**OpenSSL工具安装和生成证书操作手册**

## openssl工具安装和生成证书

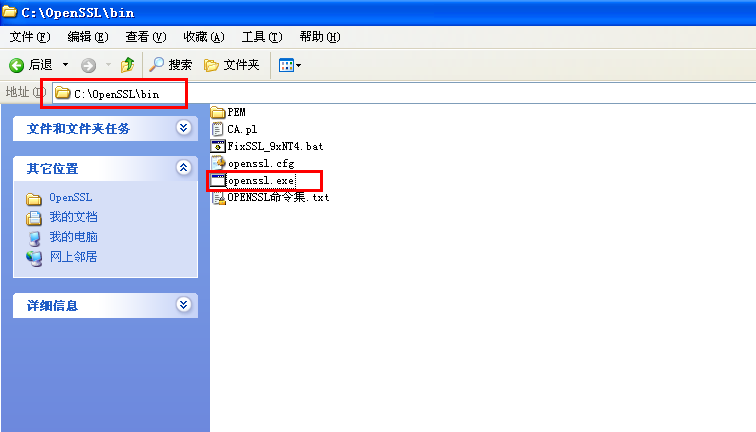
### 证书生成软件安装

点击快钱开发包里面提供的Win32OpenSSL\_Light-0\_9\_8k.exe安装软件，一直点next即可完成软件的安装，该软件用于生成证书。软件只要安装在商户技术本地电脑即可。

