F:\wangchunlan\易联\1.ISO\ISMS 资料\公司基本资料及logo\logo2.gif

**易联支付插件产品**

**商户产生RSA密钥指南**

**V1.0**

**文件编号：EL-PPI-****0614**

**文件版本：V1.0**

**文件等级：内部**

**发布范围：支付插件接入商户、技术支持**

**易联支付有限公司**

**Easylink Commercial Services Co., Ltd.**

**发布日期：2014.06.20**

**实施日期：2014.06.30**

目录

[1 简介 3](#_Toc398762322)

[2 RSA密钥生产和使用 3](#_Toc398762323)

[2.1 生产商户密钥 3](#_Toc398762324)

[2.2 RSA密钥使用逻辑 5](#_Toc398762325)

[2.2.1 JAVA开发语言使用方法 5](#_Toc398762326)

[2.2.2 ASP.NET（C#）开发语言使用方法 6](#_Toc398762327)

[2.2.3 PHP开发语言使用方法 6](#_Toc398762328)

# 简介

此文档为商户产生自己的RSA密钥和使用RSA私钥完成签名进行指导。

# RSA密钥生产和使用

## 生产商户密钥

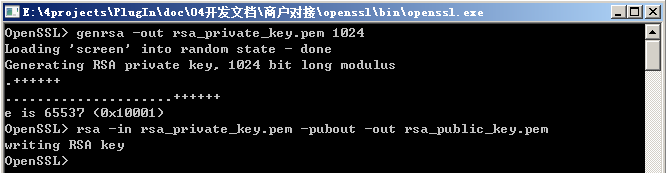
1. 打开RSA密钥生成软件：
   1. 打开RSATools文件，执行openssl.exe文件，如下图：



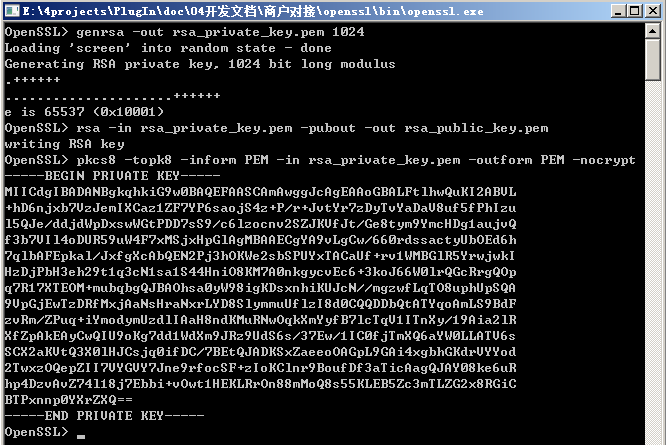
1. 生成RSA私钥：
   1. 输入“genrsa -out rsa\_private\_key.pem 1024”命令，回车后，在当前bin文件目录中会新增一个rsa\_private\_key.pem文件，其文件为原始的商户私钥（请妥善保存该文件，PHP开发语言中需要使用该文件），以下为命令正确执行截图：



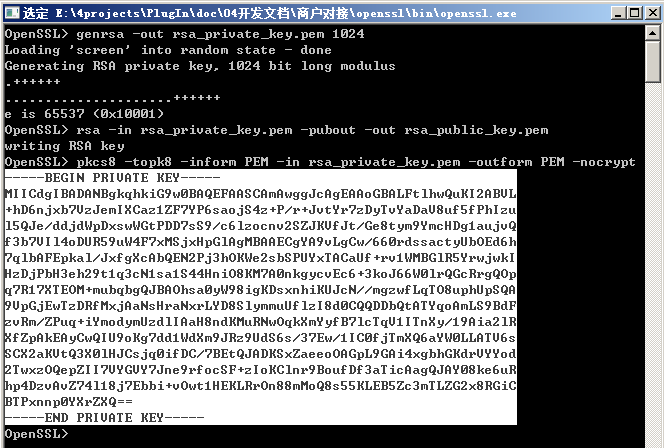
1. 生成RSA公钥：
   1. 输入“rsa -in rsa\_private\_key.pem -pubout -out rsa\_public\_key.pem”命令回车后，在当前bin文件目录中会新增一个rsa\_public\_key.pem文件，其文件为原始的商户公钥（请把该文件提供给易联，做为对您的订单接入签名验证），以下为命令正确执行截图：



