今天做这么一个事，
centos 服务器，tomcat8+nginx1.6，现在要在上面运行cas4.0。
所以需要配ssl，
然后找教程，了解到，需要把tomcat和nginx 的ssl都配置好。
到这里就晕了，tomcat配ssl需要一个.keystore文件，nginx则需要配一个.crt和一个.key的文件。
按照教程使用keytool生成了.keystore文件，
然后我需要通过.keystore导出一个.crt文件，但是找了好多教程只是导出.cer文件。
找来找去发现.crt和.cer是一个东西。
后来又找到了一个.pem的东西，好像和.crt,.cer也是一个东西。
然后我就凌乱了。
希望有高手能指点一下，SSL的公钥、私钥、证书都有些啥后缀？
若能再指点一下tomcat8+nginx1.6上安装cas4.0，那就更好了。

一、常用

> 证书(Certificate) - *.cer *.crt
> 私钥(Private Key) - *.key
> 证书签名请求(Certificate signing request) - *.csr
> 证书吊销列表(Certificate Revocation List) - *.crl

至于pem和der，是编码方式，以上三类均可以使用这两种编码方式，
因此*.pem和*.der(少见)不一定是以上三种(Cert,Key,CSR)中的某一种

> *.pem - base64编码
> *.der - 二进制编码

二、全部

X.509	一种通用的**证书格式**，包含证书持有人的公钥，加密算法等信息
pkcs1 ~ pkcs 12	公钥加密（非对称加密）的一种**标准**（Public Key Cryptography Standards），一般存储为 `*.pN`，，`*.p12` 是包含证书和密钥的封装格式
*.der	证书的二进制**存储格式**（不常用）
*.pem	证书或密钥的**Base64**文本**存储格式**，可以单独存放证书或密钥，也可以同时存放证书或密钥
*.key	单独存放的**pem**格式的密钥，一般保存为 `*.key`
*.cer *.crt	两个指的都是证书，Linux下叫crt，Windows下叫cer；存储格式可以是 `pem`，也可以是 `der`
*.csr	证书签名请求（Certificate signing request），包含证书持有人的信息，如：国家，邮件，域名等信息
*.pfx	微软IIS的实现
*.jks	Java的keytool实现的证书格式

证书的格式可以相互转换，**openssl**先生成私钥，然后再生成证书签名请求，最后通过私钥和证书签名请求生成公钥。

创建证书签名请求（Certificate signing request）和私钥（Primary key）：

```
openssl req -newkey rsa:2048 -nodes -out test.csr -keyout test.key
```

创建公约（Public key）

```
openssl x509 -req -days 365 -in test.csr -signkey test.key -out test.crt
```


三、举例说明

我把SSL系统比喻为工商局系统。

CA

首先有SSL就有CA，certificate authority。证书局，用于制作、认证证书的第三方机构，我们假设营业执照非常难制作，就像身份证一样，需要有制证
供，并且提供技术帮助工商局验证执照的真伪。

然后CA是可以有多个的，也就是可以有多个制证公司，但工商局就只有一个，它来说那个制证公司是可信的，那些是假的，需要打击。在SSL的世界
Google和Mozilla扮演了一部分这个角色。也就是说，IE、Chrome、Firefox中内置有一些CA，经过这些CA颁发，验证过的证书都是可以信的，否
你不安全。

这也是为什么前几天Chrome决定屏蔽CNNIC的CA时，CNNIC那么遗憾了。

也因为内置的CA是相对固定的，所以当你决定要新建网站时，就需要购买这些内置CA颁发的证书来让用户看到你的域名前面是绿色的，而不是红色。
大的卖证书的公司就是VeriSign如果你听说过的话，当然它被卖给了Symantec，这家伙不只出Ghost，还是个卖证书的公司。

Ceritficate

> **cer（windows中的叫法）**
> **crt（linux中的叫法）**

要开店的老板去申请营业执照的时候是需要交他的身份证的，然后办出来的营业执照上也会有他的照片和名字。
身份证相当于私钥，营业执照就是证书【**Ceritficate**】，即 **.cer**文件（或**.crt**文件）。

然后关于私钥和公钥如何解释我没想好，而它们在数据加密层面，**数据的流向**是这样的：

```
消息-->[公钥]-->加密后的信息-->[私钥]-->消息
```

公钥是可以随便扔给谁的，他把消息加了密传给我。
可以这样理解，我有一个箱子，一把锁和一把钥匙，我把箱子和开着的锁给别人，他写了信放箱子里，锁上，然后传递回我手上的途中谁都是打不开
有我可以用原来的钥匙打开，这就是SSL，公钥，私钥传递加密消息的方式。这里的密钥就是key文件。于是我们就有了.cer和.key文件。（**证书即公**

keystore

不同的语言、工具序列SSL相关文件的格式和扩展名是不一样的。

其中Java系统默用keystore、truststore来干活。
你看它的名字，Store，仓库，它里面存放着key和信任的CA，key和CA可以有多个。

- **truststore（证书仓库）——存放一个或多个CA**

*这里的**truststore**就像你自己电脑的**证书管理器**一样，如果你打开Chrome的设置，找到HTTP SSL，就可以看到里面有很多CA，truststore就是干的，它也里面也是**存一个或多个CA**让Tomcat或Java程序来调用。*