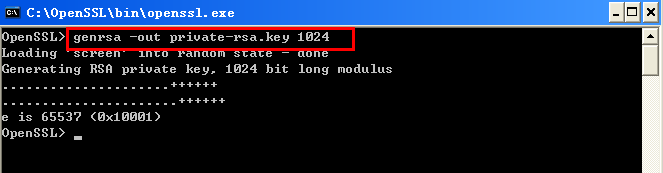
PS：win 7 操作系统，安装openssl工具需要右键以管理员身份安装运行

### 证书生成

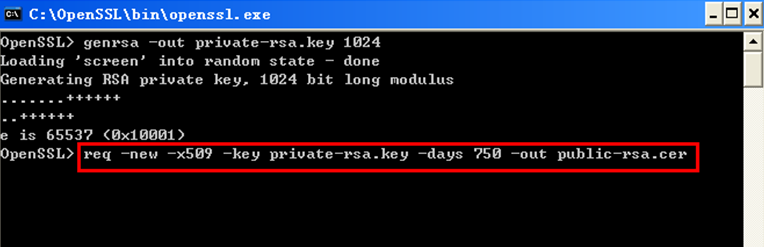
1、如下图，打开openssL.exe

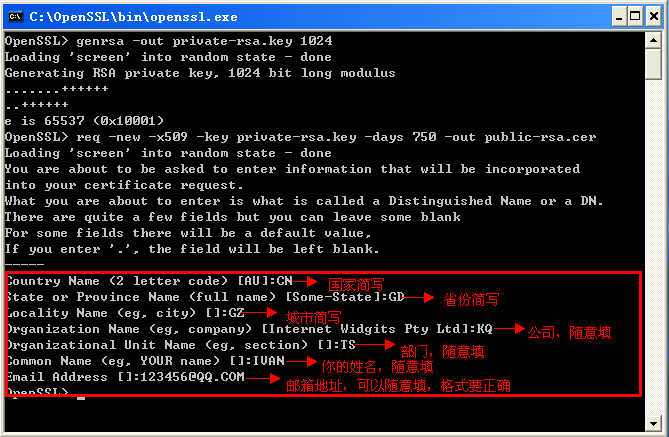


2、输入genrsa -out private-rsa.key 1024，按enter即可。

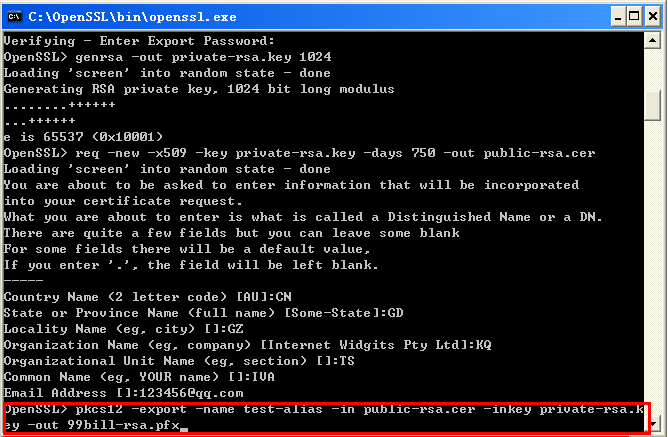


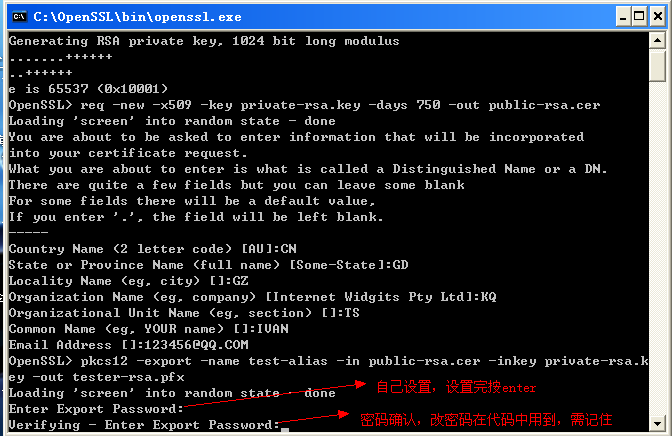
3、输入req -new -x509 -key private-rsa.key -days 750 -out public-rsa.cer，按enter，然后按照第二个图片提示进行填写。



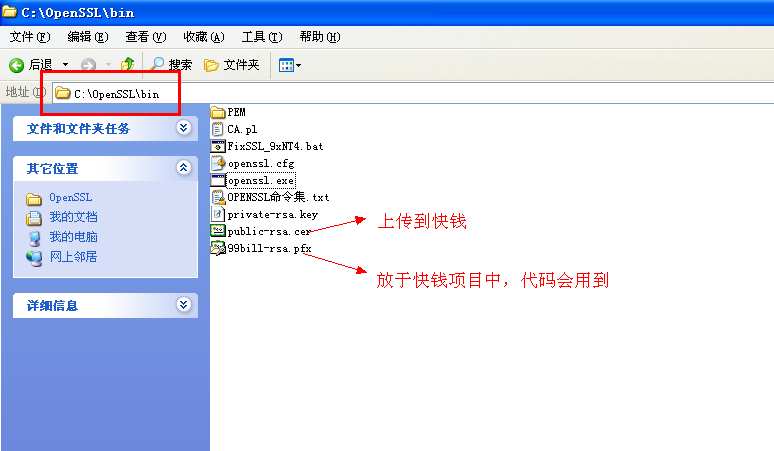


4、输入pkcs12 -export -name test-alias -in public-rsa.cer -inkey private-rsa.key -out 99bill-rsa.pfx，按enter，然后按照第二个图输入密码，密码输入时不会显示出来。商户必须记住该密码，在代码中需要用到。

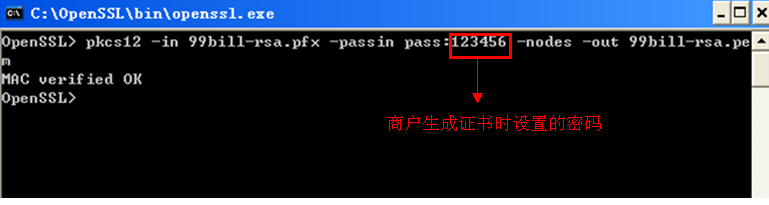


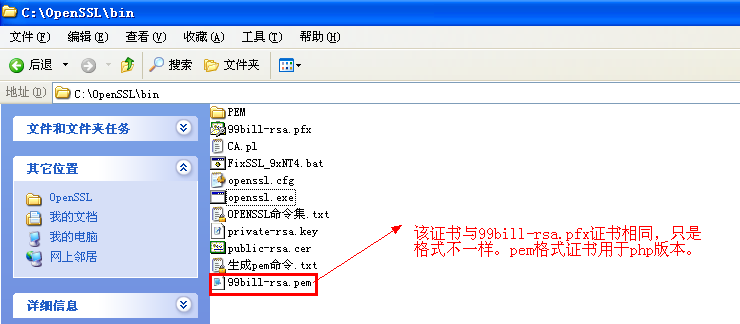


5、如下，进入openssl的bin目录，可以看到执行以上命令后生成的两个证书。



6、如果是使用PHP的商户，需要将“99bill-rsa.pfx”证书转换为“99bill-rsa.pem”，输入转换命令pkcs12 -in 99bill-rsa.pfx -passin pass:此处输入商户第4步设置的密码 -nodes -out 99bill-rsa.pem，按enter即可。进入openssl的bin目录，此时可以看到pem格式证书已经生成。