1. 生成PKCS8编码的私钥：
   1. 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：



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：



此时继续右键点击openssl窗口上边边缘，选择“编辑→复制”，把复制的内容粘贴进一个新的记事本中，可随意命名，只要知道这个是PKCS8格式的私钥即可（请妥善保存该文件）。

## RSA密钥使用逻辑

1. 商户在使用RSA签名方式的易联接口时，真正会用到的密钥是商户私钥与易联公钥。
2. 商户上传公钥给易联，易联把公钥给商户，是公钥互换的操作。
3. 这就使得商户使用自己的私钥做签名时，易联端会根据商户上传的公钥做验证签名。
4. 商户使用易联公钥做验证签名时，同理，也是因为易联用易联私钥做了签名。

### JAVA开发语言使用方法

* **商户的私钥**

1. 必须保证只有一行文字，即：没有回车、换行、空格等；
2. 需对刚生成的（原始的）私钥做pkcs8编码；
3. 编码完成后，复制该段私钥，并去掉该段里面的回车、换行、空格、“-----BEGIN RSA PRIVATE KEY-----”、“-----END RSA PRIVATE KEY-----”。
4. 商户私钥在DEMO使用位置为Constants.java代码中的的MERCHANT\_RSA\_PRIVATE\_KEY变量；

* **易联公钥**

请参考《易联支付插件产品\_商户接口报文\_V1.0.docx》或JavaDemo；

* **签名和验证签名**

请参考JavaDemo的使用例子；

### ASP.NET（C#）开发语言使用方法

* **商户的私钥**

1. 必须保证只有一行文字，即：没有回车、换行、空格等；
2. 需对刚生成的（原始的）私钥做pkcs8编码；
3. 编码完成后，复制该段私钥，并去掉该段里面的回车、换行、空格、“-----BEGIN RSA PRIVATE KEY-----”、“-----END RSA PRIVATE KEY-----”。
4. 商户私钥在DEMO使用位置为Constants.cs代码中的的MERCHANT\_RSA\_PRIVATE\_KEY变量；

* **易联公钥**

请参考《易联支付插件产品\_商户接口报文\_V1.0.docx》或AspDemo；

* **签名和验证签名**

请参考AspDemo的使用例子；

### PHP开发语言使用方法

* **商户的私钥**

1. 私钥为“genrsa -out rsa\_private\_key.pem 1024”命令产生的文件，文件内容不需要做任何编辑；
2. 文件名可以按商户命名习惯进行修改，建设保持“pem”的后缀文名；

* **易联公钥**

1. php对公钥的使用也是采用文件的方式；
2. 公钥文件请参考demo的“phpdemo\key”目录下的公钥文件：
   1. rsa\_public\_key\_test.pem : 对接测试环境的易联订单公钥文件
   2. rsa\_public\_key\_product.pem : 对接生产环境的易联订单公钥文件

* **签名和验证签名**

请参考phpdemo的使用例子；

* **Openssl配置**

1. 如果你的系统是windows系统，且system32文件目录下没有libeay32.dll、ssleay32.dll这两个文件 ，那么需要拷贝这两个文件到system32文件目录中
2. 如果您的php安装目录下（php\ext）中没有php\_openssl.dll（若已经存在，请不要覆盖），那么请把php\_openssl.dll放在这个文件夹中；
3. 在php.ini中 extension=php\_openssl.dll去掉前面的注释；
4. 判断openssl是否配置生效：打开phpinfo()，有下面的选项：