- **keystore（密钥仓库）——存放一个或多个key**

*而**keystore**就是用来**存密钥文件**key的，可以**存放多个**。*

PEM

然后是PEM，它是由RFC1421至1424定义的一种数据格式。**其实前面的.cert和.key文件都是PEM格式的**，只不过在有些系统中（比如Windows）名不同而做不同的事。

所以当你看到.pem文件时，它里面的内容可能是Ceritficate也可能是key，也可能两个都有，要看具体情况。可以通过openssl查看。

参考自：SSL中，公钥、私钥、证书的后缀名都是些啥？ - 知乎

SSL/CA 证书及其相关证书文件(pem、crt、cer、key、csr) RayPick的
SSL 证书是数字证书的一种，类似于驾驶证、护照和营业执照的电子副本。因为配置在服务器上，也称为服务器证书。SSL 证书只有正确安装到 Web 服务器，才能实现客

关于 SSL/CA 证书及其相关证书文件（pem、crt、cer、key、csr） weixin_42108319的
客户端向服务器发送"ClientHello"消息，其中包含客户端支持的TLS版本、提议的加密套件列表（加密算法和密钥交换方法的组合）、一个客户端生成的随机数（Client Ran

HTTPS证书创建_ssl证书制作
3.3.2.1 创建密钥cert-key.pem和数字证书请求csr文件 3.3.2.2 创建证书文件cert.crt 3.3.3 创建自建证书(方式二) 3.4 查看证书内容 四、Nginx代理配置 4.1 配置Nginx配置文

SSL证书后缀整理 xiaowenshiyilang的
SSL证书后缀整理 key：用来存放公私钥。 pem：证书，base64编码 der：证书，二进制文件 crt：证书 csr：证书请求文件 keystore jks truststore：java中使用，包含证书

关于加密文件后缀 .cer，.crt，.key，.csr，.crl，jks 傻傻分不清 ratel的
关于加密文件后缀 .cer，.crt，.key，.csr，.crl，jks 傻傻分不清

证书关于 pem der cer crt csr pfx 的区别 yetugeng的
刚开始接触证书的时候，对于这几个词语pem der crt cer pfx尤为的疑惑。研究了一番，总结如下。 一.名词解释 这里先介绍一下X.690，它是ITU-T标准，规定了几种ASN.

证书相关后缀文件 xx1129244705的
jks是JAVA的keytools证书工具支持的证书私钥格式。 pfx是微软支持的私钥格式。 cer是证书的公钥。 简单来说，cer就是你们家邮箱的地址，你可以把这个地址给很多人

证书相关后缀文件(SSL,X.509,PEM,DER,CRT,CSR,CER,KEY,P12)及RSA数据加密解密 shiios的
首先,要说一句还在为标题中的东西迷茫的帅哥美女工程师们,你们的福利来啦! 其次,我要感谢提供这些信息的两位资深工程师大神. 最后让我们一起揭晓这神秘的面纱吧: 证

SSL各种眼花迷乱的证书后缀 小小默：进无止
项目要用Https，自然需要知名机构的SSL证书。这里记录一下让人头疼的各种证书后缀。 ① x.509 X.509是常见通用的证书格式，包含证书持有人的公钥，加密算法等信息

搞懂 PEM、ANS、PFX、P12、p8、CER、X509 等证书相关文件格式 后缀
http证书相关的文件格式、编码、概念比较偏多。这里对文件的各种文件后缀和格式做了统一的整理和解释说明

SSL证书的格式与扩展名是什么样的 蔚可云的
编码格式 PEM 内容：以 -----BEGIN xxx----- 作为开头，以 -----END xxx----- 作为结尾，主体部分使用 base64 对 ACII 进行编码。可以储存公钥证书（服务器证书及中检证书，

证书，私钥，公钥，pfx,keystore,pem,der 都是什么? 云守护的
转自：https://blog.csdn.net/qq_30698633/article/details/77895151 我们知道，现在的网站为了数据的安全，往往都会使用证书进行签名或者加密数据。可以证书的各种

python3如何使用ssl和公钥私钥，和服务器进行认证通信?
使用 Python 3 进行 SSL 和公钥私钥认证通信的步骤如下： 1.生成自签名证书 在服务器端，需要生成自签名证书，并将其安装到服务器上。可以使用 OpenSSL 命令行工具

HD243608836
码龄8年 暂无认证

116	2万+	3万+	409万+	
原创	周排名	总排名	访问	等级

2万+	1194	1939	414	7466
积分	粉丝	获赞	评论	收藏

私信 关注

搜博主文章

热门文章

分类专栏

最新评论

最新文章

目录

CA

Ceritficate

keystore

PEM