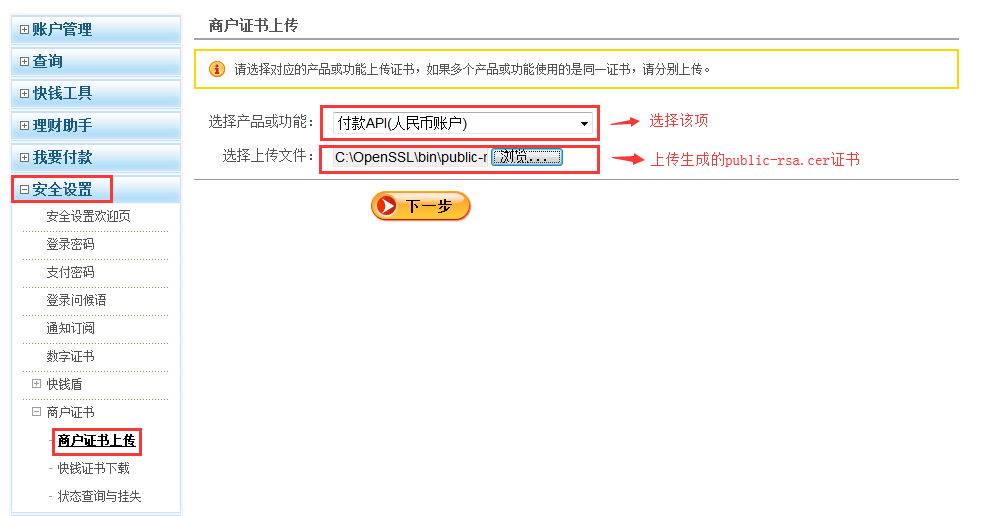




## 证书上传下载

1、上传证书，登陆[www.99bill.com](http://www.99bill.com)，账号和密码请找商户管理快钱账号的人员要，一般是商户的财务。

a、单笔付款，选择产品或功能，请选择：付款API（人民币账户）



2、证书下载，按照下图进行RSA证书下载，这里下载的是快钱公钥证书。

## 证书相关问题

**Q: 商户的证书有效期是多长时间？**

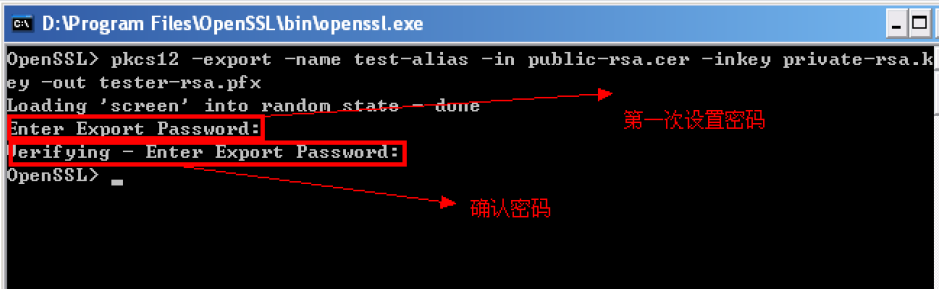
**A**: 一般按照我们的生成命令去生成商户的公私钥的时候，证书的有效期是750天

**Q: 一个商户有多个快钱帐户，证书是否可以用相同的**

**A**: 可以。证书是与商户号关联的。但是出于安全性考虑，不建议商户将所有账户都全部使用统一的证书。

**Q: 我在生成证书第三步的时候，无法“Enter Export Password”，这是什么原因呢**

**A**: 这里输入密码是不会显示出来的，但输入都是有效的，请商户记住自己输入的密码。



**Q: 关于PHP服务器上报不支持openssl\_pkcs12\_read**

**A**: PKI加密方式PHP不支持openssl\_pkcs12\_read这个函数，openssl\_pkcs12\_read 这个函数只有PHP5.2版本以上才支持，所以先要升级到PHP5.2，如果服务器是windows IIS，在windows系统中IIS环境的操作方式：

1、在c:\windows\php.ini中

将;extension=php\_openssl.dll前面分号(注释)去掉

2、复制php安装目录中的： libeay32.dll 、ssleay32.dll 至c:\windows\system32

3、复制PHP\ext目录中的php\_openssl.dll至c:\windows\system32

4、重启IIS

**Q: 上传证书的时候报：证书校验异常：上传证书的失效日期应该晚于XXXX-XX-XX日，请重新上传证书**

**A**: 一般是因为之前已经上传过证书，可将之前上传过的证书进行挂失操作，然后再上传。方法：<http://www.99bill.com> 登录快钱，安全设置-商户证书-状态查询与挂失，在对应的产品证书申请挂失。

