

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：



```
D:\接口\openssl\openssl\bin\openssl.exe
OpenSSL> genrsa -out rsa_private_key.pem 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
OpenSSL> _
```

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：

```

OpenSSL> pkcs8 -topk8 -inform PEM -in rsa_private_key.pem -outform PEM -nocrypt
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBALys+oYaxqv4FYju
8C1poM6qmHLjWPnXzqEJT0NxyFXgdaK/Qe9DcpcASod9mIAdlLixJEyYNlWeonAJ
VYV8pQ+pIVGwI9n0iaT71ldWQzcMN3Dvi/+zpgw3Hxx07HJtEi1R84pvILv1yceC
ZCqqQ40/4SemsG00oTiTyD3SM2ZvAgMBAAECgYBLTeeX6ywNC7Icu7H1j11+45yB
jri+0CJLKFoYwfuA21xYnxeEE9ny54zX04uA502oafDhGYfmWLDhIv idrpP6oalu
URb/gbU5Bdcn98gGGUgm6lpK+G5N/eauXDjP0ZjxXb114Y/Hn/oUFUM90qcuJFSU
+Ug4JgJ4Mmtdr35gYQJBAPbhx030xPcep8/dL5QQMc7ddoOrfxXewKcpDmZJi2ey
381X+DhuphQ5gSUBbbunRiDCEcuXFY+R7xrgnP+uiWcCQQDDpN8DfqRR1+cUhc0z
/TbnSPJkMT/IQoFeFOE7wMBcDIBoQePEDsr56mtc/trIUh/L6evP9bkjLzWJs/kb
/i25AkEAtOOf1k/4NUEiipdYjzuRtu8emKI2ZPKytnGx1YjUUKpyrdo1FXMnsJf6
k9JUD3/QZnNSuJJPTD506AfZyWS6TQJANDeF2Hxd1GatnaRFG02y0mvs6U30c7R5
zd6JLdyaE7sNC6Q2fppjne9qFYq975CKegykyTacqhnX4I8KEwHYQJAby60iHMA
YfSUpu//f5LMMRFK2sUif9aqlYbepJcAzJ6zbiSG5E+0xg/MjEj/Blg9rNsQDG4R
ECGJG2nPR7208g==
-----END PRIVATE KEY-----

```

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：

```

OpenSSL> rsa -in rsa_private_key.pem -pubout -out rsa_public_key.pem
writing RSA key
OpenSSL>

```

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