PZ0605的专栏

目录视图

个人资料

绿叶清风

关注 发私信

访问： 134513次

积分： 4988

等级： BLOG 5

排名： 第3911名

原创： 351篇 转载： 157篇

译文： 1篇 评论： 7条

文章搜索

文章分类

Mac OSX 使用OpenSSL生成RSA公匙、私匙（pem）与DER文件

2016-07-19 14:56 164人阅读 评论(0)

分类： 网络安全（14） ios项目（62）

说明：RSA为一种加密算法，生成的文件格式有两种，一种是PEM格式，另一种是DER格式，在Mac OSX 里面，pe

的，因此我们生成PEM文件之后，需要生成DER格式。需要按着下面的步骤走。

***.DER*=扩展名DER用于二进制DER编码的证书。这些证书也可以用CER或者CRT作为扩展名。比较合适的说法是“我**

证书”，而不是“我有一个DER证书”。

***.PEM*=扩展名PEM用于ASCII(Base64)编码的各种X.509 v3 证书。**文件开始由一行"——BEGIN ... “开始

1.mac 自带openssl环境，不用安装，直接使用openssl就可以。

2.打开终端。

3.输入命令行：baomatoMac-mini:~ lixiangyang$ ***openssl（打开openssl环境）***

4.继续下一步命令行：OpenSSL> ***genrsa -out rsa_private_key.pem 1024 (命令生成私匙)*** **下面是输出结果：**

Generating RSA private key, 1024 bit long modulus

.....++++++

..++++++

e is 65537 (0x10001)

5.下一步：OpenSSL> ***pkcs8 -topk8 -inform PEM -in rsa_private_key.pem -outform PEM –nocrypt（命令把***

PKCS8格式，密码为空就行）注意：转化之后生成的pem格式的文件（文本编译器打开的字符串），是pkcs8文件。

始 的私钥key。

下面是输出结果：

Enter Encryption Password:（密码 ）

Verifying - Enter Encryption Password:（再一次确认密码）

-----BEGIN ENCRYPTED PRIVATE KEY-----

MIICoTAbBgkqhkiG9w0BBQMwDgQInAB4b4BNL0ECAggABIICgF27qIz6cNwxy8Jg

JhWUK8kIqHLwZRznHTIBCZlu9eZHa1a0+p7FWmufYgfZz9Kz3GeK5cxILrxmwci1

TTP6Qthak7lWJLO5gJH47HBd50OeXdZWt6xD6Vp+YzyaztpmZ8SLMi5aGKw1CBVc

Dw1oJzD4BIk9LBYo9kqvZODp4waytDjaZDhnN65t8+R4TbnMK7yVsT+fTGCMkQmu

cr34jGOhoUYZBcwtxWwNbRptftnUwgdaV5jrKnQ5rJsxU3Bx+3SuaRZS7ef0Z9yO

ADpW6NACI3R9+6DT3k66qTfbz9F/tLVO6flZ8g9TY2zTJKtGYmb1N/ll0qAXFh7s

lD2WZhPdYGozICMWi1MvT55RI3hlosilQW8Ff5IXNmzFs7RgZlvfVRzVlryPXu5I

QWKnNUamRN88grHSBuXYesp/cwze0D9ma8LavoVmjaKVT85SU3J9PbPoSjbTc/nP

javascript (8)
c/c++ (13)
linux (26)
面向对象分析与设计 (7)
汇编 (1)
软件测试 (1)
设计模式 (4)
搜索引擎 (0)
杂七杂八 (2)
android译文 (1)
协议/XMPP (11)
javaWeb (17)
编译原理 (0)
数据结构与算法 (3)
ios多线程/ios网络 (11)
Node.js&MongoDB (20)
ios数据库/缓存 (8)
ios数据库 (2)
ios项目 (63)
ios autolayou (12)
html/css (23)
bootstrap (5)
swift (10)
ios框架及源码解析 (2)
photoshop (1)
mac (15)
项目管理 (3)
ios9 (4)
ios进阶 (5)
网络安全 (15)
Android移植 (3)
Linux内核 (1)
嵌入式-ARM (10)
Linux驱动 (1)
CoffeeScript (5)

文章存档

2016年09月 (41)
2016年08月 (7)
2016年07月 (22)
2016年06月 (4)
2016年05月 (9)

展开

阅读排行

前端开发面试题及答案 (1262)
自建证书配置HTTPS服务器 (1225)
js拼接字符串时，字符串的事... (1047)
ios 得用代理反向传值 (1009)
利用AutoLayout uilabel文字... (974)
ArgoUML 的简单用法 (936)
Android 面试整理 (923)
Fragment生命周期详解 (877)
android 开关按钮 (875)
前端学习知识汇总（包括js,cs... (864)

