY----- 结尾的没有换行的字符串，这个就是原始的

私钥。

2）把 RSA 私钥转换成 PKCS8 格式

输入命令： pkcs8 -topk8 -inform PEM -in rsa_private_key.pem -outform

PEM -nocrypt ，并回车 当前界面中会直接显示出生成结果 ，这个结果就是

PKCS8 格式的私钥，如下图：

右键点击 openssl 窗口上边边缘，选择编辑→标记，选中要复制的文字（如上图），

此时继续右键点击 openssl 窗口上边边缘，选择编辑→复制，

把复制的内容粘土进一个新的记事本中，可随便命名，只要知道这个是 PKCS8 格式的私钥即可。

3）生成 RSA 公钥

输入命令 rsa -in rsa_private_key.pem -pubout -out rsa_public_key.pem ，

并回车，得到生成成功的结果，如下图：

此时，我们可以在 bin 文件夹中看到一个文件名为 rsa_public_key.pem 的文件，

用记事本方式打开它，可以看到 -----BEGIN PUBLIC KEY----- 开头， -----END PUBLIC KEY----- 结尾的没有换行的字符串，这个就是公钥。

详情见开放平台对于 密钥生成说明

注意 ：请妥善保管好生成的公私钥！

附：点此查看 如何上传公钥