评论排行

Android Fragment应用实战... (1)

f20u0Gsx0bQdeMOswMpWe/AQeGj/MSs59ae93SfvWnQi0ONWeBkrQUD6OskrOJeo

jsmevTmubk191W9WiX/klOyGI/YXjl99qNmQo5wx6fWOfdRQ4/Urw5z9tozAXL5s

hYdUmV+eiNgddM/cdxpDbJtXhSvpq1RXqhBTsMPctCB8EUfG6adJ4ZgjZ8eTA3FF

2btbQ5Fqrw/y5ZFvqYlryKqoPgCa7gtKU8wQHkzDpfGUSX1eXfJQ1HZxywY44YlZ

sWwVNuVwDvnd2ZkZqHjqbyOHXPnORR8fvteaGJazD2VW8DaPMc0xIplN/Prp5VPj

nBnevsF7WDREV4cUVw5I7SsPWOMl0X/OocZOE3IPx364H6DkpYryfVs/rDWgqweK

AphvBEA=

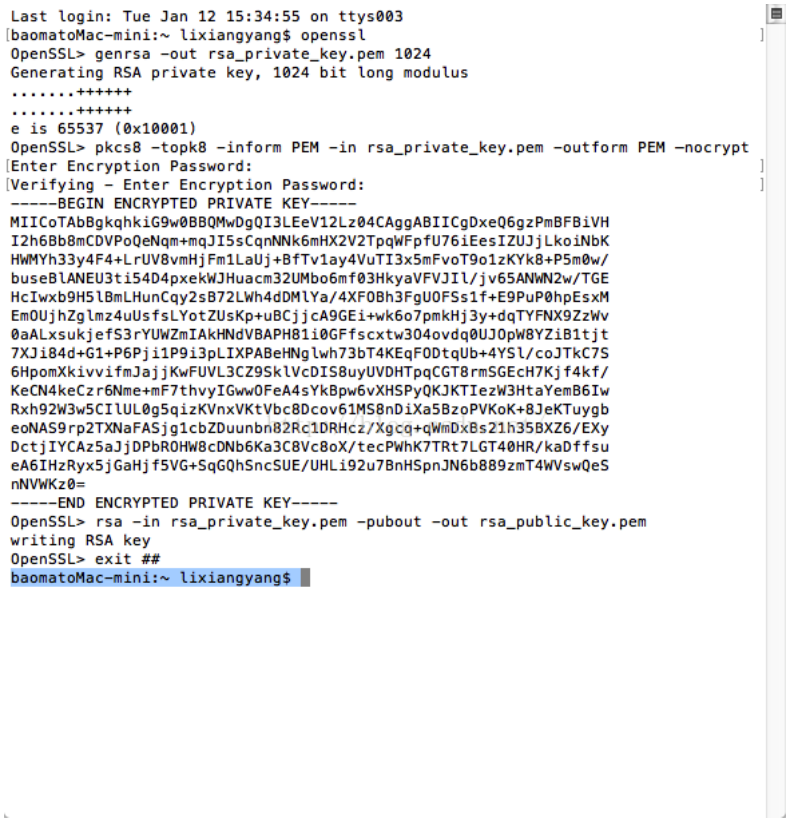
-----END ENCRYPTED PRIVATE KEY-----

6.下一步：OpenSSL> rsa -in rsa_private_key.pem -pubout -out rsa_public_key.pem ***（命令生成公匙）***

下面是结果：

writing RSA key

配置终端生成图片：



7.生成 .der 文件

OpenSSL> ***req -new -out cert.csr -key rsa_private_key.pem（创建证书请求）***

下面是输出结果：

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:

8.下一步根据提示敲回车，填写证书的内容：英文模板如下：

```
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:Hangzhou
Locality Name (eg, city) []:Zhejiang Provice
Organization Name (eg, company) [Internet Widgits Pty Ltd]:WDWL
Organizational Unit Name (eg, section) []:WDWL
Common Name (e.g. server FQDN or YOUR name) []:WDWL
Email Address []:[redacted]

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:[redacted]
An optional company name []:WDWL
```

中文模板：

```
签发者名称
    国家/地区  CN
    省/市/自治区  Hangzhou
    所在地  Zhejiang Provice
    组织  WDWL
    组织单位  WDWL
    常用名称  WDWL
    电子邮件地址  [redacted]

序列号  00 8E 4E 47 F3 3F BF BD A9
版本  1
签名算法  带 RSA 加密的 SHA-1 ( 1.2.840.113549.1.1.5 )
    参数  无
```

9.下一步：

OpenSSL> ***x509 -req -in cert.csr -out rsa_public_key.der -outform der -signkey rsa_private_key.pem -d***

署根证书）

输出结果：

Signature ok

subject=/C=CN/ST=Hangzhou/L=Zhejiang Provice/O=WDWL/OU=WDWL/CN=WDWL/emailAddress=xxxxxxx@1

Getting Private key

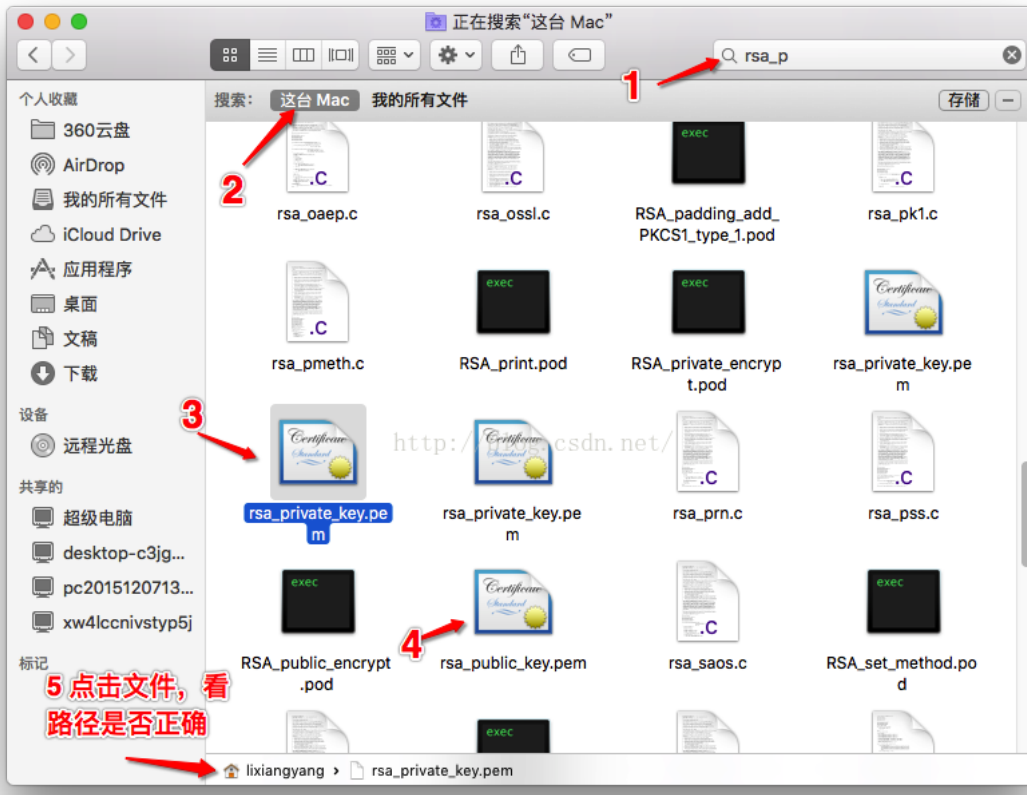
10.下一步：OpenSSL>***exit ##（关闭OpenSSL）***

结果：

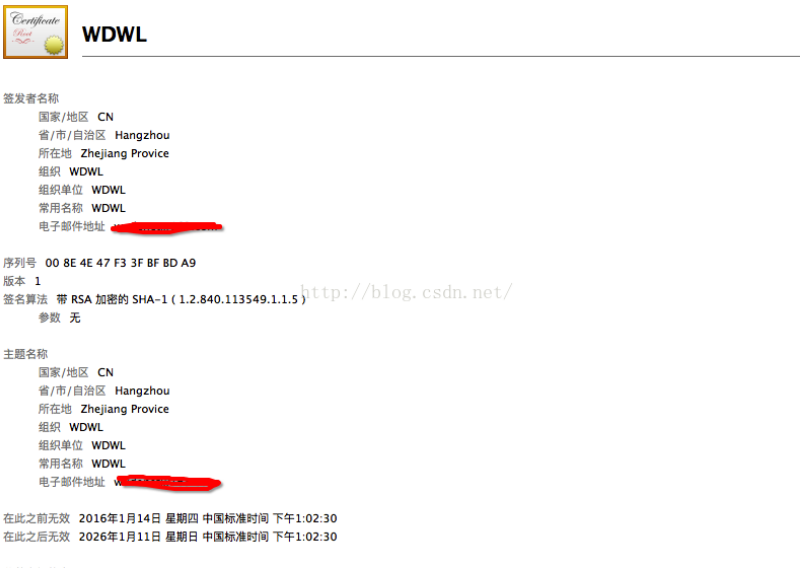
baomatoMac-mini:~ lixiangyang$

11.生成的RSA公匙私匙 与 DER 文件：

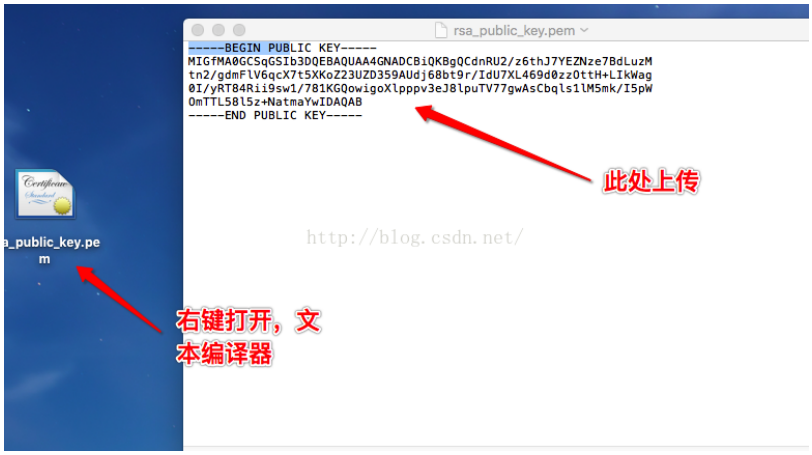
12.当生成这三个文件的时候，需要在Finder里面搜索，才能找到，并将三个文件拖到桌面上来 ，下面是图的步骤。



13.验证证书。直接将rsa_public_key.der 拖到Xcode里面，双击打开，就会看到下面的情况。表示成功。



14.通过Mac自带的 文本编辑 打开两个文件，并且将生成的字符串记录下来。将公匙传到支付宝平台上。



11.参考链接：

一》生成RSA官方链接： http://www.openssl.org/docs/manmaster/apps/rsa.html

二》生成RSA pem文件： http://blog.sina.com.cn/s/blog_6f72ff900102v408.html

三》生成RSA pem文件: http://blog.csdn.net/fenglibing/article/details/8610280

四》生成DER：http://blog.sina.com.cn/s/blog_8589a6890102vitk.html

五》ios下使用rsa算法与php进行加解密通讯：https://blog.yorkgu.me/2011/10/27/rsa-in-ios-using-publick-key-gener

六》der与pem文件格式的区别： http://blog.sina.com.cn/s/blog_a9303fd90101jmtx.html

- 下一篇 利用NSURLSession实现https请求

我的同类文章

网络安全（14） ios项目（62）

- java将字节转换成十六进制输出 2016-08-25 阅读 36
- mosquitto源码分析（四） 2016-07-26 阅读 47
- mosquitto源码分析（二） 2016-07-26 阅读 42
- android mosquitto客户端使用SSL功... 2016-07-26 阅读 99
- iOS(xcode) 加入openssl的方法 2016-07-20 阅读 168
- 利用NSURLSession实现https请求 2016-07-19 阅读 177
- mosquitto源码分析（五） 2016-07-26 阅读
- mosquitto源码分析（三） 2016-07-26 阅读
- mosquitto源码分析（一） 2016-07-26 阅读
- Mac 下 Mosquitto 安装和配置 (Mosq... 2016-07-20 阅读
- ios 编译openssl支持arm64 2016-07-20 阅读

猜你在找

精通iOS移动开发(Xcode7&Swift2…
疯狂IOS讲义之Objective-C面向…
老郭全套iOS开发课程【Objectiv…
iOS8开发视频教程Swift语言版-P…
iOS开发从入门到精通(Xcode8和S…
golang rsa公钥私钥pem文件生成
java读取OPENSSL生成的DSA的pem…
关于用Openssl生成pem文件用于G…
java读取OPENSSL生成的DSA的pem…
MAC OS下OpenSSL生成私钥和公钥…

查看评论

暂无评论

您还没有登录,请[登录]或[注册]

* 以上用户言论只代表其个人观点，不代表CSDN网站的观点或立场

核心技术类目

全部主题 Hadoop AWS 移动游戏 Java Android iOS Swift 智能硬件 Docker OpenStack VPN
IE10 Eclipse CRM JavaScript 数据库 Ubuntu NFC WAP jQuery BI HTML5 Spring Apache
HTML SDK IIS Fedora XML LBS Unity Splashtop UML components Windows Mobile Rails
Cassandra CloudStack FTC coremail OPhone CouchBase 云计算 iOS6 Rackspace Web App SpringS
Compuware 大数据 aptech Perl Tornado Ruby Hibernate ThinkPHP HBase Pure Solr Angular
Cloud Foundry Redis Scala Django Bootstrap